



HP Security Event Logging Messaging Reference

For Interfacing with Security Information and Event Management Systems



HP Security Event Logging Messaging Reference for Interfacing with Security Information and Event Management Systems

Table of contents

1	Introduction.....	2
	Purpose	3
	Configure and enable logging.....	3
	How to open the EWS.....	3
	Configure and enable logging.....	3
2	Enhanced security event logging	5
	Syslog message format.....	6
	Common variables within syslog messages	6
	Syslog messages	7
	Jetdirect logging	7
	Enhanced security event logging	7
	System time	7
	Remote control-panel.....	8
	User authentication	9
	User sign in	9
	EWS sign in	9
	Control panel sign in.....	10
	WS authentication	11
	SNMPv3 authentication.....	11
	Telnet sign in	11
	User sign out	12
	Control panel user sign out.....	12
	EWS user sign out.....	12
	User account logout	12
	Device administrator account logout.....	12
	Remote configuration account logout	13
	SNMPv3 user account logout	13
	HP SureStart.....	14

Whitelisting	15
Connection Inspector	15
Intrusion detection.....	16
Self-tests	17
PJL password verification test.....	17
Timestamp verification test.....	17
Device user access code verification test	17
LDAP settings verification test	18
Windows settings verification test	18
Data integrity test	18
Code integrity test.....	19
Secure erase.....	19
Erase drive.....	19
Erase job data.....	20
IPsec	20
IKEv1 phase 1 negotiations	21
IKEv1 phase 2 negotiations	23
IKEv2 phase 1 negotiations	24
IKEv2 phase 2 negotiations	26
IPsec ESP	27
IPsec AH.....	28
SNMPv3 decryption.....	28
Job completion.....	28
Print	28
Copy	30
Save to Device Memory.....	30
Retrieve from Device Memory	32
Email.....	34
Save to SharePoint.....	34
Save to Network Folder.....	35
Save to HTTP	37
Fax send	38
Analog fax.....	38
PC Fax Send	39
LAN fax.....	39

Internet fax.....	40
Fax receive	41
Fax polling receive	41
Fax forwarding	42
Fax archive	43
Save to USB	44
Retrieve from USB.....	45
Job notification.....	46
Internal reports/tests	47
Back up and restore	49
Backup device data	49
Restore device data	49
Device configuration	50
Syslog.....	50
Jetdirect logging	50
Enhanced security event logging.....	51
Jetdirect security settings factory defaults	52
SNMPv3 user accounts.....	52
Inactivity timeout	53
Account policy	54
Account lockout policy for device administrator account	54
Account lockout policy for remote configuration account.....	56
Account lockout policy for SNMPv3 user accounts	58
Password complexity policy for device administrator password	60
Password complexity policy for remote configuration password	60
Password complexity policy for the SNMPv3 authentication passphrase.....	61
Minimum password length policy for device administrator password	62
Minimum password length policy for remote configuration password	62
Minimum password length policy for SNMPv3 authentication passphrase	63
Date and time settings.....	63
DST settings	63
NTS settings	65
Fax settings	66
Fax archive.....	66
Fax forwarding	66

General security	67
Device administrator password	67
Service access code	68
Remote configuration password	68
Cross-site request forgery (CRSF) prevention	69
EWS session timeout	69
PjL password	70
Firmware upgrade security	70
Bootloader administrator password	71
Drive-lock password	72
File erase mode	72
Access control	72
LDAP Sign In	72
Windows Sign In	80
Device user accounts	84
Default sign-in method for control panel	86
Default sign-in method for EWS	87
Sign-in method assigned to control panel applications	88
Sign-in method assigned to EWS tabs/pages	88
Custom permission sets	89
Permissions associated with permission sets	90
Allow users to choose alternate sign-in methods at the product control panel	91
Default permission set for network users	92
Network user to permission set relationships	92
Network group to permission set relationships	95
Certificates	97
CA certificates	97
Identity certificates	98
Kerberos server certificate validation	100
HP Connection Inspector	101
IPsec/Firewall	106
IPsec/Firewall policy	106
IPsec/Firewall rules	107
IPsec/Firewall address templates	110
IPsec/Firewall service templates	111

IPsec/Firewall advanced options	112
IPsec policy with manual keying	113
IPsec policy with IKEv1	116
IPsec policy with IKEv2	118
IPsec policy with IKEv1 using Kerberos	126
3 Basic logging	128

1 Introduction

- [Purpose](#)
- [Configure and enable logging](#)

Purpose

The purpose of this document is to describe the syslog messages generated for auditable events by HP imaging and printing devices running HP FutureSmart firmware.

