System Logging

for on-premesis and SaaS deployments
VMware Workspace ONE UEM 1902

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

1 VMware Workspace ONE UEM System Logging 4

- Console Logging 6
- Device Services and Self-Service Portal Logging 7
- API Logging 9
- AWCM Logging 10
- Peripheral Component Logging 10
- Device-Side Logs 17
- Miscellaneous Logs 23
- Core Component Verbose and Targeted Logging 23
- Manage the Core Component Logging Level 24
- Enabling Targeted Logging 25
  - Enable Device-Based Targeted Logging 25
  - Enable Settings-Based Targeted Logging 25
- Peripheral Component Verbose Logging 26
  - Change the Logging Level for the ACC Service 27
  - Change the Logging Level for the EASListener Service 27
  - Change the Logging Level for the EASintegration Service 27
  - Change the Logging Level for the SEG Setup Service 28
  - Change the Logging Level for the Kerberos Service 28
  - Enable SEG Targeted Logging for Devices 28
  - Change the Logging Level for the SEGv2 Service 28
  - Change the Logging Level for the Email Notification Service 29
  - Change the Logging Level for the Content Gateway 29
  - Change the Logging Level for the Unified Access Gateway Service 29
  - Change the Logging Level for Remote File Storage 29
  - Change the Logging Level for the Content Rendering Engine 30
  - Change the Logging Level for the VMware Identity Connector 30
- Data Aggregator 30
  - Install the Data Aggregator on Your Servers 31
  - Templates for Data Aggregator 31
- Capture Logs 33
- Logging Examples 33

VMware Workspace ONE UEM System Logging

1

This documentation provides guidance on the logging functions available for your deployment of the VMware Workspace ONE™ UEM solution.

Every on-premises deployment of Workspace ONE UEM is unique and has distinct requirements. Your deployment of Workspace ONE UEM may not use all of these logs.

Core Components

Explore and implement logging for the core components of your Workspace ONE UEM deployment.

For more information, see:

- Console Logging
- Device Services and Self-Service Portal Logging
- API Logging
- AWCM Logging

Peripheral Components

Explore and implement logging for peripheral components that you may have integrated into your Workspace ONE UEM deployment.

For more information, see Peripheral Component Logging.

Device-Side Hub Logs

Explore and implement logging for end-user devices running the Workspace ONE Intelligent Hub.

For more information, see Device-Side Logs.

Miscellaneous Logs

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

For more information, see Miscellaneous Logs.

Core Component Verbose and Targeted Logging

Increase the level of logging to capture additional verbose log entries for Workspace ONE UEM core components.

For more information, see Core Component Verbose and Targeted Logging.

Peripheral Component Verbose Logging

Increase the level of logging to capture additional verbose log entries for Workspace ONE UEM peripheral components.

For more information, see Peripheral Component Verbose Logging.

Logging Best Practices

Explore and implement best practices for capturing logs for your Workspace ONE UEM deployment.

For more information, see Capture Logs and Logging Examples.

This chapter includes the following topics:

- Console Logging
- Device Services and Self-Service Portal Logging
- API Logging
- AWCM Logging
- Peripheral Component Logging
- Device-Side Logs
- Miscellaneous Logs
- Core Component Verbose and Targeted Logging
- Manage the Core Component Logging Level
- Enabling Targeted Logging
- Peripheral Component Verbose Logging
- Data Aggregator
- Capture Logs
- Logging Examples

Console Logging

The following table lists the logging functions available for the Console component. Please note that the API service is installed by default. All Logs are located in the /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	AgentBuilder.log	Contains information on rugged Hub (CAB) creation for side load enrollment.
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.
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.

Folder	Log Name	Description
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	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.
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
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

The following table lists the logging functions available for the Device Services component. Please note that the API service is installed by default. All Logs are located in the /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.

Folder	Log Name	Description
AirWatch API	AW_MEM_Api.log	Contains information relating to specifically the /API/MEM endpoint.
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	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	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).

Folder	Log Name	Description
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.
TargetedLogging	####Airwatch.log	Contains information on targeted logging enabled devices.

