Technical white paper



HP Security Event Logging Messages

For Interfacing with Security Information and Event Management Systems

Table of Contents

Introduction 4

Supported printers 4

Configure and enable logging 4

Understanding Syslog messages 5

Enhanced security event log message components 5

Syslog severity levels 6

Common message variables 7

Security Event Log 8

Export the Security Event Log 8

Enhanced security event log messages 9

Security logging 9

System time 10

User authentication 11

LDAP connection 15

HP Sure Start 15

Whitelisting 16

HP Memory Shield™ 16

Intrusion Detection 17

HP Connection Inspector 19

Secure erase 24

IPsec 25

SNMPv3 decryption 32

Job completion 32

Back up and restore 45

Network status 46

FIPS-140 compliance 46

Event log 46

Device configuration 47

Basic event log messages 120

Basic event log message components 120

Introduction

This document outlines the syslog messages generated for auditable events by HP Enterprise printers and scanners running HP FutureSmart firmware versions 5.8 and newer. These messages are essential for tracking device activities for security and compliance purposes.

Supported printers

This document describes both basic event logging and enhanced security event logging implementations on HP Enterprise printers and scanners running HP FutureSmart firmware version 5.8 and newer. As a living document, it will be updated to include future HP FutureSmart firmware versions (5.8 and newer).

Configure and enable logging

This section outlines the steps required to configure and enable logging. All of these steps are carried out through the Embedded Web Server (EWS), which provides a user-friendly interface for managing the device settings. By following these instructions, you will be able to ensure that logging is properly set up to capture relevant events for monitoring and security purposes.

1. Open the EWS.
    a. Open a Web browser.
    b. In the **Address** or **Go to** field, type the IP address that is assigned to the device (for example; http://192.168.1.1) or the host name (for example; http://www.[your_server].com).

        NOTE: If you do not know the IP address or hostname for the device, you can view this information at the product control panel. To view the IP address and hostname of the device at the product control panel, touch the **Information** button, then select **Ethernet**.
2. Configure the syslog facility.
    a. Select the **Networking** tab.
    b. Select the **Other Settings** menu.
    c. Select **Misc. Settings** tab.
    d. From the **Syslog Facility** drop-down menu, select the syslog facility used by the syslog server to classify syslog messages from the device.

        NOTE: The default syslog facility is LPR.
    e. Click **Apply**.
3. Configure the syslog server and enable logging.
    a. Select the **TCP/IP Settings** menu.
    b. Click the **Advanced** tab.

c. In the Syslog Server field, enter the IPv4 address, hostname, or Fully Qualified Domain Name (FQDN) of the syslog server.

   NOTE: Basic event logging is enabled when the syslog server is set.

d. From the **Syslog Protocol** drop-down menu, select the transport protocol used by the syslog server for receiving syslog messages.

e. In the **Syslog Port** field, enter the port number of the port used by the syslog server for receiving syslog messages.

f. Optionally, in the **Syslog Maximum Messages** field, enter the maximum number of syslog messages the device should process per minute.

   NOTE: It is highly recommended that **Syslog Maximum Messages** be set to 1000 to help prevent syslog messages from getting discarded by the device during periods in which a large number of syslog messages are generated in a short amount of time.

g. Optionally, in the **Syslog Priority** field, type 7 to ensure syslog messages for all auditable events are forwarded to the syslog server.

4. Select the checkbox to enable **Enhanced security event logging**.
5. Click **Apply**.

Understanding Syslog messages

HP printers and scanners include both basic and enhanced security event log messages with varying formats.

NOTE: For basic event log message components, see the chapter on *Basic Event Log Messages*.

Enhanced security event log message components

Enhanced security event log messages are displayed in the following format:

<priority value> <device type>: <event summary>; <event details>

Example of a raw syslog message:

<54> printer: Device Administrator Password modified; time="2025-Feb-09 11:54 AM (UTC-07:00)" user="LOCAL\administrator" source_IP="10.0.0.7" hostname="testlab01" outcome=success

The enhanced security event log message format includes the following components:

Table 1 Enhanced security event logging message components

Components	Description
<priority value>	Syslog Priority, which is calculated based on the Syslog Facility and Syslog Severity. Syslog Priority = Syslog Facility (0-23) x 8 + Syslog Severity (0-7).
<device type>	Type of device that generated the syslog message.
:	Separates <device type> from the remaining parts of the message.
<event summary>	Summary of the event.
;	Separates <event summary> from the remaining parts of the message.
<event details>	Details of the event. Event details consist of key-value pairs, with each pair separated by a single space.

Syslog severity levels

Each security event log message generated by a device is categorized with a severity level that reflects the importance or urgency of the event. The severity levels used are based on the definitions in RFC 5424 and help in accurately assessing and responding to the nature of the security event.

Table 2 Syslog severity levels

Level	Severity	Description
0	Emergency	System is unusable.
1	Alert	Action must be taken immediately.
2	Critical	Critical conditions.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notice	Normal but significant condition.
6	Informational	Informational messages.
7	Debug	Debug-level messages.

Common message variables

Basic event log and enhanced security event log messages share the following common variables:

Table 3 Common variables in both Basic event logging and Enhanced security event logging messages

Common variable	Description
<device type>	Type of device that generated the syslog message. Possible values are: • printer • scanner
<timestamp>	Date and time of the event. The format of <timestamp> is as follows: • YYYY-MMM-DD HH:MM PE (UTCTZD) Where: • YYYY = four-digit year • MMM = three-letter abbreviation of the month • DD = two-digit day of the month • HH = two-digit hour (00 through 12) • MM = two-digit minute (00 through 59) • PE = two-letter of the 12-hour period (AM or PM) • TZD = UTC offset (+HH:MM or -HH:MM) Example: 2025-Feb-13 09:10 AM (UTC -07:00)
<user>	The authenticated entity associated with the event, if applicable. Example: 10.0.0.3\user1
<client computer IP address>	The IP address of the client computer associated with the generated event. Example (IPv4): 10.0.0.28 Example (IPv6): fdb9:1caf:4150:1:ca5a:cfff:fe85:8d21
<client computer hostname>	The hostname of the client computer associated with the generated event. Example: winsrv.testlab.local
<local device IP address>	The IP address of the local device (printer/scanner) associated with the generated event.
<local device hostname>	The hostname of the local device (printer/scanner) associated with the generated event.
<sign-in method>	The sign-in method associated with the generated event. Possible values are: • local_device • windows • ldap • smartcard • *other supported authenticated agents*
<interface>	The interface associated with the generated event. Possible values are: • Wired • AP • STA

Security Event Log

In addition to forwarding both basic event log messages and enhanced security event log messages to an external syslog server, the device stores the enhanced security event log messages in an internal log file known as the Security Event Log. This log file is designed to hold up to 2,500 audit records. After the log reaches its capacity, the device automatically overwrites the oldest records with the newest ones, ensuring that the most recent security events are always captured.

Enhanced security event logging messages are always stored in the Security Event Log, regardless of the syslog settings configured on the device.

The internal log file can be exported via the Embedded Web Server, allowing for convenient access and transfer of log data for further analysis or archiving.

Example syslog message from the Security Event Log:

{"key":6,"time":"2025-02-14T19:03:29.155Z","timestamp":"133840334091553930","priority":6,"firmwareVersion":"2503213_016702","bootCycle":2,"syslogMessage":"Device Administrator Password modified; time=\"2025-Feb-14 07:03 PM (UTC+00:00)\" user=\"LOCAL\\administrator\" source_IP=\"15.4.61.146\" outcome=success"}

Table 4 Security Event Log - Message components

Item	Description
{ }	Brackets used to separate log messages in the Security Event Log.
“key”:	A numerical value representing the identifier for the log message.
"time":	The system file time (in UTC) the log message was written to the Security Event Log.
"timestamp":	Number of 100-nanosecond intervals since the epoch.
"priority":	The priority associated with the log message.
"firmwareVersion":	The firmware version the device was running when the event was generated.
"bootCycle":	A numerical value representing the boot cycle of the device.
"syslogMessage":	The enhaced security event log message string.

Export the Security Event Log

1. Open a Web browser.
2. Sign into the EWS as an administrative user or a user who has permission to access the **Security Event Log**.
3. Click the **Security** tab.
4. Select the **Security Log** menu.
5. Under the **Retrieve Security Event Log** section, click **Export**.
6. Choose a location to save the exported Security Event Log and click **Save**.

Enhanced security event log messages

This chapter describes the enhanced security event log messages, organized by functionality. The following details are provided for each message:

Table 5 Enhanced security event log message details

Item	Description
Message	The message string excluding the syslog priority, along with any variables embedded in the message.
Interface(s)	The interface(s) for events triggered by entities external to the device, if applicable.
Description	A brief explanation of the event for the message.
Syslog severity	The syslog severity level associated with the message.

Security logging

Jetdirect logging

Message: <device type>: Jetdirect logging started; time="<timestamp>" outcome=success

Interface (s): N/A

Description: Jetdirect logging was started. This message is generated during system initialization if the syslog server address is set, and enhanced security event logging is enabled.

Syslog severity: Notice

Enhanced security event logging

Message: <device type>: CCC logging started; time="<timestamp>" outcome=success

Interface (s): N/A

Description: Enhanced security event logging was started. This message is generated during system initialization if enhanced security event logging is enabled.

Syslog severity: Notice

System time

Date and time modification

Message: <device type>: System time changed; time="<timestamp>" value="<new date/time>" old_value="<old date/time>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, SNMPv3

Description: The system time was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user modified the system time via the EWS, the user key-value pair is not contained within the message.

Message: <device type>: System time changed; time="<timestamp>" value="<new date/time>" old_value="<old date/time>" user="<user>" outcome=success

Interface (s): Control Panel

Description: The system time was modified.

Syslog severity: Informational

Message: <device type>: System time changed; time="<timestamp>" value="<new date/time>" old_value="<old date/time>" source_IP="<NTS IP Address>" outcome=success

Interface (s): NTP

Description: The system time was modified by the NTP server.

Syslog severity: Informational

Network Time Server synchronization

Message: <device type>: System time synchronization with Network Time Server; time="<timestamp>" nts_addr="<NTP Server IP address or FQDN>" reason_for_failure=<failure> outcome=failure

Interface (s): NTP

Description: Time synchronization with the Network Time Server failed.

Syslog severity: Warning

Variable (s): <failure> - The cause of the Network Time Server synchronization error. Possible values are:

- NTP_UnknownFailure
- NTP_Timeout
- NTP_TimeFormat
- NTP_InternalFailure

User authentication

Sign in

EWS

Message: <device type>: EWS Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A user successfully signed in to the device via the EWS.

Syslog severity: Informational

Message: <device type>: EWS Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: A user attempted and failed to sign in to the device via the EWS.

Syslog severity: Warning

Control panel

Message: <device type>: Control Panel Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" outcome=success

Interface (s): Control Panel

Description: A user successfully signed in to the device at the control panel.

Syslog severity: Informational

Message: <device type>: Control Panel Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" outcome=failure

Interface (s): Control Panel

Description: A user attempted and failed to sign in to the device at the control panel.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Web Services (WS)

Message: <device type>: WS Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): Web Services, OXPd, REST

Description: HTTP Basic authentication failed. This message is generated when HTTP Basic authentication of an HTTP request containing a Web Service message fails.

Syslog severity: Warning

SNMPv3

Message: <device type>: SNMPv3 authentication failed; time="<timestamp>" user="SNMPv3\<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure interface=<interface>

Interface (s): SNMPv3

Description: Authentication of a received SNMPv3 packet failed.

Syslog severity: Warning

Telnet

Message: <device type>: Telnet Sign In Authentication; time="<timestamp>" user="Administrator" source_IP="<client computer IP address>" hostname="<client computer host name>" outcome=failure interface=<interface>

Interface (s): Telnet

Description: A user attempted and failed to sign in to the device via Telnet.

Syslog severity: Warning

Remote control-panel

Message: <device type>: Login; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: An EWS user successfully logged into the Remote Control-Panel.

Syslog severity: Informational

Message: <device type>: Login; time="<timestamp>" reason=<reason for failure> user="<user>" source_IP="<client computer IP address> hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: An EWS user attempted and failed to sign in to the Remote Control-Panel.

Syslog severity: Warning

Remote App

Message: <device type>: Remote App Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" outcome=success

Interface (s): N/A

Description: A user successfully signed in to a Remote Application.

Syslog severity: Informational

Sign out

Control panel

Message: <device type>: Control Panel session terminated; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: The control panel user's sign-in session was ended. This message is generated when either the control panel user ends their sign-in session by signing out or the device ends the control panel user's sign-in session due to control panel inactivity.

Syslog severity: Informational

EWS

Message: <device type>: EWS session terminated; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The EWS user's sign-in session was ended. This message is generated when the EWS user ends their sign-in session by signing out.

Syslog severity: Informational

Remote control-panel

Message: <device type>: Logout; time="<timestamp>" reason=<reason> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A user's session to the Remote Control-Panel was ended.

Syslog severity: Informational

Variable (s): <reason> - The reason the user was logged out of the Remote Control-Panel. Possible values are:

- EndedByUser
- EndedByDevice

Remote App

Message: <device type>: Remote App session terminated; time="<timestamp>" user="<user>" outcome=success

Interface (s): N/A

Description: The Remote Application user's sign-in session was ended.

Syslog severity: Informational

Account lockout

Device administrator account

Message: <device type>: Account Entered Lockout Mode; time="<timestamp>" account="Administrator" outcome=success

Interface (s): EWS, Web Services, Control Panel, Telnet

Description: The device administrator account was locked.

Syslog severity: Informational

Message: <device type>: Account Exited Lockout Mode; time="<timestamp>" account="Administrator" outcome=success

Interface (s): N/A

Description: The device administrator account was unlocked.

Syslog severity: Informational

Remote configuration account

Message: <device type>: Account Entered Lockout Mode; time="<timestamp>" account="Administrator" outcome=success

Interface (s): Web Services

Description: The remote configuration account was locked.

Syslog severity: Informational

NOTE: Though the message generated contains the account "Administrator," the account that was locked is the remote configuration account.

Message: <device type>: Account Exited Lockout Mode; time="<timestamp>" account="Administrator" outcome=success

Interface (s): N/A

Description: The remote configuration account was unlocked.

Syslog severity: Informational

NOTE: Though the message generated contains the account “Administrator,” the account that was unlocked is the remote configuration account.

SNMPv3 user account

Message: <device type>: SNMPv3 authentication entered protected mode; time="<timestamp>" SNMPv3_user_account="<SNMPv3 account username>" outcome=successinterface=<interface>

Interface (s): SNMPv3

Description: An SNMPv3 user account was locked.