The following table describes the structure of this document.

Table 1-1 HP Security Event Logging Messaging Reference for Interfacing with Security Information and Event Management Systems

Chapter	Description
Introduction	This chapter describes the intent and focus of this document, and how to configure and enable logging.
Enhanced security event logging	This chapter describes the syslog messages for enhanced security event logging.
Non-enhanced security event logging	This chapter describes the syslog messages for non-enhanced security event logging.

Configure and enable logging

The steps in this section describe how to configure and enable logging. All steps are performed using the embedded Web server (EWS) running on the device.

How to open the EWS

1. Open a Web browser.
2. 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).

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**.

Configure and enable logging

1. Open the EWS.
2. Click the **Networking** tab.
3. Select the **Other Settings** menu.
4. Click **Misc. Settings** tab.
5. From the **Syslog Facility** drop-down menu, select the syslog facility used by the syslog server to classify syslog messages from imaging and printing devices.




NOTE: The default syslog facility set on the device is LPR.

6. Click **Apply**.
7. Select the **TCP/IP Settings** menu.
8. Click the **Advanced** tab.
9. In the **Syslog Server** field, enter the IPv4 address of the syslog server.

 **NOTE:** Non-enhanced security event logging is enabled when the syslog server address is set.

10. From the **Syslog Protocol** drop-down menu, select the transport protocol used by the syslog server for receiving syslog messages.
11. In the **Syslog Port** field, enter the port number of the port used by the syslog server for receiving syslog messages.
12. 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.

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

 **NOTE:** The **Syslog Priority** setting can be used to filter syslog messages or to disable syslog.

For example; to configure the device to only forward syslog messages with a syslog severity of 5 or lower, set the **Syslog Priority** setting to 5.

Syslog is disabled when the **Syslog Priority** setting is set to 8.

14. Check the **Enhanced security event logging** checkbox.
15. Click **Apply**.

2 Enhanced security event logging

- [Syslog message format](#)
- [Common variables](#)
- [Syslog messages](#)

Syslog message format

The following is the format of syslog messages:

<##> <device type>: <event summary>; <event details>

Example syslog message:

*<134> printer: Device Administrator Password modified; time="2015-Apr-09 11:54 AM (UTC-07:00)"
user="admin" source_IP="10.0.0.7" outcome=success interface=Wired*

The following table describes the syslog message format:

Table 2-1 Syslog message format for enhanced security event logging messages

Item	Description
<i><##></i>	Encoded syslog severity/facility.
<i><device type></i>	Type of device that generated the syslog message. Possible values are: <ul style="list-style-type: none">• printer• scanner
:	Separates <i><device type></i> from the remaining parts of the message.
<i><event summary></i>	Summary of the event.
;	Separates <i><event summary></i> from the remaining parts of the message.
<i><event details></i>	Details of the event. Event details are key-value pairs separated by a single space.

Common variables within syslog messages

Consult the following table for descriptions of variables contained within all syslog message descriptions.

Table 2-2 Common variables contained within log messages

Variable	Description
<i><device type></i>	Type of device that generated the syslog message. Possible values are: <ul style="list-style-type: none">• printer• scanner NOTE: printer is used by both single-function and multifunction printers .
<i><timestamp></i>	Date and time of the event. The format of <i><timestamp></i> is as follows: <i>YYYY-MMM-DD HH:MM PE (UTC TZD)</i> Where: <ul style="list-style-type: none">• 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: 2016-Mar-26 09:10 AM (UTC -07:00)

<*timestamp*> is wrapped in double quotes

NOTE: Modifying the date or time format on the device doesn't modify the format of <*timestamp*>.

