FORTINET
High Performance Network Security

Fortinet Audit Event Logging

FortiWLC

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Table of Contents

Change Log 3
About this Document 4
Audit Events 5

Change Log

Date	Change Description
2021-05-06	Document release version.

About this Document

This document describes some common audit log events generated by FortiWLC.

Audit Events

Event	Description	Action

The following system message is displayed.
`#Remote Side sent disconnect message type 2 (protocol error); " Too many authentication failures"`
 	
Syslog messages for GUI access with incorrect password.
`Admin Login Failure Critical An admin user admin from client <10.32.12.13> failed login 1 times.`
`Admin Login Failure Critical An admin user admin from client <10.32.12.13> failed login 2 times.`
`Admin Login Failure Critical An admin user admin from client <10.32.12.13> failed login 3 times`
`Admin Login Failure Critical An admin user admin from client <10.32.12.13> failed login 4 times.`
`Admin Login Failure Critical An admin user admin from client <10.32.12.13> failed login 5 times.`
	Failure to establish an SSH session due to an incorrect password and exceeding the maximum limit of 6 retries.	**Information**

`#Certificate Error Information SSL certificate revoke installation failed [verify_ocsp_revoke_status: new_cert_19061.cer cert is revoked; verified with ocsp uri http://10.33.x.x:8090].`
 	
`#Certificate Installed Information A SSL certificate expired has been installed`
	Failure to establish an HTTPS session.
	• Uploading a revoked certificate for web server application.
	• Uploading an expired certificate.	

`#OpenVPNclient: Identifier is not matching: wlmfips.appsqa.com but actual one:/CN=aneesh1/ST=kar/C=in/O=qa/OU=qa`
 	
`.#Certificate Error Information SSL certificate revoke installation failed [verify_ocsp_revoke_status: new_cert_19061.cer cert is revoked; verified with ocsp uri http://10.x.x.x:8090].`
	Failure to establish a TLS session.
	• Installing a revoked certificate for a web server application.	

#Certificate Installed Information A SSL certificate expired has been installed #Certificate Error Information SSL certificate wlccert installation failed [The trusted root CA certificate is not installed completely or installed partially.]	• Uploading an expired certificate on the controller for a web application. • Uploading a certificate on controller whose CA is not known(path not trusted).	
Syslog messages for successful HTTPS login with time & IP address of client. #Login for admin success. #Controller Access User admin@10.x.x.13 login to controller at time Mon May 10 14:09:05 2021 is OK **GUI messages when admin logs out**. This Operation logs you out , Are you sure you wish to continue ? #You have Successfully Logged Out!!	Identification and authentication mechanism usage. • Syslog messages for successful HTTPS login with user & IP address details. • Syslog messages for HTTPS logout with user & IP address details.	**Information**
#Authentication failed local-admin < > does not exist #Controller Access User @10.x.x.13 login to controller at time Mon May 10 13:31:51 2021 is FAILED	Failure to establish an HTTPS session due to an incorrect password.	**Information**
Uploading a certificate with unknown CA	Unsuccessful attempt to	

#Certificate Error Information SSL certificate wlccert installation failed [The trusted root CA certificate is not installed completely or installed partially.] **Uploading a revoked certificate** #Certificate Error Information SSL certificate revoke installation failed [verify_ocsp_revoke_status: new_cert_19061.cer cert is revoked; verified with ocsp uri http://10.x.x.16:8090]. **Valid CA certificate import** [IMPORT:CertificateManagement-CA], Trusted Root certificate cayash imported successfully.	validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store, for example, uploading a certificate on controller whose CA is not known (path not trusted).	
#Upgrade is invoked #Upgrade Controller from:8.5-2build-5 to:8.5-3fips-7. #upgrade completed	Attempt to initiate a manual upgrade.	
Controller Access User admin@10.32.12.13 login to controller at time Tue May 11 12:45:04 2021 is OK **Syslog message for configuring session inactivity timeouts.** #Configured WebGUI User Idle Timeout (min) to 5 minute(s). #Configured lock time 5 second(s) **Syslog message for admin after 5 minutes of inactivity.** #Session Closed due to Idle Timeout(in Min) :5 #User admin got logged out at 05/10/2021 15:00:01 Login for admin success and unlock timeout reached after failure:0 **Syslog messages** #Configured ssh server rekey data limit to 2028 MB #Configured ssh server rekey timeout to 15 minute(s)	All management activities of TSF data. • Administer the TOE locally and remotely. • Configure the access banner. • Configure the session inactivity time before session termination or locking. • Update the TOE and to verify the updates, messages captured for upgrades initiated &	Informatio n

Syslog messages for controller upgrade. #Upgrade is invoked #Upgrade Controller from:8.5-2build-5 to:8.5-3fips-7 #upgrade completed #Auth User deny count set to 2 #Login for admin failed deny count:2 and current failure count:1 #[MODIFY:Location Services Configuration], Enable/Disable:Disable->Enable. #[MODIFY:System Time Zone] The time zone is set to Asia/Calcutta #[IMPORT:CertificateManagement-Server], wlccert , Certificate Imported successfully. #[IMPORT:CertificateManagement-CA], Trusted Root certificate cayash imported successfully.	started. • Configure the authentication failure parameters. • Start and stop services. • Configure thresholds for SSH rekeying. • Configure the reference identifier for the peer. • Set the time which is used for time-stamps. • Import X.509v3 certificates to the TOE's trust store.	
Syslog messages for successful upgrade 1.#Upgrade is invoked #Upgrade Controller from:8.5-2build-5 to:8.5-3fips-7. #upgrade completed. **Syslog messages for Auto AP upgrade failure** [AP 19] Auto Upgrade from:8.5-2build-5 to:8.5-3fips-7. [AP 19] Upgrade Request Failed.	Initiation and result of an upgrade.	
Syslog message for configuring the time zone #[MODIFY:System Time Zone] The time zone is set to Asia/Calcutta	Discontinuous changes to time by the administrator or through an automated process.	**Information**
GUI messages #Configured WebGUI User Idle Timeout (min) to	The termination of a local session	

5 minute(s). #Session Closed due to Idle Timeout(in Min) :5. #Configured lock time 5 second(s)	by the session locking mechanism.	
GUI messages #Configured WebGUI User Idle Timeout (min) to 5 minute(s). #User admin got logged out at 05/11/2021 12:17:04 #Session Closed due to Idle Timeout(in Min) :5.	The termination of a remote session by the session locking mechanism.	
GUI message #This Operation logs you out , Are you sure you wish to continue ? #You have Successfully Logged Out!!	The termination of an interactive session, for example, an admin terminating active GUI/CLI session.	
Syslog messages #Local [10.x.90.5]:0 -> Remote [10.36.x.x]:514 - VERIFY ERROR: depth=1, error=self signed certificate in certificate chain: /C=IN/ST=Karnataka/L=Bangalore/O=Google/OU=Google Auth.0 CA/CN=auth0.google.com. Local [10.x.x.5]:0 -> Remote [10.36.x.x]:514 - error Local [10.33.x.x]:0 -> Remote [10.36.x.x]:514 - fatal - unknown CA. Local [10.x.x.5]:0 -> Remote [10.36.202.x]:514 - connect failed	Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel.	
Successful HTTPS Login #Login for admin success. #Controller Access User admin@10.x.x.13 login to controller at time Mon May 10 14:09:05 2021 is OK	Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path	

Uploading a revoked certificate `#Certificate Error Information SSL certificate revoke installation failed [verify_ocsp_revoke_status: new_cert_19061.cer cert is revoked; verified with ocsp uri http://10.x.x.16:8090].`	functions.	