Syslog severity: Warning

Message: <device type>: SNMPv3 authentication exited protected mode; time="<timestamp>" SNMPv3_user_account="<SNMPv3 account username>" outcome=successinterface=<interface>

Interface (s): N/A

Description: An SNMPv3 user account was unlocked.

Syslog severity: Warning

LDAP connection

Message: <device type>: LDAP resolved to: "<Last LDAP IP Address>" which failed to connect; time=<timestamp> outcome=failure

Interface (s): N/A

Description: An attempt to connect to an LDAP server failed after DNS resolution was successful.

Syslog severity: Warning

HP Sure Start

Message: <device type>: Boot code corrupt; time=<timestamp>

Interface (s): N/A

Description: The device detected and recovered from a corrupted/tampered version of BIOS.

Syslog severity: Alert

Message: <device type>: Upgrade Corrupt; time=<timestamp>

Interface (s): N/A

Description: Cryptographic validation of newly downloaded firmware failed.

Syslog severity: Alert

Messages: <device type>: Invalid Boot Attempt; time="<timestamp>"

<device type>: Downgrade Attempt; time="<timestamp>"

Interface (s): N/A

Description: A downgrade to firmware that doesn't contain the SureStart feature was attempted.

Syslog severity: Alert

Message: <device type>: Unproven Installer; time=<timestamp>

Interface (s): N/A

Description: The newly downloaded firmware failed to cryptographically validate the BIOS code.

Syslog severity: Alert

Whitelisting

Message: <device type>: Code sign error; time="<timestamp>" source_IP="<local device IP address>"

Interface (s): N/A

Description: Validation of a system firmware file during the load process using digital signature failed.

Syslog severity: Alert

NOTE: The "source_IP" key-value pair may not be included in the message above depending on which HP product generated the message.

HP Memory Shield™

Message: <device type>: Memory Shield detected an intrusion. Control-Flow Integrity Incident, Memory Protection; time="<timestamp>"

Interface (s): N/A

Description: Memory Shield detected a control-flow integrity incident.

Syslog severity: Alert

Message: <device type>: Memory Shield detected an intrusion. Whitelisting incident, Prevented Script; time="<timestamp>"

Interface (s): N/A

Description: Memory Shield detected a whitelisting incident, preventing a script.

Syslog severity: Alert

Message: <device type>: Memory Shield detected an intrusion. Whitelisting incident, Prevented Executable; time="<timestamp>"

Interface (s): N/A

Description: Memory Shield detected a whitelisting incident, preventing an executable.

Syslog severity: Alert

Message: <device type>: Memory Shield detected an intrusion. Whitelisting incident, Prevented loading Kernel Module; time="<timestamp>"

Interface (s): N/A

Description: Memory Shield detected a whitelisting incident, preventing loading the Kernel Module.

Syslog severity: Alert

Message: <device type>: Memory Shield detected an intrusion. Unauthorized Policy load; time="<timestamp>"

Interface (s): N/A

Description: Memory Shield detected an unauthorized policy load.

Syslog severity: Alert

Message: <device type>: Memory Shield detected an intrusion. Undecoded intrusion type; time="<timestamp>"

Interface (s): N/A

Description: Memory Shield detected an intrusion.

Syslog severity: Alert

Intrusion Detection

Message: <device type>: <device type>: Potential intrusion. Memory corruption detected.; time=<timestamp> source_IP="<local device IP address>

Interface (s): N/A

Description: Memory corruption was detected.

Syslog severity: Alert

Message: <device type>: Intrusion detection disabled. Unable to scan for memory corruption.; time=<timestamp> source_IP="<local device IP address>

Interface (s): N/A

Description: The intrusion detection algorithm was disabled.

Syslog severity: Alert

Message: <device type>: Failed to initialize intrusion detection.; time=<timestamp> source_IP="<local device IP address>

Interface (s): N/A

Description: Initialization of the intrusion detection functionality failed.

Syslog severity: Alert

Message: <device type>: System resource error.; time=<timestamp> source_IP="<local device IP address>

Interface (s): N/A

Description: System resource error.

Syslog severity: Alert

Message: <device type>: Detection thread detected an intrusion. Hash Intrusion; time=<timestamp>

Interface (s): N/A

Description: Intrusion detection functionality detected a hash intrusion.

Syslog severity: Alert

Message: <device type>: Detection thread detected an intrusion. Page Table Walk Intrusion; time=<timestamp>

Interface (s): N/A

Description: Intrusion detection functionality detected a Page Table Walk intrusion.

Syslog severity: Alert

Message: <device type>: Detection thread detected an intrusion. TCR EL1 Intrusion; time=<timestamp>

Interface (s): N/A

Description: Intrusion detection functionality detected a TCR EL1 intrusion.

Syslog severity: Alert

Message: <device type>: Detection thread detected an intrusion. Snapshot timeout Intrusion; time=<timestamp>

Interface (s): N/A

Description: Intrusion detection functionality detected a snapshot timeout intrusion.

Syslog severity: Alert

Message: <device type>: Potential intrusion. Android disk (DMVerity) corruption detected.; time=<timestamp>

Interface (s): N/A

Description: Intrusion detection functionality detected an Android disk corruption.

Syslog severity: Alert

HP Connection Inspector

Message: <device type>: Potential intrusion. HP Connection Inspector event detected.; time="<timestamp>" source_IP="<local device IP address>"

Interface (s): N/A

Description: HP Connection Inspector detected a potential intrusion.

Syslog severity: Error

Message: <device type>: HP Connection Inspector event; time="<timestamp>" event=protected_mode_entered outcome=success

Interface (s): N/A

Description: HP Connection Inspector feature has entered protected mode.

Syslog severity: Warning

Message: <device type>: HP Connection Inspector event; time="<timestamp>" event=protected_mode_exited outcome=success

Interface (s): N/A

Description: HP Connection Inspector feature has exited protected mode.

Syslog severity: Warning

Message: <device type>: HP Connection Inspector event; time="<timestamp>" event=dns_query value="<host name>" outcome=failure

Interface (s): N/A

Description: HP Connection Inspector feature has detected DNS query failure for a hostname.

Syslog severity: Warning

Variable (s): <host name> - Host name whose DNS lookup failed.

Message: <device type>: HP Connection Inspector event; time="<timestamp>" event=dns_query value="<host name>" outcome=success

Interface (s): N/A

Description: HP Connection Inspector feature has performed a successful DNS query for a hostname.

Syslog severity: Warning

Variable (s): <host name> - Host name whose DNS lookup succeeded.

Message: <device type>: HP Connection Inspector event; time="<timestamp>" event=android_dns_query value="<host name>" outcome=failure

Interface (s): N/A

Description: HP Connection Inspector feature has detected an Android DNS query failure for a hostname.

Syslog severity: Warning

Variable (s): <host name> - Host name whose Android DNS lookup failed.

NOTE: This message applies only to devices that support HP Workpath functionality.

Message: <device type>: HP Connection Inspector event; time="<timestamp>" event=android_dns_query value="<host name>" outcome=success

Interface (s): N/A

Description: HP Connection Inspector feature has performed a successful Android DNS query for a hostname.

Syslog severity: Warning

Variable (s): <host name> - Host name whose Android DNS lookup succeeded.

NOTE:This message applies only to devices that support HP Workpath functionality.

Self-tests

PJL password verification

Message: <device type>: PJL Password Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The PJL password verification test was performed and was successful.

Syslog severity: Informational

Message: <device type>: PJL Password Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The PJL password verification test was performed and failed.

Syslog severity: Warning

Timestamp verification

Message: <device type>: Timestamp Verification Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The Timestamp verification test was performed and was successful.

Syslog severity: Informational

Message: <device type>: Timestamp Verification Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The Timestamp verification test was performed and failed.

Syslog severity: Warning

Device user access code verification

Message: <device type>: Device User Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The Device User Access Code verification test was performed and was successful.

Syslog severity: Informational

Message: <device type>: Device User Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The Device User Access Code verification test was performed and failed.

Syslog severity: Warning

LDAP settings verification

Message: <device type>: LDAP Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The LDAP Settings verification test was performed and was successful.

Syslog severity: Informational

Message: <device type>: LDAP Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The LDAP Settings verification test was performed and failed.

Syslog severity: Warning

Windows settings verification

Message: <device type>: Windows Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The Windows Settings verification test was performed and was successful.

Syslog severity: Informational

Message: <device type>: Windows Integrity Test; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The Windows Settings verification test was performed and failed.

Syslog severity: Warning

Data integrity test

Message: <device type>: Generated hash for Data Integrity Check; time="<timestamp>" reference_point="<reference point data>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A reference point for the data integrity test was succesfully set.

Syslog severity: Informational

Variable (s): <reference point data> - The value of this varilable includes the date and time the reference point was set along with the hash.

Message: <device type>: Generated hash for Data Integrity Check; time="<timestamp>" reference_point="<null>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: A reference point for the data integrity test failed to be set.

Syslog severity: Warning

Message: <device type>: Verify hash for Data Integrity Check; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The data integrity test was performed and was successful.

Syslog severity: Informational

Message: <device type>: Verify hash for Data Integrity Check; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The data integrity test was performed and failed.

Syslog severity: Warning

Code integrity test

Message: <device type>: Generate hash for Code Integrity Check; time="<timestamp>" reference_point="<reference point data>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A reference point for the code integrity test was succesfully set.

Syslog severity: Informational

Variable (s): <reference point data> - The value of this varilable includes the date and time the reference point was set along with the hash.

Message: <device type>: Generate hash for Code Integrity Check; time="<timestamp>" reference_point="<null>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: A reference point for the code integrity test failed to be set.

Syslog severity: Warning

Message: <device type>: Verify hash for Code Integrity Check; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The code integrity test was performed and was successful.

Syslog severity: Informational

Message: <device type>: Verify hash for Code Integrity Check; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The code integrity test was performed and failed.

Syslog severity: Warning

Secure erase

Erase drive

Message: <device type>: Erase Drive requested; time="<timestamp>" erase_mode=<erase mode> drive_name="<drive name>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A request to erase a storage drive was made.

Syslog severity: Informational

Variable (s): <erase mode> - Erase mode used to erase the storage drive. Possible values are:

- secure_cryptographic_erase
- unknown

Message: <device type>: Erase Drive completion; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A drive has successfully been erased.

Syslog severity: Informational

Erase job data

Message: <device type>: Erase Job Data requested; time="<timestamp>" erase_mode=<erase mode> source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A request to erase the job data on all storage drives installed on the device was made.

Syslog severity: Informational

Variable (s): <erase mode> - Erase mode used to erase the job data. Possible values are:

- non_secure_fast_erase
- Non-Secure_Fast_Erase_(No_overwrite)
- secure_fast_erase
- Secure_Fast_Erase_(Overwrite_1_time)
- secure_sanitize_erase
- Secure_Sanitize_Erase_(Overwrite_3_times)
- secure_cryptographic_erase

IPsec

The following table lists the <reason for failure> variable possible values contained within messages generated for unsuccessful IKE negotiations:

Variable (s): <reason for failure> - Reason IKE negotiations failed. Possible values are:

- Certificate_was_not_found(anywhere)
- Certificate_chain_looped(did_not_find_trusted_root)
- Certificate_contains_critical_extension_that_was_not_handled
- Certificate_issuer_was_not_valid(CA_specific_Informationalrmation_missing)
- Certificate_was_not_valid_in_the_time_interval
- Certificate_is_not_valid
- Certificate_signature_was_not_verified_correctly
- Certificate_was_revoked_by_a_CRL
- Certificate_was_not_added_to_the_cache
- Certificate_decoding_failed
- Algorithm_mismatch_between_the_certificate_and_the_search_constraints
- Key_usage_mismatch_between_the_certificate_and_the_search_constraints
- CRL_is_too_old
- CRL_is_not_valid
- CRL_signature_was_not_verified_correctly
- CRL_was_not_found(anywhere)
- CRL_was_not_added_to_the_cache
- CRL_decoding_failed
- CRL_is_not_currently_valid_but_in_the_future
- CRL_contains_duplicate_serial_numbers
- Time_interval_is_not_continuous
- Time_Informationalrmation_not_available
- Database_method_failed_due_to_timeout
- Database_method_failed

- Path_was_not_verified
- Maximum_path_length_reached
- No_IPsec_rules_configured
- Peer_IP_address_mismatch
- Local_IP_address_mismatch
- CA_not_trusted
- Access_group_mismatch
- Local_Traffic_Selector_mismatch
- Remote_Traffic_Selector_mismatch
- Local_ID_mismatch
- Remote_ID_mismatch
- Lost_on_simultaneous_SA_rekey_arbitration
- IKE_version_mismatch
- Protocol_mismatch_with_NAT-T
- Algorithm_did_not_match_policy
- Unsupported_algorithm
- Authentication_method_mismatch
- Unsupported_authentication_method
- Encapsulation_mode_mismatch
- Out_of_memory
- Encryption_algorithm_mismatch
- PRF_algorithm_mismatch
- Integrity_algorithm_mismatch
- DH_group_mismatch
- Extended_Sequence_Number_mismatch
- IKE_transform_attribute_mismatch(possible_key_size_mismatch)
- ESP_NULL_NULL_proposed
- Authentication_failed:
- No_proposal_chosen:
- Timed_out
- Internal_error

IKEv1 phase 1

Message: <device type>: IPsec IKEv1 phase 1 negotiation; time="<timestamp>" authentication_option=<authentication option> item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=success

Interface (s): IPsec

Description: IKEv1 phase 1 negotiations initiated by the IPsec peer were successful.

Syslog severity: Warning

Variable (s): <authentication option> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication. Possible values are:

- Certificates
- Pre-shared_key

Message: <device type>: IPsec IKEv1 phase 1 negotiation; time="<timestamp>" item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv1 phase 1 negotiations initiated by the IPsec peer failed.

Syslog severity: Warning

Message: <device type>: IPsec IKEv1 phase 1 negotiation; time="<timestamp>" authentication_option=<authentication option> item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=success

Interface (s): IPsec

Description: IKEv1 phase 1 negotiations initiated by the local device were successful.

Syslog severity: Warning

Variable (s): <authentication option> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication. Possible values are:

- Certificates
- Pre-shared_key

Message: <device type>: IPsec IKEv1 phase 1 negotiation; time="<timestamp>" item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv1 phase 1 negotiations initiated by the local device failed.

Syslog severity: Warning

IKEv1 phase 2

Message: <device type>: IPsec IKEv1 phase 2 negotiation; time="<timestamp>" authentication_option=<authentication option> item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=success

Interface (s): IPsec

Description: IKEv1 phase 2 negotiations initiated by the IPsec peer were successful.