Syslog messages

Jetdirect logging

Message:	< <i>device type</i> >: Jetdirect logging started; time="< <i>timestamp</i> >" outcome=success
Interface(s):	N/A
Syslog severity:	Notice
Explanation:	Jetdirect logging was started. This message is generated during system initialization if the syslog server IP address is set, and enhanced security event logging is enabled.
Variables:	< <i>device type</i> > - see Table 2-2 . < <i>timestamp</i> > - see Table 2-2 .

Enhanced security event logging

Message:	< <i>device type</i> >: CCC logging started; time="< <i>timestamp</i> >" outcome=success
Interface(s):	N/A
Syslog severity:	Notice
Explanation:	Enhanced security event logging was started. This message is generated during system initialization if enhanced security event logging is enabled.
Variables:	< <i>device type</i> > - see Table 2-2 . < <i>timestamp</i> > - see Table 2-2 .

System time

Message:	< <i>device type</i> >: System time changed; time="< <i>timestamp</i> >" value="< <i>value</i> >" old_value="< <i>old value</i> >" user="< <i>user</i> >" source_IP="< <i>client computer IP address</i> >" outcome=success
Interface(s):	EWS, WS*, SNMPv3
Syslog severity:	Informational
Explanation:	The system time was modified.
Variables:	< <i>device type</i> > - see Table 2-2 . < <i>timestamp</i> > - see Table 2-2 .

	<value> - New system time.
	<old value> - Old system time.
	<user> - Authenticated user who modified the system time. If an unauthenticated user modified the system time, the user key-value pair is not contained within the message.
	<client computer IP address> - IP address of the client computer that sent the system time modification request.
Message:	<device type>: System time changed; time="<timestamp>" value="<value>" old_value="<old value>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	The system time was modified.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <value> - New system time. <old value> - Old system time. <user> - Authenticated user who modified the system time. If an unauthenticated user modified the system time, the user key-value pair is not contained within the message.
Message:	<device type>: System time changed; time="<timestamp>" value="<value>" old_value="<old vlaue>" source_IP="<NTS IP address>" outcome=success
Interface(s):	NTP
Syslog severity:	Informational
Explanation:	The local device synchronized its system time with the Network Time Server.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <value> - New system time. <old value> - Old system time. <NTS IP address> - IP address of the Network Time Server.

Remote control-panel

Message:	<device type>: Login; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	Remote control-panel session was launched.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who launched the remote control-panel.

	<i><client computer IP address></i> - IP address of the client computer that sent the request to launch the remote control-panel.
Message:	<i><device type></i> : Logout; time=" <i><timestamp></i> " reason= <i><reason></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	Remote control-panel session was ended.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><reason></i> - Reason the session was ended. Possible values are:</p> <ul style="list-style-type: none"> • EndedByUser • EndedByDevice <p><i><user></i> - User who started the remote control-panel session that was ended.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to start the remote control-panel session that was ended.</p>

User authentication

User sign in

EWS sign in

Message:	<i><device type></i> : EWS Sign In Authentication; time=" <i><timestamp></i> " sign-in_method= <i><sign-in method></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A user signed in to the device via the EWS.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><sign-in method></i> - Sign-in method that was used to perform authentication. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents installed on the device.</p> <p><i><user></i> - Authentication database, followed by “\” and the authenticated user identity.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the user authentication request.</p>
Message:	<i><device type></i> : EWS Sign In Authentication; time=" <i><timestamp></i> " sign-in_method= <i><sign-in method></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=failure
Interface(s):	EWS
Syslog severity:	Warning

Explanation:	A user unsuccessfully attempted to sign in to the device via the EWS.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><sign-in method> - Sign-in method that was used to perform authentication. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents installed on the device.</p> <p><user> - Attempted user identity.</p> <p><client computer IP address> - IP address of the client computer that sent the user authentication request.</p>

Control panel sign in

Message:	<device type>: Control Panel Sign In Authentication; time="<timestamp>" sign-in_method= <sign-in method> user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A user signed in to the device at the control panel.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><sign-in method> - Sign-in method that was used to perform authentication. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents installed on the device.</p> <p><user> - Authentication database, followed by “\” and the authenticated user identity.</p>

Message:	<device type>: Control Panel Sign In Authentication; time="<timestamp>" sign-in_method= <sign-in method> user="<user>" outcome=failure
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A user unsuccessfully attempted to sign in to the device at the control panel.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><sign-in method> - Sign-in method that was used to perform authentication. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard

Possible values also include the names of third-party authentication agents installed on the device.