API Logging

The following table lists the logging functions available for the API component. All Logs are located in the /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.
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.

Folder	Log Name	Description
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	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

The following table lists the logging functions available for the AWCM component. All Logs are located in the /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.

Peripheral Component Logging

Explore and implement logging for peripheral components that you may have integrated into your Workspace ONE UEM deployment.

All Logs are located in the /AirWatch/Logs folder unless otherwise specified.

VMware AirWatch Cloud Connector (ACC)

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

Classic Secure Email Gateway (SEG)

Folder	Log Name	Description
EASListener	Username.log or EASIdentifier.log	Contains information on a single device's transactions with the SEG and forwarded responses to Exchange. You must enable this targeted log as it is not enabled by default.
EASListener	AW.EAS.Web.Listener.Log	Contains information on all device transactions with the SEG and forwarded responses to exchange.
SEG Console	AW.EAS.Web.Log	Contains information on back end service communication as well as updated device policy records.
SEG Setup	AW.EAS.Setup.log	Contains log information on initial configuration and changes to SEG setup configurations.
Services	AirWatchDiagnositcServiceSEG.log	Contains information on SEG diagnostic sample processing and saving.
Services	AW.EAS.IntegrationService.log	Contains information on SEG device policy API integration and MEM Configuration service communication.
Services	AirWatch.Kerberos.AuthService.log	Contains information on Kerberos token authentication.
Inetpub > Logs > W3SVC1	U_ex####.log	Contains history of IIS endpoints accessed and response codes delivered (Ex: /Microsoft-Server-Activesync).

Secure Email Gateway v2 (SEGv2)

Folder	Log Name	Description
SecureEmailGateway	App.log	Contains information on device transactions and an analysis of each request passed through SEGv2.
SecureEmailGateway	http-transaction.log	Contains information on overview of each email request passed through SEGv2 (Transaction summary).
SecureEmailGateway	Policy-update.txt	Contains information on the policy cache and any real-time or bulk policy updates.
SecureEmailGateway	Active-sync-payload-reporting.txt	Contains information on console transaction reporting including details on EAS request info posted to console.
SecureEmailGateway	Non-compliant-devices.txt	Contains information on the blocked transactions and detail analysis of those refused requests.

Email Notification Service

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.

Email Notification Service v2

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.

VMware Tunnel

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.

VMware AirWatch Content Gateway

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.

Unified Access Gateway (System Information)

For UAG-based services using the Log Archive download option under the UAG Admin UI Support Settings page.

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
/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

Unified Access Gateway

For UAG based services using the Log Archive download option under the UAG Admin UI Support Settings page.

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

Folder	Log Name	Description
/Opt/VMware/Gateway/Logs	esmanager-std-out.log	Contains information on the Edge service manager which shows back end processes performed on the appliance
/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	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.

Remote File Storage

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

Content Rendering Engine

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

VMware Identity Manager Service

Folder	Log Name	Description
/…/opt/vmware/horizon/workspace/logs	Accessontrol-service.log	Access control service logging which handles role based access control for vIDM 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.

Folder	Log Name	Description
/…/opt/vmware/horizon/workspace/logs	Audit.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.
/…/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 Identity Manager Enterprise System 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 the Identity Manager.
/…/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).

Folder	Log Name	Description
/…/opt/vmware/horizon/workspace/logs	Localhost.log	Contains information on the Spring framework. Date indicates roll-over.
/…/opt/vmware/horizon/workspace/logs	logGroupprov-calc-stats.log	Contains information on an additional background calculator specifically the group provisioning calculations.
/…/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	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 Identity Manager service for Windows.

VMware Identity Manager Connector

Folder	Log Name	Description
/VMware/IDMConnector/	Idm-connector-installer.log	Contains information on install history and status of the Identity Manager 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 Identity Manager 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.

Workspace One Intelligence

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

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

Dell Factory Provisioning Service

The following table lists the 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/Factory Provisioning Services/Services/Logs/	AW.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/Logs/	AW.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.