Syslog severity: Warning

Variable (s): <authentication option> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication. Possible values are:

- Certificates
- Pre-shared_key

Message: <device type>: IPsec IKEv1 phase 2 negotiation; time="<timestamp>" item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv1 phase 2 negotiations initiated by the IPsec peer failed.

Syslog severity: Warning

Message: <device type>: IPsec IKEv1 phase 2 negotiation; time="<timestamp>" authentication_option=<authentication option> item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=success

Interface (s): IPsec

Description: IKEv1 phase 2 negotiations initiated by the local device were successful.

Syslog severity: Warning

Variable (s): <authentication option> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication. Possible values are:

- Certificates
- Pre-shared_key

Message: <device type>: IPsec IKEv1 phase 2 negotiation; time="<timestamp>" item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv1 phase 2 negotiations initiated by the local device failed.

Syslog severity: Warning

IKEv2 phase 1

Message: <device type>: IPsec IKEv2 phase 1 negotiation; time="<timestamp>" local_authentication_option=<local authentication option> remote_authentication_option=<remote authentication option> item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=success

Interface (s): IPsec

Description: IKEv2 phase 1 negotiations initiated by the IPsec peer were successful.

Syslog severity: Warning

Variable (s): <local authentication option> - Authentication method that was used by the IPsec peer to authenticate the local device. Possible values are:

- Certificates
- Pre-shared_key

<remote authentication option> - Authentication method that was used by the local device to authenticate the IPsec peer. Possible values are:

- Certificates
- Pre-shared_key

NOTE: If both the local device and the IPsec peer used pre-shared key to perform mutual authentication, this message is not generated.

Message: <device type>: IPsec IKEv2 phase 1 negotiation; time="<timestamp>" item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv2 phase 1 negotiations initiated by the IPsec peer failed.

Syslog severity: Warning

Message: <device type>: IPsec IKEv2 phase 1 negotiation; time="<timestamp>" local_authentication_option=<local authentication option> remote_authentication_option=<remote authentication option> item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=success

Interface (s): IPsec

Description: IKEv2 phase 1 negotiations initiated by the local device were successful.

Syslog severity: Warning

Variable (s): <local authentication option> - Authentication method that was used by the local device to authenticate the IPsec peer. Possible values are:

- Certificates
- Pre-shared_key

<remote authentication option> - Authentication method that was used by the IPsec peer to authenticate the local device. Possible values are:

- Certificates
- Pre-shared_key

NOTE: If both the local device and the IPsec peer used pre-shared key to perform mutual authentication, this message is not generated.

Message: <device type>: IPsec IKEv2 phase 1 negotiation; time="<timestamp>" item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv2 phase 1 negotiations initiated by the local device failed.

Syslog severity: Warning

IKEv2 phase 2

Message: <device type>: IPsec IKEv2 phase 2 negotiation; time="<timestamp>" local_authentication_option=<local authentication option> remote_authentication_option=<remote authentication option> item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=success

Interface (s): IPsec

Description: IKEv2 phase 2 negotiations initiated by the IPsec peer were successful.

Syslog severity: Warning

Variable (s): <local authentication option> - Authentication method that was used by the IPsec peer to authenticate the local device. Possible values are:

- Certificates
- Pre-shared_key

<remote authentication option> - Authentication method that was used by the local device to authenticate the IPsec peer. Possible values are:

- Certificates
- Pre-shared_key

NOTE: If both the local device and the IPsec peer used pre-shared key to perform mutual authentication, this message is not generated.

Message: <device type>: IPsec IKEv2 phase 2 negotiation; time="<timestamp>" item=printer_role value=Responder source_IP="<IPsec peer IP address>" hostname="<IPsec peer hostname>" destination_IP="<local device IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv2 phase 2 negotiations initiated by the IPsec peer failed.

Syslog severity: Warning

Message: <device type>: IPsec IKEv2 phase 2 negotiation; time="<timestamp>" local_authentication_option=<local authentication option> remote_authentication_option=<remote authentication option> item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=success

Interface (s): IPsec

Description: IKEv2 phase 2 negotiations initiated by the local device were successful.

Syslog severity: Warning

Variable (s): <local authentication option> - Authentication method that was used by the local device to authenticate the IPsec peer. Possible values are:

- Certificates
- Pre-shared_key

<remote authentication option> - Authentication method that was used by the IPsec peer to authenticate the local device. Possible values are:

- Certificates
- Pre-shared_key

NOTE: If both the local device and the IPsec peer used pre-shared key to perform mutual authentication, this message is not generated.

Message: <device type>: IPsec IKEv2 phase 2 negotiation; time="<timestamp>" item=printer_role value=Initiator source_IP="<local device IP address>" hostname="<local device hostname>" destination_IP="<IPsec peer IP address>" outcome=failure Reason=<reason for failure>

Interface (s): IPsec

Description: IKEv2 phase 2 negotiations initiated by the local device failed.

Syslog severity: Warning

IPsec ESP

Message: <device type>: IPsec using ESP failed; time="<timestamp>" source_IP="<source IP address>" hostname="<source hostname>" destination_IP="<destination IP address>" outcome=failure

Interface (s): IPsec

Description: The processing of an IPsec ESP packet failed.

Syslog severity: Warning

IPsec AH

Message: <device type>: IPsec using AH failed; time="<timestamp>" source_IP="<source IP address>" hostname="<source hostname>" destination_IP="<destination IP address>" outcome=failure

Interface (s): IPsec

Description: The processing of an IPsec AH packet failed.

Syslog severity: Warning

IPsec ESP/AH

Message: <device type>: IPsec using ESP/AH failed; time="<timestamp>" source_IP="<source IP address>" hostname="<source hostname>" destination_IP="<destination IP address>" outcome=failure

Interface (s): IPsec

Description: The processing of an IPsec ESP or AH packet failed.

Syslog severity: Warning

SNMPv3 decryption

Message: <device type>: SNMPv3 decryption failed; time="<timestamp>" user="SNMPv3\<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure interface=<interface>

Interface (s): SNMPv3

Description: The decryption of a received SNMPv3 packet failed.

Syslog severity: Warning

Job completion

Print

Message: <device type>: Print job completion; time="<timestamp>" job_name="<job name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, SNMP, P9100, WS Print, IPP, FTP, LPD

Description: A job was successfully printed.

Syslog severity: Informational

Message: <device type>: Print job completion; time="<timestamp>" job_name="<job name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=canceled

Interface (s): EWS, Web Services, SNMP, P9100, WS Print, IPP, FTP, LPD

Description: A job that was printing was canceled.

Syslog severity: Warning

Message: <device type>: Print job completion; time="<timestamp>" job_name="<job name>" user="<user>" outcome=success

Interface (s): Control Panel

Description: A job was successfully printed.

Syslog severity: Warning

Message: <device type>: Print job completion; time="<timestamp>" job_name="<job name>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: A job that was printing was canceled.

Syslog severity: Warning

Message: <device type>: Print job completion; time="<timestamp>" job_name="" user="Guest" source_IP="0.0.0.0" outcome=success

Interface (s): Control Panel

Description: The network security report was successfully printed.

Syslog severity: Warning

Message: <device type>: Print job completion; time="<timestamp>" job_name="" user="Guest" source_IP="0.0.0.0" outcome=canceled

Interface (s): Control Panel

Description: The printing of the network security report was canceled.

Syslog severity: Warning

Message: <device type>: Print and Save to Device Memory job completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, P9100, WS Print, IPP, FTP, LPD

Description: A Proof & Hold or Quick Copy job was successfully printed and saved to device memory.

Syslog severity: Informational

Copy

Message: <device type>: Copy job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel, OXPd

Description: A copy job was completed successfully.

Syslog severity: Informational

Message: <device type>: Copy job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel, OXPd

Description: A copy job was canceled.

Syslog severity: Warning

Save to device memory

Message: <device type>: Save to Device Memory job completion; time="<timestamp>" job_type=print user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, P9100, WS Print, IPP, FTP, LPD

Description: A pin-protected or encrypted stored print job was successfully stored on the device.

Syslog severity: Informational

Message: <device type>: Save to Device Memory job completion; time="<timestamp>" job_type=copy user="<user>" outcome=success

Interface (s): Control Panel

Description: A copy job was stored.

Syslog severity: Informational

Message: <device type>: Save to Device Memory job completion; time="<timestamp>" job_type=copy user="<user>" outcome=canceled

Interface (s): Control Panel

Description: The storing of a copy job was canceled.

Syslog severity: Warning

Message: <device type>: Save to Device Memory job completion; time="<timestamp>" job_type=fax user="<user>" outcome=success

Interface (s): Analog Fax

Description: A received fax was stored.

Syslog severity: Informational

Message: <device type>: Save to Device Memory job completion; time="<timestamp>" job_type=fax user="<user>" outcome=canceled

Interface (s): Analog Fax

Description: The storing of a received fax was canceled.

Syslog severity: Warning

Retrieve from device memory

Message: <device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=<job type> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services, SNMP

Description: A stored job on the device was printed successfully.

Syslog severity: Informational

Variable (s): <job type> - Type of job. Possible values are:

- copy
- print

Message: <device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=<job type> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=canceled

Interface (s): Web Services, SNMP

Description: A stored job on the device was printed but then canceled prior to the completion of the job.

Syslog severity: Warning

Variable (s): <job type> - Type of job. Possible values are:

- copy
- print

Message: <device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=<job type> user="<user>" outcome=success

Interface (s): EWS, Web Services, Control Panel, OXPd

Description: A stored job on the device was printed successfully.

Syslog severity: Informational

Variable (s): <job type> - Type of job. Possible values are:

- copy
- print
- fax

Message: <device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=<job type> user="<user>" outcome=canceled

Interface (s): EWS, Web Services, Control Panel, OXPd

Description: A stored job on the device was printed but then canceled prior to the completion of the job.

Syslog severity: Warning

Variable (s): <job type> - Type of job. Possible values are:

- copy
- print
- fax

Scan to Email

Message: <device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: An email was sent to all recipients successfully.

Syslog severity: Informational

Message: <device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: An email was canceled.

Syslog severity: Warning

Message: <device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=partial_success

Interface (s): Control Panel

Description: An email addressed to two or more recipients was sent successfully to at least one recipient but not to all recipients.

Syslog severity: Warning

Message: <device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel

Description: The processing of an email failed.

Syslog severity: Warning

Save to SharePoint®

Message: <device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: A Save to SharePoint job was completed successfully.

Syslog severity: Informational

Message: <device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: A Save to SharePoint job was canceled.

Syslog severity: Warning

Message: <device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=partial_success

Interface (s): Control Panel

Description: A Save to SharePoint job that was addressed to multiple SharePoint paths was sent successfully to at least one SharePoint path but not to all SharePoint paths.

Syslog severity: Warning

Message: <device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel

Description: A Save to SharePoint job failed.

Syslog severity: Warning

Save to network folder

Message: <device type>: Save to Network Folder job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: A Save to Network Folder job was completed successfully.

Syslog severity: Informational

Message: <device type>: Save to Network Folder job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: A Save to Network Folder job was canceled.

Syslog severity: Warning

Message: <device type>: Save to Network Folder job completion; time="<timestamp>" user="<user>" outcome=partial_success

Interface (s): Control Panel

Description: A Save to Network Folder job addressed to multiple shared folder paths was sent successfully to at least one shared folder path but not to all shared folder paths.

Syslog severity: Warning

Message: <device type>: Save to Network Folder job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel

Description: A Save to Network Folder job failed.

Syslog severity: Warning

Message: <device type>: Save to Network Folder job completion; time="<timestamp>" user="Guest" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): OXPd

Description: A Save to Network Folder job was completed successfully.

Syslog severity: Informational

Message: <device type>: Save to Network Folder job completion; time="<timestamp>" user="Guest" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=canceled

Interface (s): OXPd

Description: A Save to Network Folder job was canceled.

Syslog severity: Warning

Message: <device type>: Save to Network Folder job completion; time="<timestamp>" user="Guest" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): OXPd

Description: A Save to Network Folder job failed.

Syslog severity: Warning

Save to HTTP

Message: <device type>: Save to HTTP job completion; time="<timestamp>" user="Guest" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): OXPd

Description: A Save to HTTP job was completed successfully.

Syslog severity: Informational

Message: <device type>: Save to HTTP job completion; time="<timestamp>" user="Guest" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=canceled

Interface (s): OXPd

Description: A Save to HTTP job was canceled.

Syslog severity: Warning

Message: <device type>: Save to HTTP job completion; time="<timestamp>" user="Guest" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): OXPd

Description: A Save to HTTP job failed.

Syslog severity: Warning

Scan+

Message: <device type>: Scan+ job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: A Scan+ job was sent to all reccipients successfully.

Syslog severity: Informational

Message: <device type>: Scan+ job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: A Scan+ job was canceled.

Syslog severity: Warning

Message: <device type>: Scan+ job completion; time="<timestamp>" user="<user>" outcome=partial_success

Interface (s): Control Panel

Description: A Scan+ job to two or more recipients was sent successfully to at least one recipient but not to all recipients.

Syslog severity: Warning

Message: <device type>: Scan+ job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel

Description: The processing of a Scan+ job failed.

Syslog severity: Warning

Fax send

Message: <device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel, OXPd, 9100

Description: A fax send job was completed successfully.

Syslog severity: Informational

Message: <device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel, OXPd, 9100

Description: A fax send job was canceled.

Syslog severity: Warning

Message: <device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=partial_success

Interface (s): Control Panel, OXPd, 9100

Description: A fax send job addressed to multiple fax destinations was sent successfully to at least one fax destination but not to all fax destinations.

Syslog severity: Warning

Message: <device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel, OXPd, 9100

Description: A fax send job failed.

Syslog severity: Warning

Fax receive

Message: <device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Analog Fax

Description: An analog fax was received and printed.

Syslog severity: Informational

Message: <device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Analog Fax

Description: An incoming analog fax was canceled.

Syslog severity: Warning

Message: <device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=partial_success

Interface (s): Analog Fax

Description: At least one page of a multipage incoming analog fax was printed before the fax transmission was interrupted.

Syslog severity: Warning

Message: <device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Analog Fax

Description: A remote fax device established a fax session with the local device but the fax session was terminated before any of the incoming fax was printed.

Syslog severity: Warning

Fax polling receive

Message: <device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: A fax polling receive job was completed successfully.

Syslog severity: Informational

Message: <device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: A fax polling receive job was canceled.

Syslog severity: Warning

Message: <device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel

Description: A fax polling receive job failed.