<user> - Attempted user identity.

WS authentication

Message:	<device type>: WS Sign In Authentication; time="<timestamp>" sign-in_method=local_device user="<user>" source_IP="<client computer IP address>" outcome=failure
Interface(s):	WS*, OXPd
Syslog severity:	Warning
Explanation:	HTTP Basic authentication failed. This message is generated when HTTP Basic authentication of an HTTP request containing a WS message fails.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Attempted user identity. <client computer IP address> - IP address of the client computer that sent the HTTP request.

SNMPv3 authentication

Message:	<device type>: SNMPv3 authentication failed; time="<timestamp>" user="SNMPv3\<user>" source_IP="<client computer IP address>" outcome=failure interface=<interface>
Interface(s):	SNMPv3
Syslog severity:	Warning
Explanation:	Authentication of a received SNMPv3 packet failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Attempted SNMPv3 user identity. <client computer IP address> - IP address of the client computer that sent the SNMPv3 request. <interface> - Networking interface on the local device that received the SNMPv3 request. Possible values are: <ul style="list-style-type: none">• Wired• AP• STA

Telnet sign in

Message:	<device type>: Telnet Sign In Authentication; time="<timestamp>" user="Administrator" source_IP="<client computer IP address>" outcome=failure interface=<interface>
Interface(s):	Telnet
Syslog severity:	Warning
Explanation:	A user unsuccessfully attempted to sign in to the device via telnet.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 .

<client computer IP address> - IP address of the client computer that sent the user authentication request.

<interface> - Device networking interface on which the administrator authentication request was received. Possible values are:

- Wired
 - AP
 - STA
-

User sign out

Control panel user sign out

Message:	<device type>: Control Panel session terminated; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	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.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authentication database, followed by "\" and the authenticated user identity. This is the user whose session was ended.

EWS user sign out

Message:	<device type>: EWS session terminated; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	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.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authentication database, followed by "\" and the authenticated user identity. This is the user whose session was ended. <client computer IP address> - IP address of the client computer from which the signed-in user was accessing the EWS.

User account lockout

Device administrator account lockout

Message:	<device type>: Account Entered Lockout Mode; time="<timestamp>" account="Administrator" outcome=success
Interface(s):	EWS, WS, control panel, telnet
Syslog severity:	Informational
Explanation:	The device administrator account was locked.

Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
Message:	<device type>: Account Exited Lockout Mode; time="<timestamp>" account="Administrator" outcome=success
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	The device administrator account was unlocked.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .

Remote configuration account lockout

Message:	<device type>: Account Entered Lockout Mode; time="<timestamp>" account="Administrator" outcome=success
Interface(s):	WS
Syslog severity:	Informational
Explanation:	The remote configuration account was locked.
	NOTE: Though the message generated contains the account "Administrator," the account that was locked is the remote configuration account.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
Message:	<device type>: Account Exited Lockout Mode; time="<timestamp>" account="Administrator" outcome=success
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	The remote configuration account was unlocked.
	NOTE: Though the message generated contains the account "Administrator," the account that was unlocked is the remote configuration account.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .

SNMPv3 user account lockout

Message:	<device type>: SNMPv3 authentication entered protected mode; time="<timestamp>" SNMPv3_user_account="<user account>" outcome=success interface="<interface>"
Interface(s):	SNMPv3
Syslog severity:	Warning
Explanation:	An SNMPv3 user account was locked.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user account> - SNMPv3 user account that was locked.
	<interface> - Networking interface on the local device. Possible values are:
	<ul style="list-style-type: none"> Wired

	<ul style="list-style-type: none"> • AP • STA
Message:	<i><device type></i> : SNMPv3 authentication exited protected mode; time=" <i><timestamp></i> " SNMPv3_user_account=" <i><user account></i> " outcome=success interface= <i><interface></i>
Interface(s):	SNMPv3
Syslog severity:	Warning
Explanation:	An SNMPv3 user account was unlocked.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user account></i> - SNMPv3 user account that was unlocked. <i><interface></i> - Networking interface on the local device. Possible values are: <ul style="list-style-type: none"> • Wired • AP • STA