Airlift

The following table lists the 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

Device-Side Logs

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

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

Method	Log Name	Description
Console.app	*.txt	Contains information related to all device side transactions including MDM, enrollment, access, and application run history.
/Library/Application Support/Airwatch/Data/Logs	AirWatchDaemon.log	Contains information needed to analyze issues with core macOS Hub functionalities such as products, CAs, and Hub profiles.
/Library/Application Support/Airwatch/Data/Logs/	AirWatchAgent.log	Contains information on the UI/UX functionality with the macOS Hub.
/Library/Application Support/Airwatch/Data/Logs	AirWatchAWCM.log	Contains information on the macOS Hub to AWCM connectivity.
/Library/Application Support/Airwatch/Data/Logs	AirWatchRemoteManagement.log	Contains information related to remote management communications.
/var/log/	System.log	Contains information on the mdmd and other OS specific activities. Not used for macOS 10.12+.
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

Method	Log Name	Description
Enhanced log targeting (Apple)	N/A	For more information, see the Apple documentation on Profiles and Logs available on developer.apple.com.
/Library/Application Support/AirWatch/Data/Munki/managed installs/logs/	ManagedSoftwareUpdate.log	Main Munki logging file. Which will contain information pertaining to application deployment of .dmg MAC OS applications.
/Library/Application Support/Airwatch/Data/Munki/munki_repo/munkiData/	Munki_data.plist	Munki Data Cache
/Library/Preferences/	AirWatchManagedInstalls.plist	Munki preference file
/Library/Application Support/AirWatch/Data/Munki/Managed Installs/	InstallInfo.plist	Munki install list
/Library/Application Support/AirWatch/Data/Munki/Managed Installs/	ManagedInstallReport.plist	Munki managed install report
/Library/Application Support/AirWatch/Data	AppStatuses_WS1.plist	WS1 app install status percentages

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** and tap **Software Information** 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

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

Widows Desktop Devices (Protection Agent)

For deployments using the VMware AirWatch Protection Agent, 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.

Method	Log Name	Description
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.
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 Protection Agent)

If your deployment does not include the VMware AirWatch Protection Agent, 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.
/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 nrolment method.

Windows 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.

Method	Log Name	Description
/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.

Miscellaneous Logs

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

Some logging may require additional components or requirements to gather.

Application Wrapping Logs

Method/Folder	Log Name	Description
App Wrapping Server	AppWrap.log	Contains information on status and results of application wrapping attempts.
ADB/Android Studio/RXLogger	*.txt	Contains information on app level traffic such as system messages and stack traces.
Console app on macOS	*.txt	Contains information related to all device side transactions such as MDM, enrollment, and application run history.

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.

Core Component Verbose and Targeted Logging

Increase the level of logging to capture additional verbose log entries for Workspace ONE UEM core components.

To manage logging levels, see Manage the Core Component Logging Level.

To implement targeted verbose logging, see Enabling Targeted Logging.

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]
```

Info Log Example

Workspace ONE UEM info 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
```

Log Example Key

Every log entry contains the following 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.

Manage the Core Component Logging Level

The Workspace ONE UEM console controls the logging level for AirWatch core components. Change these logging levels when you are troubleshooting issues with core components.

The two logging levels provide different levels of detail. When you are not troubleshooting a component, set the logging level to **Disabled** to reduce use of hardware resources.

Procedure

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

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

What to do next

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

Enabling Targeted Logging

The AirWatch Console can target verbose logging for specific devices. Targeted logs assist in gathering all necessary logging when troubleshooting a particular device or set of devices.

Enable device-based or settings-based targeted logging, depending on the size of the device pool you need to access.

For more information about enabling device-based targeted logging, see Enable Device-Based Targeted Logging.

For more information about enabling setttings-based targeted logging, see Enable Settings-Based Targeted Logging.

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**.

Peripheral Component Verbose Logging

Each peripheral component handles logging differently from the core components handled by the Workspace ONE UEM console. You must access each component server to change the logging level.

Important After you finished troubleshooting, revert the logging level back to Disabled to preserve hardware resources.