Syslog severity: Warning

Fax forwarding

Message: <device type>: Fax Forwarding job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): N/A

Description: A received or sent fax was forwarded to one or more fax numbers.

Syslog severity: Informational

Message: <device type>: Fax Forwarding job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): N/A

Description: The forwarding of a received or sent fax was canceled.

Syslog severity: Warning

Message: <device type>: Fax Forwarding job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): N/A

Description: The forwarding of a received or sent fax failed.

Syslog severity: Warning

Fax archive

Message: <device type>: Fax Archive job completion; time="<timestamp>" job_type=<job type> destination_type=<destination type> user="<user>" outcome=success

Interface (s): N/A

Description: The archival of a sent or received fax was successful.

Syslog severity: Informational

Variable (s): <job type> - This is the type of fax that was archived. Possible values are:

- sent_fax
- reveived_fax

<destination type> - This is the destination of the fax archive. Possible values are:

- e-mail
- network_folder
- ftp_server

Message: <device type>: Fax Archive job completion; time="<timestamp>" job_type=<job type> destination_type=<destination type> user="<user>" outcome=canceled

Interface (s): N/A

Description: The archival of a sent or received fax was canceled.

Syslog severity: Warning

Variable (s): <job type> - This is the type of fax that was attempted to be archived. Possible values are:

- sent_fax
- reveived_fax

<destination type> - This is the attempted destination of the fax archive. Possible values are:

- e-mail
- network_folder
- ftp_server

Message: <device type>: Fax Archive job completion; time="<timestamp>" job_type=<job type> destination_type=<destination type> user="<user>" outcome=failure

Interface (s): N/A

Description: The archival of a sent or received fax failed.

Syslog severity: Warning

Variable (s): <job type> - This is the type of fax that was attempted to be archived. Possible values are:

- sent_fax
- reveived_fax

<destination type> - This is the attempted destination of the fax archive. Possible values are:

- e-mail
- network_folder
- ftp_server

Save to USB

Message: <device type>: Save to USB job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: A Save to USB job was completed successfully.

Syslog severity: Informational

Message: <device type>: Save to USB job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: A Save to USB job was canceled.

Syslog severity: Warning

Message: <device type>: Save to USB job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel

Description: A Save to USB job failed.

Syslog severity: Warning

Retrieve from USB

Message: <device type>: Retrieve from USB job completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: A Retrieve from USB job was completed successfully.

Syslog severity: Informational

Message: <device type>: Retrieve from USB job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): Control Panel

Description: A Retrieve from USB job was canceled.

Syslog severity: Warning

Message: <device type>: Retrieve from USB job completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): Control Panel

Description: A Retrieve from USB job failed.

Syslog severity: Warning

Job notification

Message: <device type>: Job Notification completion; time="<timestamp>" user="<user>" outcome=success

Interface (s): N/A

Description: A job notification report was delivered by email.

Syslog severity: Informational

Message: <device type>: Job Notification completion; time="<timestamp>" user="<user>" outcome=canceled

Interface (s): N/A

Description: A job notification sent via email was canceled.

Syslog severity: Warning

Message: <device type>: Job Notification completion; time="<timestamp>" user="<user>" outcome=failure

Interface (s): N/A

Description: A job notification sent via email failed.

Syslog severity: Warning

Message: <device type>: Print job completion; time="<timestamp>" job_name="Notification Job" user="<user>" outcome=success

Interface (s): N/A

Description: A job notification report was printed.

Syslog severity: Informational

Message: <device type>: Print job completion; time="<timestamp>" job_name="Notification Job" user="<user>" outcome=canceled

Interface (s): N/A

Description: The printing of a job notification report was canceled.

Syslog severity: Warning

Back up and restore

Backup device data

Message: <device type>: Device Data Backup Completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The device data backup operation completed successfully.

Syslog severity: Informational

Message: <device type>: Device Data Backup Exported; time="<timestamp>" destination="<shared folder path>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The device data backup was exported successfully.

Syslog severity: Informational

Restore device data

Message: <device type>: Device Data Restore Completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: Device data from a backup was restored on the device.

Syslog severity: Informational

NOTE: Depending on the device data restored, additional messages can be generated.

Network status

Message: <device type>: Network Reconnected; time="<timestamp>" outcome=success

Interface (s): N/A

Description: The network connection has been reconnected.

Syslog severity: Notice

Message: <device type>: Network Disconnected; time="<timestamp>" outcome=success

Interface (s): N/A

Description: The network connection has been disconnected.

Syslog severity: Notice

FIPS-140 compliance

Message: <device type>: Not FIPS-140 compliant. Usage of non-FIPS supported algorithms configured/enabled.; time="<timestamp>"

Interface (s): N/A

Description: A message indicating that the device is not FIPS-140 compliant, because non-FIPS supported algorithms are enabled or configured when FIPS-140 mode is enabled.

Syslog severity: Warning

Event log

Message: <device type>: Event Log Cleared; time="<timestamp>" user="<user>" outcome=success

Interface (s): Control Panel

Description: The event log was cleared.

Syslog severity: Informational

Device configuration

Syslog

Message: <device type>: Syslog settings modified; time="<timestamp>" user ="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: A syslog setting was modified. This message is generated when any of the following syslog settings are modified:

- Server address
- Protocol
- Port
- Maximum messages
- Priority
- Facility

Syslog severity: Warning

Jetdirect logging

Message: <device type>: Jetdirect logging started; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: Jetdirect logging was enabled. This message is generated when the syslog server IP address is set and enhanced security event logging is enabled.

Syslog severity: Notice

Message: <device type>: Jetdirect logging stopped; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: Jetdirect logging was disabled. This message is generated when the syslog server IP address is cleared and enhanced security event logging is disabled.

Syslog severity: Warning

Enhanced security event logging

Message: <device type>: CCC logging started; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: Enhanced security event logging was enabled.

Syslog severity: Notice

Message: <device type>: CCC logging stopped; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: Enhanced security event logging was disabled.

Syslog severity: Warning

Jetdirect security settings factory defaults

Message: <device type>: Jetdirect security settings reset to factory defaults; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: The Jetdirect security settings were reset to factory defaults.

Syslog severity: Warning

Message: <device type>: Jetdirect security settings reset to factory defaults; time="<timestamp>" outcome=success interface=<interface>

Interface (s): Control Panel

Description: The Jetdirect security settings were reset to factory defaults.

Syslog severity: Warning

SNMPv3 user accounts

Message: <device type>: SNMPv3 user account added; time="<timestamp>" user="<user>" SNMPv3_user_account="<SNMPv3 account username>" source_IP="<client computer IP address>" hostname=<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, REST

Description: An SNMPv3 user account was added.

Syslog severity: Informational

NOTE: The "interface=<interface>" field may not be present in the message, depending on the interface used to perform the operation.

Message: <device type>: SNMPv3 user account deleted; time="<timestamp>" user="<user>" SNMPv3_user_account=<SNMPv3 account username> source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, REST

Description: An SNMPv3 user account was deleted.

Syslog severity: Informational

NOTE: The "interface=<interface>" field may not be present in the message, depending on the interface used to perform the operation.

Inactivity timeout

Message: <device type>: Control Panel Inactivity Timeout Changed; time="<timestamp>" new_value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The inactivity timeout setting was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Control Panel Inactivity Timeout Changed; time="<timestamp>" new_value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: The inactivity timeout setting failed to be modified.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Control Panel Inactivity Timeout Changed; time="<timestamp>" new_value=<value> old_value=<old value> user="<user>" outcome=success

Interface (s): Control Panel

Description: The inactivity timeout setting was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Account policy

Account lockout policy for the device administrator account

Message: <device type>: Account Lockout Policy enabled; time="<timestamp>" account=local_administrator user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The account lockout policy for the device administrator account was enabled.

Syslog severity: Informational

Message: <device type>: Account Lockout Policy disabled; time="<timestamp>" account=local_administrator user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The account lockout policy for the device administrator account was disabled.

Syslog severity: Informational

Message: <device type>: Account Lockout Policy setting modified; time="<timestamp>" account=local_administrator item=<setting> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: An account lockout policy setting for the device administrator account was modified.

Syslog severity: Informational

Variable (s): <setting> - The account lockout policy setting that was modified for the device administrator account. Possible values are:

- maximum_login_attempts
- default_lockout_time
- counter_reset_time

Account lockout policy for the remote configuration account

Message: <device type>: Account Lockout Policy enabled; time="<timestamp>" account=remote_configuration user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The account lockout policy for the remote configuration account was enabled.

Syslog severity: Informational

Message: <device type>: Account Lockout Policy disabled; time="<timestamp>" account=remote_configuration user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The account lockout policy for the remote configuration account was disabled.

Syslog severity: Informational

Message: <device type>: Account Lockout Policy setting modified; time="<timestamp>" account=remote_configuration item=<setting> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: An account lockout policy setting for the remote configuration account was modified.

Syslog severity: Informational

Variable (s): <setting> - The account lockout policy setting that was modified for the remote configuration account. Possible values are:

- maximum_login_attempts
- default_lockout_time
- counter_reset_time

Account lockout policy for SNMPv3 user accounts

Message: <device type>: Account Lockout Policy enabled; time="<timestamp>" account=SNMPv3 user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP, REST

Description: The account lockout policy for the SNMPv3 account was enabled.

Syslog severity: Informational

Message: <device type>: Account Lockout Policy disabled; time="<timestamp>" account=SNMPv3 user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP, REST

Description: The account lockout policy for the SNMPv3 account was disabled.

Syslog severity: Informational

Message: <device type>: Account Lockout Policy setting modified; time="<timestamp>" account=SNMPv3 item=<setting> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP, REST

Description: An account lockout policy setting for the SNMPv3 account was modified.

Syslog severity: Informational

Variable (s): <setting> - The account lockout policy setting that was modified for the SNMPv3 account. Possible values are:

- maximum_login_attempts
- default_lockout_time
- counter_reset_time

Password complexity policy for the device administrator password

Message: <device type>: Password Complexity Policy enabled; time="<timestamp>" account=local_administrator user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The password complexity policy for the device administrator password was enabled.

Syslog severity: Informational

Message: <device type>: Password Complexity Policy disabled; time="<timestamp>" account=local_administrator user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The password complexity policy for the device administrator password was disabled.

Syslog severity: Informational

Password complexity policy for the remote configuration password

Message: <device type>: Password Complexity Policy enabled; time="<timestamp>" account=remote_configuration user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The password complexity policy for the remote configuration password was enabled.

Syslog severity: Informational

Message: <device type>: Password Complexity Policy disabled; time="<timestamp>" account=remote_configuration user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The password complexity policy for the remote configuration password was disabled.

Syslog severity: Informational

Password complexity policy for the SNMPv3 authentication passphrase

Message: <device type>: Password Complexity Policy enabled; time="<timestamp>" account=SNMPv3 user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP, REST

Description: The password complexity policy for the SNMPv3 authentication passphrase was enabled.

Syslog severity: Informational

Message: <device type>: Password Complexity Policy disabled; time="<timestamp>" account=SNMPv3 user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP, REST

Description: The password complexity policy for the SNMPv3 authentication passphrase was disabled.

Syslog severity: Informational

Minimum password length policy for the device administrator password

Message: <device type>: Minimum Password Length Policy setting modified; time="<timestamp>" account=local_administrator item=minimum_password_length value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The minimum password length policy for the device administrator password was modified.

Syslog severity: Informational

Minimum password length policy for the remote configuration password

Message: <device type>: Minimum Password Length Policy setting modified; time="<timestamp>" account=remote_configuration item=minimum_password_length value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The minimum password length policy for the remote configuration password was modified.

Syslog severity: Informational

Minimum password length policy for the SNMPv3 authentication passphrase

Message: <device type>: Minimum Password Length Policy modified; time="<timestamp>" account=SNMPv3 item=minimum_password_length value="<value>" old_value="old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP, REST

Description: The minimum password length policy for the SNMPv3 authentication passphrase was modified.

Syslog severity: Informational

Date and time settings

Date and time settings

Message: <device type>: Date and Time configuration modified; time="<timestamp>" item=adjust_for_daylight_savings value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, SNMP

Description: The adjust for daylight savings setting was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

If the message is generated through the SNMP interface, the syslog message generated will not contain the “user”, “source_IP”, or “hostname” fields.

Message: <device type>: Date and Time configuration modified; time="<timestamp>" item=adjust_for_daylight_savings value=<value> old_value=<old value> user="<user>" outcome=success

Interface (s): Control Panel

Description: The adjust for daylight savings setting was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Date and Time configuration modified; time="<timestamp>" item=<item> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, SNMP

Description: A daylight savings time setting or the time zone was modified.

Syslog severity: Informational

Variable (s): <item> - A daylight savings setting that was modified or time zone. Possible values are:

- DST_start_month
- DST_start_occurrence
- DST_start_week_day
- DST_start_hour
- DST_end_month
- DST_end_occurrence
- DST_end_week_day
- DST_end_hour
- DST_offset_minutes
- time_zone

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

If the message is generated through the SNMP interface, the syslog message generated will not contain the “user”, “source_IP”, or “hostname” fields.

Message: <device type>: Date and Time configuration modified; time="<timestamp>" item=time_zone value="<value>" old_value="<old value>" user="<user>" outcome=success

Interface (s): Control Panel

Description: The time zone was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Date and Time configuration modified; time="<timestamp>" item=DST_settings_reset_to_factory_defaults user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, SNMP

Description: The daylight savings time settings were reset to factory defaults.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

If the message is generated through the SNMP interface, the syslog message generated will not contain the “user”, “source_IP”, or “hostname” fields.

NTS settings

Message: <device type>: Date and Time configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Network Time Server settings were modified.

Syslog severity: Informational

Variable (s): <item> - The Network Time Server setting that was modified. Possible values are:

- automatically_synchronize_with_network_time_server
- network_time_server_address
- local_port_to_receive_time_from_network_time_server
- frequency_of_time_synchronization_with_network_time_server_in_hours

<value> - The new value of the setting that was modified. Possible values are:

- enabled
- disabled
- New value of item modified

<old value> - The old value of the setting that was modified. Possible values are:

- enabled
- disabled
- New value of item modified

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: System Time Use Defaults; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The Network Time Server settings were successfully reset to factory defaults.

Syslog severity: Informational

Message: <device type>: System Time Use Defaults; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): Web Services

Description: The Network Time Server settings failed to be reset to factory defaults.

Syslog severity: Warning

Fax settings

Fax archive

Message: <device type>: Fax setting modified; time="<timestamp>" item=fax_archive value=<value> old_value=<old value> source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Fax archive settings were modified.