HP SureStart

Message:	<i><device type></i> : Boot code corrupt; time=" <i><timestamp></i> " source_IP=" <i><local device IP address></i> "
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	The device detected and recovered from a corrupted/tampered version of BIOS.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><local device IP address></i> - IP address of the local device.
Message:	<i><device type></i> : Upgrade corrupt; time=" <i><timestamp></i> " source_IP=" <i><local device IP address></i> "
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	Cryptographic validation of newly downloaded firmware failed.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><local device IP address></i> - IP address of the local device.
Message:	<i><device type></i> : Invalid boot attempt; time=" <i><timestamp></i> " source_IP=" <i><local device IP address></i> "
	<i><device type></i> : Downgrade attempted; time=" <i><timestamp></i> " source_IP=" <i><local device IP address></i> "
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	A downgrade to firmware that doesn't contain the SureStart feature was attempted. The two messages above are generated when a downgrade to firmware that doesn't contain the SureStart feature was attempted.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 .

	<local device IP address> - IP address of the local device.
Message:	<device type>: Unproven Installer; time= <timestamp> source_IP=" <local device IP address>"
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	The newly downloaded firmware failed to cryptographically validate the BIOS code.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<local device IP address> - IP address of the local device.

Whitelisting

Message:	<device type>: Code sign error; time=" <timestamp>" source_IP=" <local device IP address>"
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	Validation of a system firmware file during the load process using digital signature failed.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<local device IP address> - IP address of the local device.

Connection Inspector

Message:	<device type>: Potential intrusion. HP Connection Inspector event detected. time=" <timestamp>" source_IP=" <local device IP address>"
Interface(s):	N/A
Syslog severity:	Error
Explanation:	HP Connection Inspector detected a potential intrusion.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<local device IP address> - IP address of the local device.
Message:	<device type>: HP Connection Inspector event; time=" <timestamp>" event= protected_mode_exited outcome=success
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	HP Connection Inspector feature has exited protected mode.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
Message:	<device type>: HP Connection Inspector event; time=" <timestamp>" event= protected_mode_entered outcome=success
Interface(s):	N/A
Syslog severity:	Warning

Explanation:	HP Connection Inspector feature has entered protected mode.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 .
Message:	<device type>: HP Connection Inspector event; time="<timestamp>" event= dns_query value="<host name>" outcome=failure
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	HP Connection Inspector feature has detected dns query failure for a hostname.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <host name> - Host name whose DNS lookup failed.

Intrusion detection

Message:	<device type>: Potential intrusion. Memory corruption detected.; time="<timestamp>" source_IP="<local device IP address>"
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	Memory corruption was detected. NOTE: Corruption of memory could be indicative of injection of malware.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <local device IP address> - IP address of the local device.
Message:	<device type>: Intrusion detection disabled. Unable to scan for memory corruption.; time="<timestamp>" source_IP="<local device IP address>"
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	The intrusion detection algorithm was disabled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <local device IP address> - IP address of the local device.
Message:	<device type>: Failed to initialize intrusion detection.; time="<timestamp>" source_IP="<local IP address>"
Interface(s):	N/A
Syslog severity:	Alert
Explanation:	Initialization of the intrusion detection functionality failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <local device IP address> - IP address of the local device.

Self-tests

PJL password verification test

Message:	<i><device type></i> : PJL Password Integrity Test; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome= <i><test result></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The PJL password verification test was performed.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><client computer IP address></i> - IP address of the client computer that sent the request to perform the PJL password verification test. <i><test result></i> - Result of the test. Possible values are: <ul style="list-style-type: none">• success• failure

Timestamp verification test

Message:	<i><device type></i> : Timestamp Verification Integrity Test; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome= <i><test result></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The timestamp verification test was performed.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><client computer IP address></i> - IP address of the client computer that sent the request to perform the test. <i><test result></i> - Result of the test. Possible values are: <ul style="list-style-type: none">• success• failure

Device user access code verification test

Message:	<i><device type></i> : Device User Integrity Test; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome= <i><test result></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The device user access code verification test was performed.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><client computer IP address></i> - IP address of the client computer that sent the request to perform the device user access code verification test. <i><test result></i> - Result of the test. Possible values are: <ul style="list-style-type: none">• success• failure