Email Notification Service v2

By default, ENSv2 runs at the most verbose level of logging.

VMware Tunnel

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

AirWatch Content Gateway

To change the logging levels for the Content Gateway, access the logback.xml file contained in the Content Gateway Config folder. Change the level to debug in the <logger name="com.airwatch" level="info" /> line. The service may take a few minutes to register the logging change.

Unified Access Gateway

To change the logging levels for the Unified Access Gateway service:In the Unified Access Gateway Admin UI, navigate to **Support SettingsLog Level Settings**. Select **INFO**, **ERROR**, **WARNING**, or **DEBUG** based on your requirements. The service may take a few minutes to register the logging change.

Level	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.

Remote File Storage

To change the logging levels for Remote File Storage:

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

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

  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.

3 Save changes and restart each service.

VMware Identity Manager Service

To change the logging level for the VMware Identity Manager Service in the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > Admin > Diagnostics > Logging**.

Workspace One Intelligence

By default, Workspace ONE Intelligence (ETL) runs at the most verbose level of logging.

Memcached

By default, Memcached runs at the most verbose level of logging.

Change the Logging Level for the ACC Service

Procedure

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.

Change the Logging Level for the EASListener Service

Procedure

1 Access the SEG service page contained at http://localhost/segsetup.

2 Select **Verbose** from the logging level box.

3 Select **Save**.

4 Wait a few minutes for the EASListener to pick up the logging change.

Change the Logging Level for the EASintegration Service

Procedure

1 Access the AW.EAS.IntegrationService.exe.config file contained in the /AW.Eas.IntegrationService folder.

2 Change the level from **Error** to **Verbose** in the <loggingConfiguration> line.

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

Change the Logging Level for the SEG Setup Service

Procedure

1 Access the Web.config file contained in the /AW.Eas.Setup folder.

2 Change the level from **Error** to **Verbose** in the <loggingConfiguration> line.

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

Change the Logging Level for the Kerberos Service

Procedure

1 Access the AirWatch.Kerberos.AuthService.exe.config file contained in the /AirWatch.KCD.AuthService folder.

2 Change the level from **Error** to **Verbose** in the <loggingConfiguration> line.

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

Enable SEG Targeted Logging for Devices

Procedure

1 Access the admin page at https://localhost/SEGconsole/.

2 Under **Targeted Logging**, select **EAS device Identifier** or **Username** and select **Add Target**.

3 Select **Enter Additional Details** and **Add Target** if you need additional information.

4 Select **Start Targeted Logging** to begin.

5 Once reproduction is complete, select **Stop Targeted Logging**.

By default, logs are written to the **Logs > EASListener** Folder.

Change the Logging Level for the SEGv2 Service

Procedure

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.

Change the Logging Level for the Email Notification Service

Procedure

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.

Change the Logging Level for the Content Gateway

Procedure

1 Access the logback.xml file contained in the Content Gateway Config folder.

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.

Change the Logging Level for the Unified Access Gateway Service

Procedure

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

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

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.

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

Change the Logging Level for Remote File Storage

Procedure

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

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

3 Edit 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.

4 Save changes and restart each service.

Change the Logging Level for the Content Rendering Engine

Procedure

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.

4 Restart each service after saving changes.

Change the Logging Level for the VMware Identity Connector

Procedure

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.

Data Aggregator

The data aggregator command line client runs a predefined SQL query that collects logs from multiple sources, compresses the logs into a ZIP file, and copies the ZIP file to a location of your choosing. This service streamlines the task of troubleshooting which results in less round trip time.

The command line client runs on demand and must be installed on each server from which logs are to be collected. You have the option to define which server(s) the SQL query runs on. You define the target location for the zipped log file.

The data aggregator service can collect logs from the following sources.

- IIS logs

- HTPERR logs
- AirWatch logs
- Predefined SQL queries
- Windows Event logs

To use the data aggregator command line client:

- Install the Data Aggregator on Your Servers
- Implement the Templates for Data Aggregator

Install the Data Aggregator on Your Servers

You must install the data aggregator on each server you intend to collect logs from.