Syslog severity: Informational

Variable (s): <value> - The new value of the fax archive setting. Possible values are:

- do_not_archive
- archive_only
- archive_and_print

<old value> - The old value of the fax archive setting. Possible values are:

- do_not_archive
- archive_only
- archive_and_print

Fax forwarding

Message: <device type>: Fax setting modified; time="<timestamp>" item=fax_forwarding value=<value> old_value=<old value> source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Fax forwarding settings were modified.

Syslog severity: Informational

Variable (s): <value> - The new value of the fax forwarding setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the fax forwarding setting. Possible values are:

- disabled
- enabled

General security

Device administrator password

Message: <device type>: Device Administrator Password modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The device administrator password was set, cleared, or modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Device Administrator Password modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to set, clear, or modify the device administrator password was unsuccessful.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Service access code

Message: <device type>: Service User PIN modified; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The service user PIN (a.k.a., service access code) was modified.

Syslog severity: Informational

Message: <device type>: Service User PIN modified; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to modify the service user PIN (a.k.a., service access code) was unsuccessful.

Syslog severity: Warning

Remote configuration password

Message: <device type>: Remote Configuration Password Modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The remote configuration password was set, cleared, or modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Remote Configuration Password Modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to set, clear, or modify the remote configuration password was unsuccessful.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Cross-site request forgery (CRSF) prevention

Message: <device type>: Embedded Web Server Options modified; time="<timestamp>" item=Cross-site_Request_Forgery_(CSRF)_prevention value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Cross-site request forgery prevention was either enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - The new value of the CSRF prevention setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the CSRF prevention setting. Possible values:

- disabled
- enabled

Message: <device type>: Embedded Web Server Options modified; time="<timestamp>" item=Cross-site_Request_Forgery_(CSRF)_prevention value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: The attempt to either enable or disable cross-site request forgery prevention failed.

Syslog severity: Warning

Variable (s): <value> - The new value of the CSRF prevention setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the CSRF prevention setting. Possible values:

- disabled
- enabled

EWS session timeout

Message: <device type>: EWS Session Timeout modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The EWS session timeout setting was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: EWS Session Timeout modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to modify the EWS session timeout was unsuccessful.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

PJL password

Message: <device type>: PJL Password modified; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, 9100

Description: The PJL password was set, cleared, or modified.

Syslog severity: Informational

Message: <device type>: PJL Password modified; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services, 9100

Description: An attempt to set, clear, or modify the PJL password was unsuccessful.

Syslog severity: Warning

PJL Device Access Commands

Message: <device type>: PJL Security configuration modified; time="<timestamp>" item=PJL_Device_Access_Commands value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: PJL Device Access commands was enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - The new value of the setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the setting. Possible values are:

- disabled
- enabled

PJL Drive Access

Message: <device type>: PJL Drive Access enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, SNMP

Description: The PJL Drive Access was enabled.

Syslog severity: Informational

Message: <device type>: PJL Drive Access disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, SNMP

Description: The PJL Drive Access was disabled.

Syslog severity: Informational

PS Drive Access

Message: <device type>: PS Drive Access enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The PS Drive Access was enabled.

Syslog severity: Informational

Message: <device type>: PS Drive Access disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The PS Drive Access was disabled.

Syslog severity: Informational

PostScript Privileged Operators

Message: <device type>: PostScript Security configuration modified; time="<timestamp>" item=PS_Privileged_Operators value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: PostScript security configuration was modified.

Syslog severity: Informational

Variable (s): <value> - The new value of the setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the setting. Possible values are:

- disabled
- enabled

Firmware upgrade security

Message: <device type>: Firmware Upgrade Security configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A firmware upgrade security configuration setting was modified.

Syslog severity: Informational

Variable (s): <item> - The firmware upgrade security configuration setting modified. Possible values are:

- Allow_firmware_upgrades_sent_as_print_jobs_(port_9100)
- Allow_installation_of_legacy_packages_signed_with_SHA-1_Hashing_algorithm

<value> - The new value of the firmware upgrade security configuration setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the firmware upgrade security configuration setting. Possible values are:

- disabled
- enabled

Message: <device type>: Firmware Upgrade Security configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to modify a firmware upgrade security configuration setting was unsuccessful.

Syslog severity: Warning

Variable (s): <item> - The firmware upgrade security configuration setting that was attempted to be modified. Possible values are:

- Allow_firmware_upgrades_sent_as_print_jobs_(port_9100)
- Allow_installation_of_legacy_packages_signed_with_SHA-1_Hashing_algorithm

<value> - The new value of the firmware upgrade security configuration setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the firmware upgrade security configuration setting. Possible values are:

- disabled
- enabled

Bootloader administrator password

Message: <device type>: Boot Administrator Password modified; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services

Description: The pre-boot menu administrator password (a.k.a., bootloader or boot administrator password) was set, cleared, or modified.

Syslog severity: Informational

Message: <device type>: Boot Administrator Password modified; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): Web Services

Description: An attempt to set, clear, or modify the pre-boot menu administrator password (a.k.a., bootloader or boot administrator password) was unsuccessful.

Syslog severity: Warning

Drive-lock password

Message: <device type>: Encrypted Drives Random Password Set; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A new random drive-lock password was generated.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Encrypted Drives Random Password Set; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname=“<client computer hostname>“ outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to generate a new random drive-lock password was unsuccessful.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

File erase mode for managing temporary job files

Message: <device type>: Managing Temporary Job Files configuration modified; time="<timestamp>" item=File_Erase_Mode value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The file erase mode used to erase temporary job files was modified.

Syslog severity: Informational

Variable (s) <value> - The new value of the file erase mode. Possible values are:

- Non-Secure_Fast_Erase_(No_overwrite)
- Secure_Fast_Erase_(Overwrite_1_time)
- Secure_Sanitize_Erase_(Overwrite_3_times)

<old value> - The old value of the file erase mode. Possible values are:

- Non-Secure_Fast_Erase_(No_overwrite)
- Secure_Fast_Erase_(Overwrite_1_time)
- Secure_Sanitize_Erase_(Overwrite_3_times)

Access control

LDAP sign in

Message: <device type>: LDAP Sign In enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: LDAP sign in was successfully enabled.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: LDAP Sign In enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to enable LDAP sign in failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: LDAP Sign In disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: LDAP sign in was successfully disabled.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: LDAP Sign In disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to disable LDAP sign in failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: LDAP Sign In configuration modified; time="<timestamp>" item=<item> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: LDAP sign in configuration was successfully modified.

Syslog severity: Informational

Variable (s): <item> - The item that was modified in the LDAP sign in configuration. Possible values are:

- LDAP_server_address
- LDAP_server_port
- use_a_secure_connection_SSL
- bind_prefix
- server_connection_credentials_to_use
- LDAP_administrator_DN
- name_entered_match_attribute
- email_address_retrieve_attribute
- name_retrieve_attribute
- group_retrieve_attribute
- exact_match_on_group_attribute

<value> - The new value of the modified setting. Possible values are:

- enabled
- disabled
- new setting value

<old value> - The old value of the modified setting. Possible values are:

- enabled
- disabled
- old setting value

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: LDAP Sign In configuration modified; time="<timestamp>" item=<item> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to modify LDAP sign in configuration was unsuccessful.

Syslog severity: Warning

Variable (s): <item> - The item that was attempted to be modified in the LDAP sign in configuration. Possible values are:

- LDAP_server_address
- LDAP_server_port
- bind_prefix
- server_connection_credentials_to_use
- name_entered_match_attribute
- email_address_retrieve_attribute
- name_retrieve_attribute
- group_retrieve_attribute

<value> - The new value of the modified setting. Possible values are:

- new setting value

<old value> - The old value of the modified setting. Possible values are:

- old setting value

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: LDAP Sign In configuration modified; time="<timestamp>" item=LDAP_administrator_password user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The LDAP administrator password within the LDAP sign in configuration was successfully modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: LDAP Sign In configuration modified; time="<timestamp>" action=<action> value="<value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: LDAP sign in configuration was successfully modified.

Syslog severity: Informational

Variable (s): <action> - The action performed on LDAP sign in configuration. Possible values are:

- bind_and_search_root_added
- bind_and_search_root_deleted

<value> - The value of the bind and search root added or deleted.

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: LDAP Sign In configuration modified; time="<timestamp>" action=bind_and_search_root_order_modified user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The LDAP bind and search root order within the LDAP sign in configuration was successfully modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: LDAP Sign In configuration modified; time="<timestamp>" action=LDAP_sign_in_configuration_deleted user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services

Description: The LDAP sign in configuration was successfully deleted.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: LDAP Authentication Test; time="<timestamp>" username="<user name>" server="<server IP address or FQDN>" port="<port>" admin_name="<admin name>" bind_prefix="<bind prefix>" search_root="<search root>" name_match_attribute="<attribute>" email_attribute="<attribute>" group_attribute="<attribute>" group_exact_match=<group exact match> source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The LDAP authentication test was executed and successful.

Syslog severity: Informational

Message: <device type>: LDAP Authentication Test; time="<timestamp>" username="<user name>" server="<server IP address or FQDN>" port="<port>" admin_name="<admin name>" bind_prefix="<bind prefix>" search_root="<search root>" name_match_attribute="<attribute>" email_attribute="<attribute>" group_attribute="<attribute>" group_exact_match=<group exact match> source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The LDAP authentication test was executed and unsuccessful.

Syslog severity: Warning

Windows sign in

Message: <device type>: Windows Sign In enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Windows sign in was successfully enabled.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Windows Sign In enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to enable Windows sign in failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Windows Sign In disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Windows sign in was successfully disabled.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Windows Sign In configuration modified; time="<timestamp>" item=<item> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Windows sign in configuration was successfully modified.

Syslog severity: Informational

Variable (s): <item> - The item that was modified in the Windows sign in configuration. Possible values are:

- default_windows_domain
- name_entered_match_attribute
- email_address_retrieve_attribute
- name_retrieve_attribute
- reverse_DNS_lookups
- use_a_secure_connection_SSL
- Inherit_ParentGroup_Permission

<value> - The new value of the modified setting. Possible values are:

- enabled
- disabled
- new setting value

<old value> - The old value of the modified setting. Possible values are:

- enabled
- disabled
- old setting value

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: Windows Sign In configuration modified; time="<timestamp>" item=<item> value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to modify Windows sign in configuration was unsuccessful.

Syslog severity: Warning

Variable (s): <item> - The item that was attempted to be modified in the Windows sign in configuration. Possible values are:

- name_entered_match_attribute
- email_address_retrieve_attribute
- name_retrieve_attribute

<value> - The new value of the modified setting. Possible values are:

- new setting value

<old value> - The old value of the modified setting. Possible values are:

- old setting value

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: Windows Sign In configuration modified; time="<timestamp>" action=<action> value="<value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: Windows sign in configuration was successfully modified.

Syslog severity: Informational

Variable (s): <action> - The action performed on Windows sign in configuration. Possible values are:

- trusted_domain_added
- trusted_domain_deleted
- preferred_server_added
- preferred_server_deleted

<value> - The value of the trusted domain or preferred server added or deleted.

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Windows Sign In configuration modified; time="<timestamp>" action=trusted_domain_added value="<value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: A trusted domain was attempted to be added to the Windows sign in configuration and was unsuccessful.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Windows Authentication Test; time="<timestamp>" domain="<domain>" username="<user name>" reverse_DNS=<reverse DNS value> name_attribute="<attribute>" email_attribute="<attribute>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: The Windows authentication test was executed and successful.

Syslog severity: Informational

Message: <device type>: Windows Authentication Test; time="<timestamp>" domain="<domain>" username="<user name>" reverse_DNS=<reverse DNS value> name_attribute="<attribute>" email_attribute="<attribute>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: The Windows authentication test was executed and unsuccessful.

Syslog severity: Warning

Device user accounts

Message: <device type>: Device User Account added; time="<timestamp>" user="<display name>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A device user account was added.

Syslog severity: Informational

Message: <device type>: Device User Account modified; time="<timestamp>" user="<display name>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A device user account was modified.

Syslog severity: Informational

Message: <device type>: Device User Account deleted; time="<timestamp>" user="<display name>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A device user account was deleted.

Syslog severity: Informational

Message: <device type>: Device User Account deleted; time="<timestamp>" all_users_deleted source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: All device user accounts were deleted.

Syslog severity: Informational

Message: <device type>: Device User Account deleted; time="<timestamp>" all_users_deleted source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to delete all device user accounts was unsuccessful.

Syslog severity: Warning

Message: <device type>: Device User Accounts imported; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: One or more device user accounts were successfully imported.

Syslog severity: Informational

Message: <device type>: Device User Accounts exported; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: One or more device user accounts were successfully exported.

Syslog severity: Informational

Message: <device type>: Device User Accounts exported; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=canceled

Interface (s): EWS, Web Services

Description: The exporting of one or more device user accounts was canceled.

Syslog severity: Informational

Message: <device type>: Device User Accounts exported; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: The exporting of one or more device user accounts was unsuccessful.

Syslog severity: Warning

Message: <device type>: Default Permission Set for sign-in method modified; time="<timestamp>" sign-in_method=local_device permission_set="<new permission set name>" old_value="<old permission set name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The default permission set to be associated with new device user accounts was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Default sign-in method for the control panel

Message: <device type>: Default Sign-in method for control panel applications modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The default sign-in method for the control panel was modified.

Syslog severity: Informational

Variable (s): <value> - The new sign-in method associated with control panel applications. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authentication agents

<old value> - The old sign-in method associated with control panel applications. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Default sign-in method for the EWS

Message: <device type>: Default Sign-in method for EWS tabs modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The default sign-in method for the EWS was successfully modified.

Syslog severity: Informational

Variable (s): <value> - The new sign-in method associated with EWS tabs. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authentication agents

<old value> - The old sign-in method associated with EWS tabs. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: Default Sign-in method for EWS tabs modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS, Web Services

Description: An attempt to modify the default sign-in method for the EWS was unsuccessful.

Syslog severity: Warning

Variable (s): <value> - The new sign-in method associated with EWS tabs. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authentication agents

<old value> - The old sign-in method associated with EWS tabs. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Default sign-in method for remote apps

Message: <device type>: Default Sign-in method for whitelisted remote apps modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The default sign-in method for whitelisted remote apps was successfully modified.

Syslog severity: Informational

Variable (s): <value> - The new sign-in method associated with whitelisted remote apps. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authentication agents

<old value> - The old sign-in method associated with whitelisted remote apps. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Sign-in method assigned to control panel applications

Message: <device type>: Sign In and Permission Policy settings modified; time="<timestamp>" control_panel_application="<application>" item=sign-in_method value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A new sign-in method was assigned to a control panel application.