LDAP settings verification test

Message:	<i><device type></i> : LDAP Integrity Test; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome= <i><test result></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The LDAP settings verification test was performed.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><client computer IP address></i> - IP address of the client computer that sent the request to perform the LDAP settings verification test. <i><test result></i> - Result of the test. Possible values are: <ul style="list-style-type: none">• success• failure

Windows settings verification test

Message:	<i><device type></i> : Windows Integrity Test; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome= <i><test result></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The Windows settings verification test was performed.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><client computer IP address></i> - IP address of the client computer that sent the request to perform the Windows settings verification test. <i><test result></i> - Result of the test. Possible values are: <ul style="list-style-type: none">• success• failure

Data integrity test

Message:	<i><device type></i> : Generated CRC for Data Integrity Check; time=" <i><timestamp></i> " reference_point=" <i><reference point></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A point of reference for the data integrity test was set.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><reference point></i> - Date and time of the CRC checksum creation plus the CRC checksum. Example: 3/23/2016 12:25:22 PM (8D-9A-72-9C) <i><client computer IP address></i> - IP address of the client computer that sent the request to set a reference point.
Message:	<i><device type></i> : Verify CRC for Data Integrity Check; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome= <i><test result></i>
Interface(s):	EWS

Syslog severity:	Informational
Explanation:	The data integrity test was performed.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to perform the data integrity test.</p> <p><i><test result></i> - Result of the test. Possible values are:</p> <ul style="list-style-type: none"> • success • failure

Code integrity test

Message:	<i><device type></i> : Generate CRC for Code Integrity Check; time=" <i><timestamp></i> " reference_point=" <i><reference point></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A point of reference for the code integrity test was set.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><reference point></i> - Date and time of the CRC checksum creation plus the CRC checksum. Example: 3/23/2016 12:25:22 PM (8D-9A-72-9C)</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to set a reference point.</p>
Message:	<i><device type></i> : Verify CRC for Code Integrity Check; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome= <i><test result></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The code integrity test was performed.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to perform the code integrity test.</p> <p><i><test result></i> - Result of the test. Possible values are:</p> <ul style="list-style-type: none"> • success • failure

Secure erase

Erase drive

Message:	<i><device type></i> : Erase Drive requested; time=" <i><timestamp></i> " erase_mode= <i><mode></i> drive_name=" <i><drive name></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A request to erase a storage drive was made.

Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><mode> - Erase mode to erase the storage drive. Possible values are:</p> <ul style="list-style-type: none"> • secure_cryptographic_erase • unknown <p><drive name> - Name of the storage drive to be erased.</p> <p><client computer IP address> - IP address of the client computer that sent the request to erase the storage drive.</p>
-------------------	---

Erase job data

Message:	<device type>: Erase Job Data requested; time="<timestamp>" erase_mode= <mode> source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A request to erase the job data on the storage drives installed on the device was made.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><mode> - Erase mode to erase the job data. Possible values are:</p> <ul style="list-style-type: none"> • non_secure_fast_erase • secure_fast_erase • secure_sanitize_erase <p><client computer IP address> - IP address of the client computer that sent the request to erase the job data.</p>

IPsec

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

Table 2-3 <reason for failure> variable contained within messages generated for unsuccessful IKE negotiations

Variable	Description
<reason for failure>	<p>Reason IKE negotiations failed. Possible values are:</p> <ul style="list-style-type: none"> • 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_Informationalrmtion_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

Table 2-3 *<reason for failure>* variable contained within messages generated for unsuccessful IKE negotiations

Variable	Description
	<ul style="list-style-type: none"> • 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 negotiations

Message:	<p><i><device type></i>: IPsec IKEv1 phase 1 negotiation; time=" <i><timestamp></i>" authentication_option= <i><authentication option></i> item=printer_role value=Responder source_IP=" <i><IPsec peer IP address></i>" destination_IP=" <i><local device IP address></i>" outcome=success</p>
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv1 phase 1 negotiations initiated by the IPsec peer were successful.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><authentication option></i> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication. Possible values are:</p> <ul style="list-style-type: none"> • Certificates • Pre-shared_key • Kerberos