Procedure

1. Run the DataAggregatorServiceClient.exe file on the server.
2. When prompted, select the target location into which the service copies the completed ZIP file.

The installer creates a “config” folder relative to where the service is installed. This folder contains the request XML files for both logs and SQL queries. For more information, see Templates for Data Aggregator.

Templates for Data Aggregator

The following are sample templates in XML format for logs and SQL queries. You can customize this XML content to fit your needs.

XML for Logs

This sample XML code defines each log you want to include in the ZIP file.

```
<DataAggregatorLogs>    <Logs>        <Log name="AirWatch Logs" location="C:\AirWatch\Logs"
specificFile=""/>        <Log name="HTTPERR Logs" location="C:\Windows\System32\LogFiles\HTTPERR"
specificFile=""/>        <Log name="AirWatch Event Logs" location="C:\Windows\Sysnative\winevt\Logs"
specificFile="AirWatch.evtx"/>    </Logs></DataAggregatorLogs>
```

XML for SQL Queries

This sample SQL query defines the tables to be included in the log files. Replace the QueryVariables element with your values when prompted by the client application.

```
<DataAggregatorSqlQueries>
    <Applications>
        <QueryVariables>
            <Variable name="@DeviceId" type = "INT" value = ""/>
        </QueryVariables>
        <SqlQueries>
            <SqlQuery>
                <Name>System sample</Name>
                <Query>
                    select * from interrogator.interrogatorsystemsample (nolock)
                    where deviceid = @DeviceId order by SampleTime desc
                </Query>
            </SqlQuery>
            <SqlQuery>
                <Name>Security info sample</Name>
                <Query>
                    select * from interrogator.SecurityInformationSample (nolock)
                    where deviceid = @DeviceId
                </Query>
            </SqlQuery>
            <SqlQuery>
                <Name>Certificate sample</Name>
                <Query>
                    select * from interrogator.CertificateListItem (nolock)
                    where DeviceId = @DeviceId
                </Query>
            </SqlQuery>
            <SqlQuery>
                <Name>Compliance Log</Name>
                <Query>
                    select * from interrogator.ComplianceLog (nolock)
                    where DeviceId = @DeviceId
                </Query>
            </SqlQuery>
            <SqlQuery>
                <Name>Disk encryption sample</Name>
                <Query>
                    select * from interrogator.DiskEncryptionSample (nolock)
                    where DeviceId = @DeviceId
                </Query>
            </SqlQuery>
            <SqlQuery>
                <Name>Hashtable</Name>
                <Query>
                    select * from interrogator.Hashtable (nolock)
                    where deviceid = @DeviceId
                </Query>
            </SqlQuery>
            <SqlQuery>
                <Name>Cell Info Sample</Name>
                <Query>
                    select * from interrogator.InterrogatorCellInformationSample (nolock)
                    where deviceid = @DeviceId
                </Query>
            </SqlQuery>
            <SqlQuery>
                <Name>Profile list sample</Name>
                <Query>
                    select * from interrogator.ProfileListSample (nolock)
                    where deviceid = @DeviceId
                </Query>
            </SqlQuery>
```

```
            <SqlQuery>
                <Name>Scheduler</Name>
                <Query>
                    select * from interrogator.Scheduler (nolock)
                    where DeviceId = @DeviceId
                </Query>
            </SqlQuery>
        </SqlQueries>
    </Applications>
</DataAggregatorSqlQueries>
```

Capture Logs

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

Procedure

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.

   Changing the filename ensures that the log is not overwritten.

   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.

   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.

Logging Examples

The following table provides examples of the verbose logging that you can gather to troubleshoot an issue. These logs are AirWatch-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.

Example	Log Files
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).
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 & Classic SEG)	AW.Meg.Queue.Service.log (DS), AW.EAS.Web.Listener.log, AW.EAS.Web.log, and AW.EAS.Integrationservice.log
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.

Example	Log Files
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.
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
App Wrapping errors	AppWrap.log.