Syslog severity: Informational

Variable (s): <application> - Control panel application. Possible values depend on the control panel applications supported by the device and any third-party solutions that have been installed on the device.

<value> - New sign-in method. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

<old value> - Old sign-in method. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Sign-in method assigned to EWS tabs/pages

Message: <device type>: Sign In and Permission Policy settings modified; time="<timestamp>" EWS_tab="<EWS tab>" item=sign-in_method value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The sign-in method assigned to an EWS tab was modified.

Syslog severity: Informational

Variable (s): <EWS tab> - EWS tab. Possible EWS tabs depend on the control panel applications supported by the device and any third-party solutions that have been installed on the device.

<value> - New sign-in method. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

<old value> - Old sign-in method. Possible values are:

- local_device
- ldap
- windows
- smartcard
- other supported authenticated agents

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Custom permission sets

Message: <device type>: Permission Set added; time="<timestamp>" permission_set="<permission set name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A custom permission set was added.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Permission Set modified; time="<timestamp>" permission_set="<permission set name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The name of a custom permission set was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Permission Set copied; time="<timestamp>" permission_set="<permission set name>" copied_from_permission_set="<base permission set name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A custom permission set was added by copying an existing permission set.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Permission Set deleted; time="<timestamp>" permission_set="<permission set name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A custom permission set was deleted.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Permissions associated with permission sets

Message: <device type>: Permission Set modified; time="<timestamp>" permission_set="<permission set name>" permission=<permission> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A permission was either granted or denied to a permission set.

Syslog severity: Informational

Variable (s): <permission> - Permission. Possible permissions depend on the protected features supported by the device and any third-party solutions that have been installed on the device.

<value> - New permission status. Possible permission statuses are:

- access_granted
- access_denied

<old value> - Old permission status. Possible permission statuses are:

- access_denied
- access_granted

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Permission Set modified; time="<timestamp>" permission_set="<permission set name>" permission=all_permissions value=access_denied old_value=access_granted user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services

Description: All permissions were denied to a permission set.

Syslog severity: Informational

Allow users to choose alternate sign-in methods at the product control panel

Message: <device type>: Sign In and Permission Policy settings modified; time="<timestamp>" item=allow_users_to_choose_alternate_sign-in_methods value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The “Allow users to choose alternate sign-in methods at the product control panel” setting was enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - The new value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Automatically sign users out after starting each job

Message: <device type>: Sign In and Permission Policy settings modified; time="<timestamp>" item=automatically_sign_users_out_after_starting_each_job value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The automatically sign users out after starting each job configuration option was enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - New value of the configuration option. Possible values are:

- enabled
- disabled

<old value> - Old value of the configuration option. Possible values are:

- enabled
- disabled

Default permission set for network users

Message: <device type>: Default Permission Set for sign-in method modified; time="<timestamp>" sign-in_method=<sign-in method> permission_set="<permission set name>" old_value="<old permission set name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The default permission set for a sign-in method was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Network user to permission set relationships

Message: <device type>: User to Permission Set Relationship added; time="<timestamp>" network_user_name="<network user name>" permission_set="<permission set name>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A network user to permission set relationship was added.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: User to Permission Set Relationship modified; time="<timestamp>" network_user_name="<network user name>" permission_set="<permission set name>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services

Description: A network user to permission set relationship was modified.

Syslog severity: Informational

Message: <device type>: User to Permission Set Relationship deleted; time="<timestamp>" network_user_name="<network user name>" permission_set="<permission set name>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A network user to permission set relationship was deleted.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: All User to Permission Set Relationships deleted; time="<timestamp>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services

Description: All network user to permission set relationships for a specific remote sign-in method were deleted.

Syslog severity: Informational

Network group to permission set relationships

Message: <device type>: Group to Permission Set Relationship added; time="<timestamp>" network_group_name="<network group name>" permission_set="<permission_set name>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A network group to permission set relationship was added.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Group to Permission Set Relationship modified; time="<timestamp>" network_group_name="<network group name>" permission_set="<permission set name>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services

Description: A network group to permission set relationship was modified.

Syslog severity: Informational

Message: <device type>: Group to Permission Set Relationship deleted; time="<timestamp>" network_group_name="<network group name>" permission_set="<permission_set name>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A network group to permission set relationship was deleted.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the "user" field.

Message: <device type>: All Group to Permission Set Relationships deleted; time="<timestamp>" sign_in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): Web Services

Description: All group to permission set relationships for a specific remote sign-in method were deleted.

Syslog severity: Informational

Top level button

Message: <device type>: Top Level button created, ButtonId : <button ID>, ButtonTitle : <button title>, ButtonUrl : <button URL> ; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): OXPd

Description: A Top Level button was added.

Syslog severity: Informational

Variable (s): <button ID> - ID of the Top Level button.

<button title> - Title of Top Level button.

<button URL> - URL of Top Level button.

Message: <device type>: Top Level button modified, ButtonId : <button ID>, Old ButtonTitle : <old button title>, New ButtonTitle : <new button title>, Old ButtonUrl : <old button URL>, New ButtonUrl : <new button URL>; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): OXPd

Description: A Top Level button was modified.

Syslog severity: Informational

Variable (s): <button ID> - ID of the Top Level button.
<old button title> - Old title of Top Level button.
<new button title> - New title of Top Level button.
<old button URL> - Old URL of Top Level button.
<new button URL> - New URL of Top Level button.

Message: <device type>: Top Level button deleted, ButtonId : <button ID>; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): OXPd

Description: A Top Level button was deleted.

Syslog severity: Informational

Variable (s): <button ID> - ID of the Top Level button that was deleted.

Certificates

CA certificates

Message: <device type>: Device CA certificate installed; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A device CA certificate was installed.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Device CA certificate deleted; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A device CA certificate was deleted.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Identity certificates

Message: <device type>: Self-signed device Identity certificate created; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A new self-signed device identity certificate was generated.

Syslog severity: Informational

Message: <device type>: Device Identity CSR created; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: A device identity certificate signing request was generated.

Syslog severity: Informational

Message: <device type>: Device Identity certificate from CSR installed; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A device identity certificate generated from a certificate signing request was installed.

Syslog severity: Informational

Message: <device type>: Device Identity certificate and private key installed; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A device identity certificate with private key was installed.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Device Identity certificate deleted; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A device identity certificate was deleted.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Device Identity certificate for network identity selected; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A new device identity certificate was selected for network identity.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Device Identity certificate for e-mail selected; time="<timestamp>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A new device identity certificate was selected for email signing.

Syslog severity: Informational

Message: <device type>: Certificate selected for IPSec usage; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services, OXPd

Description: A new device identity certificate was selected for IPSec usage.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Kerberos server certificate validation

Message: <device type>: Online Certificate Status Protocol URL added; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: An Online Certificate Status Protocol URL was added for Kerberos server certificate validation.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Online Certificate Status Protocol URL added; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: An attempt was made to add an Online Certificate Status Protocol URL for Kerberos server certificate validation and failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Online Certificate Status Protocol URL deleted; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: An Online Certificate Status Protocol URL for Kerberos server certificate validation was deleted.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Online Certificate Status Protocol URL deleted; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: An attempt was made to delete an Online Certificate Status Protocol URL for Kerberos server certificate validation and failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Certification Validation settings modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A certificate validation setting for Kerberos server certificate validation was modified.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Certification Validation settings modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: An attempt was made to modify a certificate validation setting for Kerberos server certificate validation and failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Remote App Whitelisting

Message: <device type>: Remote App has been whitelisted.; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A remote application has been added to the allowlist.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: Remote App has been delisted.; time="<timestamp>" user="<user>" source_IP="<client computer IP address" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: A remote application has been removed from the allowlist.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

HP Connection Inspector

Message: <device type>: HP Connection Inspector enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname=“<client computer hostname>“ outcome=success interface=<interface>

Interface (s): EWS

Description: HP Connector Inspector feature was enabled.

Syslog severity: Informational

Message: <device type>: HP Connection Inspector enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure interface=<interface>

Interface (s): EWS

Description: An attempt to enable the HP Connector Inspector feature failed.

Syslog severity: Informational

Message: <device type>: HP Connection Inspector disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: HP Connector Inspector feature was disabled.

Syslog severity: Informational

Message: <device type>: HP Connection Inspector disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure interface=<interface>

Interface (s): EWS

Description: An attempt to disable the HP Connector Inspector feature failed.

Syslog severity: Informational

Message: <device type>: HP Connection Inspector settings modified; time="<timestamp>" action=factory_defaults_restored user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: HP Connection Inspector settings were restored to factory defaults.

Syslog severity: Informational

Message: <device type>: HP Connection Inspector Protected Mode settings modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<source_IP>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: A Protected Mode setting for the HP Connection Inspector feature was modified.

Syslog severity: Informational

Variable (s): <item> - HP Connectoin Inspector Protected Mode setting that was modified. Possible values are:

- dns_failure_threshold
- monitoring_window
- protected_mode_duration
- number_of_times_in_protected_mode
- cumulative_protected_mode_duration

Message: <device type>: HP Connection Inspector Protected Mode settings modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<source_IP>" hostname="<client computer hostname>" outcome=failure interface=<interface>

Interface (s): EWS

Description: An attempt to modify a Protected Mode setting for the HP Connection Inspector feature failed.

Syslog severity: Informational

Variable (s): <item> - HP Connectoin Inspector Protected Mode setting that was attempted to be modified. Possible values are:

- dns_failure_threshold
- monitoring_window
- protected_mode_duration
- number_of_times_in_protected_mode
- cumulative_protected_mode_duration

Message: <device type>: HP Connection Inspector Advanced settings modified; time="<timestamp>" action=<action> value="<value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An entry was added to or deleted from the whitelist/exception list for the HP Connection Inspector feature.

Syslog severity: Informational

Variable (s): <action> - Whether an entry was added or deleted from the whitelist. Possible values are:

- whitelist-exception_list_entry_added
- whitelist-exception_list_entry_deleted

Message: <device type>: HP Connection Inspector Advanced settings modified; time="<timestamp>" action=<action> value="<value>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure interface=<interface>

Interface (s): EWS

Description: An attempt was made to add or delete an entry from the whitelist/exception list for the HP Connection Inspector feature and failed.

Syslog severity: Informational

Variable (s): <action> - Whether an entry was attempted to be added or deleted from the whitelist. Possible values are:

- whitelist-exception_list_entry_added
- whitelist-exception_list_entry_deleted

HP Workpath Platform

Message: <device type>: HP Workpath Platform disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: HP Workpath Platform feature was disabled.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: HP Workpath Platform disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: An attempt to disable the HP Workpath Platform feature failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: HP Workpath Platform enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS

Description: HP Workpath Platform feature was enabled.

Syslog severity: Informational

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

Message: <device type>: HP Workpath Platform enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=failure

Interface (s): EWS

Description: An attempt to enable the HP Workpath Platform feature failed.

Syslog severity: Warning

NOTE: If an unauthenticated user performs the operation which causes the above message to be generated, the syslog message will not contain the “user” field.

USB Ports

Message: <device type>: Hardware Ports configuration modified; time="<timestamp>" item=Device_USB value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The Device USB configuration option was enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

Message: <device type>: Hardware Ports configuration modified; time="<timestamp>" item=Device_USB value=<value> old_value=<old value> user="<user>" outcome=success

Interface (s): Control Panel

Description: The Device USB configuration option was enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

Message: <device type>: Hardware Ports configuration modified; time="<timestamp>" item=Host_USB_plug_and_play value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success

Interface (s): EWS, Web Services

Description: The Host USB Plug and Play configuration option was enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

FIPS-140

Message: <device type>: FIPS-140 mode enabled.Reboot required for FIPS-140 mode modification to take effect. Rebooting now; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS

Description: FIPS-140 mode was enabled.

Syslog severity: Informational

Message: <device type>: FIPS-140 mode disabled.Reboot required for FIPS-140 mode modification to take effect. Rebooting now; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS

Description: FIPS-140 mode was disabled.

Syslog severity: Informational

Android Debug Bridge

Message: <device type>: Android Debug Bridge (ADB) enablement initiated; time="<timestamp>" outcome=success

Interface (s): EWS, Control Panel

Description: The enablement of the Android Debug Bridge (ADB) has been initiated.

Syslog severity: Informational

Message: <device type>: Android Debug Bridge (ADB) enabled; time="<timestamp>" outcome=success

Interface (s): EWS, Control Panel

Description: Android Debug Bridge (ADB) was enabled.

Syslog severity: Informational

Message: <device type>: Android Debug Bridge (ADB) disabled; time="<timestamp>" outcome=success

Interface (s): EWS, Control Panel

Description: Android Debug Bridge (ADB) was disabled.

Syslog severity: Informational

Jetdirect Security Settings

Message: <device type>: Jetdirect security settings reset to factory defaults; time="<timestamp>" outcome=success interface=<interface>

Interface (s): Control Panel

Description: Jetdirect security settings were reset to factory defaults.

Syslog severity: Informational

Message: <device type>: Jetdirect security settings reset to factory defaults; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: Jetdirect security settings were reset to factory defaults.

Syslog severity: Informational

Message: <device type>: Jetdirect 802.1x Authentication settings reset to factory defaults; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP

Description: Jetdirect 802.1x Authentication settings were reset to factory defaults.

Syslog severity: Informational

Device Discovery

Message: <device type>: Device Discovery configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: An item within Device Discovery configuration was successfully modified.

Syslog severity: Informational

Variable (s): <item> - The Device Discovery configuration item modified.
Possible values are:

- SLP
- Bonjour
- Multicast_IPv4
- WS-Discovery

<value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

Management Protocols

Message: <device type>: Management Protocols configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: An item within Management Protocols configuration was successfully modified.

Syslog severity: Informational

Variable (s): <item> - The Management Protocols configuration item modified. Possible values are:

- Verify_Certificate_for_IPP_IPPS_pull_printing
- HP_Jetdirect_XML_Services
- Telnet
- TFTP_Configuration_File

<value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

Name Resolution

Message: <device type>: Name Resolution configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: An item within Name Resolution configuration was successfully modified.

Syslog severity: Informational

Variable (s): <item> - The Name Resolution configuration item modified. Possible values:

- LLMNR
- Enable_WINS_Port
- WINS_Registration

<value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

Print Services

Message: <device type>: Print Services configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: An item within Print Services configuration was successfully modified.