<p>NOTE: If both the local device and the IPsec peer used Kerberos to perform mutual authentication, this message is not generated.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p> <p><local device IP address> - IP address of the local device.</p>	
Message:	<device type>: IPsec IKEv1 phase 1 negotiation; time=" <timestamp>" item=printer_role value=Responder source_IP=" <IPsec peer IP address>" destination_IP=" <local device IP address>" outcome=failure Reason= <reason for failure>
Interface(s):	IPsec
Recommended SIEM severity:	
Syslog severity:	Warning
Explanation:	IKEv1 phase 1 negotiations initiated by the IPsec peer failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p> <p><local device IP address> - IP address of the local device.</p> <p><reason for failure> - see Table 2-3.</p>
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>" destination_IP=" <IPsec peer IP address>" outcome=success
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv1 phase 1 negotiations initiated by the local device were successful.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><authentication option> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication. Possible values are:</p> <ul style="list-style-type: none"> • Certificates • Pre-shared_key • Kerberos <p>NOTE: If both the local device and the IPsec peer used Kerberos to perform mutual authentication, this message is not generated.</p> <p><local device IP address> - IP address of the local device.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p>
Message:	<device type>: IPsec IKEv1 phase 1 negotiation; time=" <timestamp>" item=printer_role value=Initiator source_IP=" <local device IP address>" destination_IP=" <IPsec peer IP address>" outcome=failure Reason= <reason for failure>
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv1 phase 1 negotiations initiated by the local device failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

<local device IP address> - IP address of the local device.

<IPsec peer IP address> - IP address of the IPsec peer.

<reason for failure> - see [Table 2-3](#).

IKEv1 phase 2 negotiations

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>" destination_IP=" <local device IP address>" outcome=success
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv1 phase 2 negotiations initiated by the IPsec peer were successful.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><authentication option> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication during IKEv1 phase 1 negotiations. Possible values are:</p> <ul style="list-style-type: none">• Certificates• Pre-shared_key• Kerberos <p>NOTE: If both the local device and the IPsec peer used Kerberos to perform mutual authentication, this message is not generated.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p> <p><local device IP address> - IP address of the local device.</p>
Message:	<device type>: IPsec IKEv1 phase 2 negotiation; time=" <timestamp>" item=printer_role value=Responder source_IP=" <IPsec peer IP address>" destination_IP=" <local device IP address>" outcome=failure Reason= <reason for failure>
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv1 phase 2 negotiations initiated by the IPsec peer failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p> <p><local device IP address> - IP address of the local device.</p> <p><reason for failure> - see Table 2-3.</p>
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>" destination_IP=" <IPsec peer IP address>" outcome=success
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv1 phase 2 negotiations initiated by the local device were successful.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<authentication option> - Authentication method that was used by both the local device and the IPsec peer to perform mutual authentication during IKEv1 phase 1 negotiations. Possible values are:

- Certificates
- Pre-shared_key
- Kerberos

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

<local device IP address> - IP address of the local device.

<IPsec peer IP address> - IP address of the IPsec peer.

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

Interface(s):	IPsec
----------------------	-------

Syslog severity:	Warning
-------------------------	---------

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

Variables:	<device type> - see Table 2-2 .
-------------------	---

<timestamp> - see [Table 2-2](#).

<local device IP address> - IP address of the local device.

<IPsec peer IP address> - IP address of the IPsec peer.

<reason for failure> - see [Table 2-3](#).

IKEv2 phase 1 negotiations

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>" destination_IP=" <local device IP address>" outcome=success
-----------------	--

Interface(s):	IPsec
----------------------	-------

Syslog severity:	Warning
-------------------------	---------

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

Variables:	<device type> - see Table 2-2 .
-------------------	---

<timestamp> - see [Table 2-2](#).

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

- Certificate
- Pre-Shared_Key

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

- Certificate
- 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.