Syslog severity: Informational

Variable (s): <item> - The Print Services configuration item modified. Possible values are:

- 9100_printing
- LPD
- Web_Services_Print
- AirPrint
- IPP
- IPPS

<value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- disabled
- enabled

Web Communications

Message: <device type>: Encrypt All Web Communication (not including IPP) disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: Encrypt All Web Communication (not including IPP) was disabled.

Syslog severity: Informational

Message: <device type>: Encrypt All Web Communication (not including IPP) enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: Encrypt All Web Communication (not including IPP) was enabled.

Syslog severity: Informational

Active Ciphers list

Message: <device type>: Active Ciphers list for TLS modified; time="<timestamp>" cipher=<cipher> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: The active ciphers list for TLS authentication were modified.

Syslog severity: Informational

Variable (s): <cipher> - The cipher that was modified. Possible values are:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA256
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES256-SHA
- DHE-RSA-AES256-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- DHE-RSA-AES128-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA

<value> - The value of the modified setting. Possible values are:

- available
- active

<old value> - The old value of the modified setting. Possble values are:

- available
- active

Block Access to Specific HTTP Services

Message: <device type>: Block Access to Specific HTTP Services configuration modified; time="<timestamp>" value="<value>" user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS

Description: Access to specific HTTP services was enabled or disabled.

Syslog severity: Informational

Variable (s): <value> - The HTTP service configuration that was enabled or disabled. Possible values are:

- disable_port_80
- disable_port_443
- disable_port_7627

SSL/TLS Protocol

Message: <device type>: SSL/TLS Protocol configuration modified; time="<timestamp>" MinTLS value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS

Description: The minimum TLS version supported was modified.

Syslog severity: Informational

Variable (s): <value> - New minimum TLS version. Possible values are:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

<old value> - Old minimum TLS version. Possible values are:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

Message: <device type>: SSL/TLS Protocol configuration modified; time="<timestamp>" MaxTLS value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname=<client computer hostname> outcome=success interface=<interface>

Interface (s): EWS

Description: The maximum TLS version supported was modified.

Syslog severity: Informational

Variable (s): <value> - New maximum TLS version. Possible values are:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

<old value> - Old maximum TLS version. Possible values are:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

Message: <device type>: SSL/TLS Protocol configuration modified; time="<timestamp>" item=<item> value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): SNMP

Description: The TLS versions supported were modifed.

Syslog severity: Informational

Variable (s): <item> - TBD. Possible values are:

- TLS_1.0
- TLS_1.1
- TLS_1.2

<value> - The value of the modified setting. Possible values are:

- enabled
- disabled

<old value> - The old value of the modified setting. Possible values are:

- enabled
- disabled

SNMP v1/v2

Message: <device type>: SNMPv1/v2 read-write access enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: SNMPv1/v2 read-write access was enabled.

Syslog severity: Informational

Message: <device type>: SNMPv1/v2 read-only access enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: SNMPv1/v2 read-only access was enabled.

Syslog severity: Informational

Message: <device type>: SNMPv1/v2 disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: SNMPv1/v2 was disabled.

Syslog severity: Informational

Message: <device type>: SNMPv1/v2 Set Community Name modified; time="<timestamp>" status=<status> old status=<old status> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: SNMPv1/v2 Set Community Name was modified.

Syslog severity: Informational

Variable (s): <status> - The new status of the Set Community Name. Possible values are:

- set
- not_set

<old status> - The old status of the Set Community Name.
Possible values are:

- set
- not_set

Message: <device type>: SNMPv1/v2 Get Community Name modified; time="<timestamp>" status=<status> old status=<old status> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: SNMPv1/v2 Get Community Name was modified.

Syslog severity: Informational

Variable (s): <status> - The new status of the Get Community Name. Possible values are:

- set
- not_set

<old status> - The old status of the Get Community Name.
Possible values are:

- set
- not_set

Message: <device type>: SNMPv1/v2 default Get Community Name of “public” enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: SNMPv1/v2 default Get Community Name of public was enabled.

Syslog severity: Informational

NOTE: In the event generated above, “public” may or not be contained in quotes.

Message: <device type>: SNMPv1/v2 default Get Community Name of “public” disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP, Telnet

Description: SNMPv1/v2 default Get Community Name of public was disabled.

Syslog severity: Informational

NOTE: In the event generated above, “public” may or not be contained in quotes.

IPsec

IPsec policy

Message: <device type>: IPsec enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: The IPsec policy was enabled.

Syslog severity: Warning

Message: <device type>: IPsec disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, SNMP

Description: The IPsec policy was disabled.

Syslog severity: Warning

Message: <device type>: IPsec disabled; time="<timestamp>" user="guest" outcome=success interface=<interface>

Interface (s): Control Panel

Description: The IPsec policy was disabled.

Syslog severity: Warning

IPsec rules

Message: <device type>: IPsec rule added; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec rule was added.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec rule position changed; time="<timestamp>" rule_<old index>_moved_to_<new index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: Index of an IPsec rule in the rules list was modified.

Syslog severity: Warning

Variable (s): <old index> - Old index of the rule in the rules list. Possible values are: 1 – 10

<new index> - New index of the rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec rule deleted; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec rule was deleted.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec rule enabled; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec rule was enabled.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec rule disabled; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec rule was disabled.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec default rule action modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The action-on-match for the default IPsec rule was modified.

Syslog severity: Warning

Variable (s): <value> - New action-on-match. Possible values are:

- allow
- drop

<old value> - Old action-on-match. Possible values are:

- drop
- allow

IPsec address templates

Message: <device type>: IPsec address policy added; time="<timestamp>" policy_name="<address policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec address template was added.

Syslog severity: Warning

Message: <device type>: IPsec address policy modified; time="<timestamp>" policy_name="<address policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec address template was modified.

Syslog severity: Warning

Message: <device type>: IPsec address policy deleted; time="<timestamp>" policy_name="<address policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec address template was deleted.

Syslog severity: Warning

IPsec service templates

Message: <device type>: IPsec service policy added; time="<timestamp>" policy_name="<service policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec service template was added.

Syslog severity: Warning

Message: <device type>: IPsec service policy modified; time="<timestamp>" policy_name="<service policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec service template was modified.

Syslog severity: Warning

Message: <device type>: IPsec service policy deleted; time="<timestamp>" policy_name="<service policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec service template was deleted.

Syslog severity: Warning

IPsec advanced options

Message: <device type>: IPsec configuration change; time="<timestamp>" item=advanced_settings value=<advanced option> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec policy advanced configuration option was modified.

Syslog severity: Warning

Variable (s): <advanced option> - IPsec policy advanced configuration option that was modified. Possible values are:

- WS-Discovery_service
- IGMPv2_service
- ICMPv6_service
- ICMPv4_service
- Bonjour_service
- SLP_service
- DHCPv6_service
- DHCPv4_BOOTP_service
- NTP_service
- Fail_Safe_option
- IKE_Retries
- IKE_Retransmit_interval
- Dead_Peer_Timer

IPsec policy with manual keying

Message: <device type>: IPsec policy added; time="<timestamp>" policy_name="<IPsec policy name>" item=authentication_method value=Manual_keys user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: A manual keys IPsec policy was added.

Syslog severity: Warning

Message: <device type>: IPsec policy modified ; time="<timestamp>" policy_name="<IPsec policy name>" item=authentication_method value=IKEv1 old_value=Manual_Keys identity_authentication_option=<identity authentication option> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: A manual keys IPsec policy was modified and converted into an IKEv1 IPsec policy.

Syslog severity: Warning

Variable (s): <identity authentication option> - Authentication method that will be used to mutually authenticate both endpoints. Possible values are:

- Pre-shared_key
- Certificates
- Kerberos

Message: <device type>: IPsec policy modified ; time="<timestamp>" policy_name="<IPsec policy name>" item=authentication_type value=IKEv2 old_value=Manual_Keys local_identity_authentication_option=<local identity authentication option> local_identity_type="<local identity type>" item=remote_identity_authentication_option=<remote identity authentication option> remote_identity_type="<remote identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: A manual keys IPsec policy was modified and converted into an IKEv2 IPsec policy.

Syslog severity: Warning

Variable (s): <local identity authentication option> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:

- Pre-shared_key
- Certificates

<local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<remote identity authentication option> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:

- Pre-shared_key
- Certificates

<remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=authentication_method value=Manual_keys old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv1 IPsec policy was modified and converted into a manual keys IPsec policy.

Syslog severity: Warning

Variable (s): <old value> - The value of the old IPsec policy option. Possible values are:

- IKEv1
- IKEv2

Message: <device type>: IPsec policy deleted; time="<timestamp>" policy_name="<IPsec policy name>" item=authentication_method value=Manual_keys user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: A manual keys IPsec policy was deleted.

Syslog severity: Warning

IPsec policy with IKEv1

Message: <device type>: IPsec policy added; time="<timestamp>" policy_name="<IPsec policy name>" item=identity_authentication_option value=<value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv1 IPsec policy was added.

Syslog severity: Warning

Variable (s): <value> - Authentication method that will be used by both endpoints to perform mutual authentication. Possible values are:

- Pre-shared_key
- Certificates
- Kerberos

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=identity_authentication_option value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv1 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <value> - Authentication method that will be used by both endpoints to perform mutual authentication. Possible values are:

- Pre-shared_key
- Certificates
- Kerberos

<old value> - Previous authentication method that will be used by both endpoints to perform mutual authentication. Possible values are:

- Pre-shared_key
- Certificates
- Kerberos

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=authentication_type value=IKEv1 old_value=IKEv2 identity_authentication_option value=<value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv2 IPsec policy was modified and converted into an IKEv1 IPsec policy.

Syslog severity: Warning

Variable (s): <value> - Authentication method that will be used by both endpoints to perform mutual authentication. Possible values are:

- Pre-shared_key
- Certificates
- Kerberos

Message: <device type>: IPsec policy deleted; time="<timestamp>" policy_name="<IPsec policy name>" item=identity_authentication_option value=<value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv1 IPsec policy was deleted.

Syslog severity: Warning

Variable (s): <value> - Authentication method that will be used by both endpoints to perform mutual authentication. Possible values are:

- Pre-shared_key
- Certificates
- Kerberos

IPsec policy with IKEv2

Message: <device type>: IPsec policy added; time="<timestamp>" policy_name="<IPsec policy name>" local_identity_authentication_option=<local identity authentication option> local_identity_type="<local identity type>" remote_identity_authentication_option=<remote identity authentication option> remote_identity_type="<remote identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv2 IPsec policy was added.

Syslog severity: Warning

Variable (s): <local identity authentication option> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:

- Pre-shared_key
- Certificates

<local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<remote identity authentication option> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:

- Pre-shared_key
- Certificates

<remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=local_identity_type value="<value>" old_value="<old value>" local_identity_authentication_option=<local identity authentication option> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The local identity type in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <value> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<old value> - Previous identity type that was used by the IPsec peer to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<local identity authentication option> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:

- Pre-shared_key
- Certificates

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=Identity local_identity_authentication_option=<local identity authentication option> local_identity_type="<local identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The local identity in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <local identity authentication option> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:

- Pre-shared_key
- Certificates

<local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=Key local_identity_authentication_option=Pre-Shared_Key local_identity_type="<local identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The pre-shared key contained in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=local_identity_authentication_option value=<value> old_value=<old value> local_identity_type="<local identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The local identity authentication option in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <value> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:

- Pre-shared_key
- Certificates

<old value> - Previous local identity authentication that was used by the IPsec peer to authentication the local device. Possible values are:

- Pre-shared_key
- Certificates

<local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=remote_identity_type value="<value>" old_value="<old value>" remote_identity_authentication_option=<remote identity authentication option> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The remote identity type in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <value> - Identity type the local device will use to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<old value> - Previous identity type the local device used to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<remote identity authentication option> - Authentication method the local device will use to authentication the IPsec peer. Possible values are:

- Pre-shared_key
- Certificates

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=Identity remote_identity_authentication_option=<remote identity authentication option> remote_identity_type="<remote identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The remote identity in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <remote identity authentication option> - Authentication method the local device will use to authentication the IPsec peer. Possible values are:

- Pre-shared_key
- Certificates

<remote identity type> - Identity type the local device will use to authenticate the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=Key remote_identity_authentication_option=Pre-Shared_Key remote_identity_type="<remote identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The pre-shared key contained in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=remote_identity_authentication_option value=<value> old_value=<old value> remote_identity_type="<remote identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The remote identity authentication option in an IKEv2 IPsec policy was modified.

Syslog severity: Warning

Variable (s): <value> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:

- Pre-shared_Key
- Certificates

<old value> - Previous authentication method the local device used to authenticate the IPsec peer. Possible values are:

- Pre-shared_Key
- Certificates

<remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy modified; time="<timestamp>" policy_name="<IPsec policy name>" item=authentication_type value=IKEv2 old_value=IKEv1 local_identity_authentication_option=<local identity authentication option> local_identity_type="<local identity type>" remote_identity_authentication_option=<remote identity authentication option> remote_identity_type="<remote identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv1 IPsec policy was modified and converted into an IKEv2 IPsec policy.

Syslog severity: Warning

Variable (s): <local identity authentication option> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:

- Pre-shared_Key
- Certificates

<local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<remote identity authentication option> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:

- Pre-shared_Key
- Certificates

<remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Message: <device type>: IPsec policy deleted; time="<timestamp>" policy_name="<IPsec policy name>" local_identity_authentication_option=<local identity authentication option> local_identity_type="<local identity type>" remote_identity_authentication_option=<remote identity authentication option> remote_identity_type="<remote identity type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IKEv2 IPsec policy was deleted.

Syslog severity: Warning

Variable (s): <local identity authentication option> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:

- Pre-shared_Key
- Certificates

<local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

<remote identity authentication option> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:

- Pre-shared_Key
- Certificates

<remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:

- Distinguished_Name
- FQDN
- E-mail
- IP_Address
- Key-ID

Firewall

Message: <device type>: Bypass HTTPS option applied; time="<timestamp>" value=<value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, Control Panel, SNMP, REST

Description: The bypass HTTPS configuration option was modified.

Syslog severity: Warning

Variable (s): <value> - New value of the bypass HTTPS option. Possible values are:

- allow
- drop

Message: <device type>: Default firewall rule applied; time="<timestamp>" value=<value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, Control Panel, SNMP, REST

Description: The default firewall rule configuration option was modified.

Syslog severity: Warning

Variable (s): <value> - New value of the default firewall rule configuration option. Possible values are:

- allow
- drop

Message: <device type>: Firewall Security enabled; time="<timestamp>" interface_type="<interface_type>" user="<user>" source_IP="<source_IP>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: Firewall security was enabled.

Syslog severity: Warning

Variable (s): <interface_type> - Applicable interface. Possible values are:

- all_interfaces
- primary_ethernet
- secondary_ethernet
- wireless_sta

Message: <device type>: Firewall Security disabled; time="<timestamp>" interface_type="<interface_type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, Control Panel, SNMP, REST

Description: Firewall security was disabled.

Syslog severity: Warning

Variable (s): <interface_type> - Applicable interface. Possible values are:

- all_interfaces
- primary_ethernet
- secondary_ethernet
- wireless_sta

Firewall rules

Message: <device type>: Firewall rule added; time="<timestamp>" rule_name="<firewall rule name>" rule_action=<rule action> state=<state> protocol=<protocol> rule_direction=<rule direction> remote_ip_address="<remote IP address>" port=<port list> interface_type="<interface type>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An Firewall rule was added.

Syslog severity: Warning

Variable (s): <rule action> - The firewall rule action. Possible values are:

- drop
- allow

<state> - The state of the firewall rule. Possible values are:

- disabled
- enabled

<protocol> - The protocols included in the firewall rule. Possible values are:

- any_protocol
- tcp
- udp
- icmpv4
- icmpv6

<rule direction> – The firewall rule direct. Possible values are:

- in
- out
- both

<remote IP address> - The remote IP address/addresses associated with he firewall rule. Possible values are:

- Specific IPv4 address
- Specific IPv6 address
- Range of IPv4 addresses
- Range of IPv6 addresses
- all_ip_addresses
- all_ipv4_addresses
- all_ipv6_addresses

<port> - The port list. Possilbe values are:

- all_ports
- Port list associates with the rule

<interface type> - The interface associated with the firewall rule. Possible values are:

- all_interfaces
- primary_ethernet
- secondary_ethernet
- wireless_sta

Message: <device type>: Firewall rule deleted; time="<timestamp>" rule_name="<firewall rule name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: A Firewall rule was deleted.

Syslog severity: Warning

Message: <device type>: Firewall all rules deleted; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: All firewall rules were deleted.

Syslog severity: Warning

IPsec/Firewall

IPsec/Firewall policy

Message: <device type>: IPsec/Firewall enabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The IPsec/Firewall policy was enabled.

Syslog severity: Warning

Message: <device type>: IPsec/Firewall disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS, Telnet, SNMP

Description: The IPsec/Firewall policy was disabled.

Syslog severity: Warning

Message: <device type>: IPsec/Firewall disabled; time="<timestamp>" user="<user>" outcome=success interface=<interface>

Interface (s): Control Panel

Description: The IPsec/Firewall policy was disabled.

Syslog severity: Warning

IPsec/Firewall rules

Message: <device type>: IPsec/Firewall rule added; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall rule was added.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec/Firewall rule position changed; time="<timestamp>" rule_<old index>_moved_to_<new index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: Index of an IPsec/Firewall rule in the rules list was modified.

Syslog severity: Warning

Variable (s): <old index> - Old index of the rule in the rules list. Possible values are: 1 – 10

<new index> - New index of the rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec/Firewall rule deleted; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall rule was deleted.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec/Firewall rule enabled; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall rule was enabled.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec/Firewall rule disabled; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall rule was disabled.

Syslog severity: Warning

Variable (s): <rule index> - Index of rule in the rules list. Possible values are: 1 – 10

Message: <device type>: IPsec/Firewall default rule action modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: The action-on-match for the default IPsec/Firewall rule was modified.

Syslog severity: Warning

Variable (s): <value> - New action-on-match. Possible values are:

- allow
- drop

<old value> - Old action-on-match. Possible values are:

- drop
- allow

IPsec/Firewall address templates

Message: <device type>: IPsec/Firewall address policy added; time="<timestamp>" policy_name="<address policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall address template was added.

Syslog severity: Warning

Message: <device type>: IPsec/Firewall address policy modified; time="<timestamp>" policy_name="<address policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall address template was modified.

Syslog severity: Warning

Message: <device type>: IPsec/Firewall address policy deleted; time="<timestamp>" policy_name="<address policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall address template was deleted.

Syslog severity: Warning

IPsec/Firewall service templates

Message: <device type>: IPsec/Firewall service policy added; time="<timestamp>" policy_name="<service policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall service template was added.

Syslog severity: Warning

Message: <device type>: IPsec/Firewall service policy modified; time="<timestamp>" policy_name="<service policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall service template was modified.

Syslog severity: Warning

Message: <device type>: IPsec/Firewall service policy deleted; time="<timestamp>" policy_name="<service policy name>" user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall service template was deleted.

Syslog severity: Warning

IPsec/Firewall advanced options

Message: <device type>: IPsec/Firewall configuration change; time="<timestamp>" item=advanced_settings value=<advanced option> user="<user>" source_IP="<client computer IP address>" hostname="<client computer hostname>" outcome=success interface=<interface>

Interface (s): EWS

Description: An IPsec/Firewall policy advanced option was modified.

Syslog severity: Warning

Variable (s): <advanced option> - IPsec/Firewall policy advanced option that was modified. Possible values are:

- WS-Discovery_service
- IGMPv2_service
- ICMPv6_service
- ICMPv4_service
- Bonjour_service
- SLP_service
- DHCPv6_service
- DHCPv4_BOOTP_service
- NTP_service
- Fail_Safe_option
- IKE_Retries
- IKE_Retransmit_interval
- Dead_Peer_Timer

Basic event log messages

This chapter describes the basic security event log messages.

Basic event log message components

The Basic event log message format includes the following components.

Table 6 Basic event logging message components

Components	Description
Message	The message string excluding the syslog priority, along with any variables embedded in the message.
Interface(s)	The interface(s) for events triggered by entities external to the device, if applicable.
Description	A brief explanation of the event for the message.
Syslog severity	The syslog severity level associated with the message.

Basic event log messages

Message: <device type>: powered up

Interface (s): N/A

Description: Powered up.

Syslog severity: Warning

Message: <device type>: connection from <client computer IP address> denied due to access failure interface=<interface>

Interface (s): N/A

Description: Connection denied due to access failure.

Syslog severity: Notice

Message: <device type>: connection with <client computer IP address> aborted

Interface (s): N/A

Description: Connection aborted.

Syslog severity: Informational

Message: <device type>: <action>

Interface (s): N/A

Description: Whether the device is performing an action.

Syslog severity: Informational

Variable (s): <action> - Possible values are:

- printing
- plotting
- scanning
- running

Message: <device type>: ready to <action>

Interface (s): N/A

Description: The device is ready to perform an action.

Syslog severity: Informational

Variable (s): <action> - Possible values are:

- print
- plot
- scan
- run

Message: <device type>: not ready to <action>

Interface (s): N/A

Description: The device is not ready to perform an action.

Syslog severity: Informational

Variable (s): <action> - Possible values are:

- print
- plot
- scan
- run

Message: <device type>: offline or intervention needed

Interface (s): N/A

Description: Offline or intervention needed.

Syslog severity: Error

Message: <device type>: paper problem

Interface (s): N/A

Description: Paper problem.

Syslog severity: Error

Message: <device type>: paper out

Interface (s): N/A

Description: Paper out.

Syslog severity: Error

Message: <device type>: paper jam

Interface (s): N/A

Description: Paper jam.

Syslog severity: Error

Message: <device type>: toner/ink low

Interface (s): N/A

Description: Toner/ink low.

Syslog severity: Warning

Message: <device type>: page punt

Interface (s): N/A

Description: Page punt.

Syslog severity: Error

Message: <device type>: memory out

Interface (s): N/A

Description: Memory out.

Syslog severity: Error

Message: <device type>: cover/door open

Interface (s): N/A

Description: Cover/door open.

Syslog severity: Error

Message: <device type>: output full

Interface (s): N/A

Description: Output full.

Syslog severity: Error

Message: <device type>: peripheral fatal error: <error>

Interface (s): N/A

Description: A fatal error of a peripheral occurred.

Syslog severity: Critical

Variable (s): <error> - The error number associated with the peripheral fatal error.

Message: <device type>: network peripheral interface fatal error: <error>

Interface (s): N/A

Description: Network peripheral interface fatal error.

Syslog severity: Critical

Variable (s): <error> - The error number associated with the network peripheral fatal error.

Message: <device type>: interface reconfigured

Interface (s): N/A

Description: Interface reconfigured.

Syslog severity: Informational

Message: <device type>: system name changed

Interface (s): N/A

Description: System name changed.

Syslog severity: Informational

Message: <device type>: peripheral is disconnected

Interface (s): N/A

Description: Peripheral is disconnected.

Syslog severity: Warning

Message: <device type>: syslog started

Interface (s): N/A

Description: Syslog started.

Syslog severity: Debug

Message: <device type>: syslog ended

Interface (s): N/A

Description: Syslog ended.

Syslog severity: Debug

Message: <device type>: configuration change <client computer IP address> interface=<interface>

Interface (s): N/A

Description: Configuration change.

Syslog severity: Informational

Message: <device type>: authentication failed from <client computer IP address> interface=<interface>

Interface (s): N/A

Description: Authentication failed.

Syslog severity: Informational

Message: <device type>: peripheral low-power state

Interface (s): N/A

Description: Peripheral low-power state.

Syslog severity: Informational

Message: <device type>: registered system name <system name> with WINS server <WINS server IP address> interface=<interface>

Interface (s): N/A

Description: Registered system name with WINS server.

Syslog severity: Informational

Message: <device type>: failed to register system name <system name> with primary WINS server <WINS server IP address> interface=<interface>

Interface (s): N/A

Description: Failed to register system name with primary WINS server.

Syslog severity: Warning

Message: <device type>: failed to register system name <system name> with secondary WINS server <WINS server IP address> interface=<interface>

Interface (s): N/A

Description: Failed to register system name with secondary WINS server.

Syslog severity: Warning

Message: <device type>: WINS: unable to change present system name to default system name <system name>, system busy interface=<interface>

Interface (s): N/A

Description: Unable to change the present system name to the default system name.

Syslog severity: Warning

Message: <device type>: WINS: registration successful, inconsistency with JD database and WINS server database. interface=<interface>

Interface (s): N/A

Description: WINS: registration successful, inconsistency with JD database and WINS server database.

Syslog severity: Warning

Message: <device type>: error cleared

Interface (s): N/A

Description: Error cleared.

Syslog severity: Informational

Message: <device type>: IPv6 error: <message> Address: <IPv6 address> interface=<interface>

Interface (s): N/A

Description: An IPv6 error occurred.

Syslog severity: Error

Variable (s): <message> - The message associated with the IPv6 error. Possible values:

- Duplicate Address Detection Failed (LL). Restart the system.
- Duplicate Address Detection Failed (DHCPv6).
- Duplicate Address Detection Failed (Stateless).
- Duplicate Address Detection Failed (Manual).

Message: <device type>: IPv6 warning: Address Cache Overflow. Address: <IPv6 address> interface=<interface>

Interface (s): N/A

Description: An IPv6 address cache overflow occurred.

Syslog severity: Warning

Message: <device type>: Security: Security Configuration modified through the use of <user interface> by <client computer IP address> interface=<interface>

Interface (s): EWS, Control Panel, Telnet

Description: Security configuration modified.

Syslog severity: Informational

Variable (s): <user interface> - Possible values are:

- WebUI
- control panel
- telnet
- push button

Message: <device type>: Device assessment with configuration server failed interface=<interface>

Interface (s): N/A

Description: Device assessment with configuration server failed.

Syslog severity: Informational

Message: <device type>: Security IPsec: enabled on <local device IP address> interface interface=<interface>

Interface (s): EWS, Control Panel

Description: IPsec was enabled.

Syslog severity: Warning

Message: <device type>: Security IPsec: disabled on <local device IP address> interface interface=<interface>

Interface (s): EWS, Control Panel

Description: IPsec was disabled.

Syslog severity: Warning

Message: <device type>: Security: Snmpv3 user account name is created interface=<interface>

Interface (s): EWS, SNMP

Description: SNMPv3 user account name is created.

Syslog severity: Informational

Message: <device type>: Security: Snmpv3 user account name is deleted interface=<interface>

Interface (s): EWS, SNMP

Description: Snmpv3 user account name is deleted.

Syslog severity: Informational

Message: <device type>: Security: Snmpv1/v2 set community name is set interface=<interface>

Interface (s): EWS, SNMP

Description: Snmpv1/v2 set community name is set.

Syslog severity: Informational

Message: <device type>: Security: Snmpv1/v2 set community name is not set interface=<interface>

Interface (s): EWS, SNMP

Description: Snmpv1/v2 set community name is not set.

Syslog severity: Informational

Message: <device type>: Security: Snmpv1/v2 get community name is set interface=<interface>

Interface (s): EWS, SNMP

Description: Snmpv1/v2 get community name is set.

Syslog severity: Informational

Message: <device type>: Security: Snmpv1/v2 get community name is not set interface=<interface>

Interface (s): EWS, SNMP

Description: Snmpv1/v2 get community name is not set.

Syslog severity: Informational

Message: <device type>: Security: Admin password changed interface=<interface>

Interface (s): EWS

Description: Admin password changed.

Syslog severity: Informational

Message: <device type>: Security: New user name is created for 802.1x authentication interface=<interface>

Interface (s): EWS

Description: New user name created for 802.1x authentication.

Syslog severity: Informational

Message: <device type>: Security: CA certificate modified interface=<interface>

Interface (s): EWS

Description: CA certificate modified.

Syslog severity: Informational

Message: <device type>: Security: Jetdirect certificate modified interface=<interface>

Interface (s): EWS

Description: Jetdirect certificate modified.

Syslog severity: Informational

Message: <device type>: Security: Identity certificate installed interface=<interface>

Interface (s): EWS

Description: Identity certificate installed.

Syslog severity: Warning

Message: <device type>: Security: Identity certificate deleted interface=<interface>

Interface (s): EWS

Description: Identity certificate deleted.

Syslog severity: Warning

Message: <device type>: Security: CA certificate installed interface=<interface>

Interface (s): EWS

Description: CA certificate installed.

Syslog severity: Warning

Message: <device type>: Security: CA certificate deleted interface=<interface>

Interface (s): EWS

Description: CA certificate deleted.

Syslog severity: Warning

Message: <device type>: Security: Security settings reset interface=<interface>

Interface (s): EWS, Control Panel

Description: Security settings reset.

Syslog severity: Warning

www.hp.com/support/
Current HP driver, support, and security alerts
delivered directly to your desktop

© Copyright 2025 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Revision 2.0; March 2025