	<IPsec peer IP address> - IP address of the IPsec peer.
	<local device IP address> - IP address of the local device.
Message:	<device type>: IPsec IKEv2 phase 1 negotiation; time=" <timestamp>" item=printer_role value=Responder source_IP=" <IPsec peer IP address>" destination_IP=" <local device IP address>" outcome=failure Reason= <reason for failure>
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv2 phase 1 negotiations initiated by the IPsec peer failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <IPsec peer IP address> - IP address of the IPsec peer. <local device IP address> - IP address of the local device. <reason for failure> - see Table 2-3 .
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>" destination_IP=" <IPsec peer IP address>" outcome=success
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv2 phase 1 negotiations initiated by the local device were successful.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <local authentication option> - Authentication method that was used by the IPsec peer to authenticate the local device. Possible values are: <ul style="list-style-type: none"> • Certificate • Pre-Shared_Key <remote authentication option> - Authentication method that was used by the local device to authenticate the IPsec peer. Possible values are: <ul style="list-style-type: none"> • Certificate • 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. <local device IP address> - IP address of the local device. <IPsec peer IP address> - IP address of the IPsec peer.
Message:	<device type>: IPsec IKEv2 phase 1 negotiation; time=" <timestamp>" item=printer_role value=Initiator source_IP=" <local device IP address>" destination_IP=" <IPsec peer IP address>" outcome=failure Reason= <reason for failure>
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv2 phase 1 negotiations initiated by the local device failed.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<local device IP address> - IP address of the local device.

<IPsec peer IP address> - IP address of the IPsec peer.

<reason for failure> - see [Table 2-3](#).

IKEv2 phase 2 negotiations

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>" destination_IP=" <local device IP address>" outcome=success
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv2 phase 2 negotiations initiated by the IPsec peer were successful.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <local authentication option> - Authentication method that was used by the IPsec peer to authenticate the local device during IKEv2 phase 1 negotiations. Possible values are: <ul style="list-style-type: none">• Certificate• Pre-Shared_Key <remote authentication option> - Authentication method that was used by the local device to authenticate the IPsec peer during IKEv2 phase 1 negotiations. Possible values are: <ul style="list-style-type: none">• Certificate• Pre-Shared_Key NOTE: If both the local device and the IPsec peer used pre-shared key to perform mutual authentication during IKEv2 phase 1 negotiations, this message is not generated. <IPsec peer IP address> - IP address of the IPsec peer. <local device IP address> - IP address of the local device.

Message:	<device type>: IPsec IKEv2 phase 2 negotiation; time=" <timestamp>" item=printer_role value=Responder source_IP=" <IPsec peer IP address>" destination_IP=" <local device IP address>" outcome=failure Reason=" <reason for failure>
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv2 phase 2 negotiations initiated by the IPsec peer failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <IPsec peer IP address> - IP address of the IPsec peer. <local device IP address> - IP address of the local device. <reason for failure> - see Table 2-3 .

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>" destination_IP="<IPsec peer IP address>" outcome=success
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv2 phase 2 negotiations initiated by the local device were successful.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><local authentication option> - Authentication method that was used by the IPsec peer to authenticate the local device during IKEv2 phase 1 negotiations. Possible values are:</p> <ul style="list-style-type: none"> • Certificate • Pre-Shared_Key <p><remote authentication option> - Authentication method that was used by the local device to authenticate the IPsec peer during IKEv2 phase 1 negotiations. Possible values are:</p> <ul style="list-style-type: none"> • Certificate • Pre-Shared_Key <p>NOTE: If both the local device and the IPsec peer used pre-shared key to perform mutual authentication during IKEv2 phase 1 negotiations, this message is not generated.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p> <p><local device IP address> - IP address of the local device.</p>
Message:	<device type>: IPsec IKEv2 phase 2 negotiation; time="<timestamp>" item=printer_role value=Initiator source_IP="<local device IP address>" destination_IP="<IPsec peer IP address>" outcome=failure Reason=<reason for failure>
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	IKEv2 phase 2 negotiations initiated by the local device failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><local device IP address> - IP address of the local device.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p> <p><reason for failure> - see Table 2-3.</p>

IPsec ESP

Message:	<device type>: IPsec using ESP failed; time="<timestamp>" source_IP="<IPsec peer IP address>" destination_IP="<local device IP address>" outcome=failure
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	The processing of a received IPsec ESP packet failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><IPsec peer IP address> - IP address of the IPsec peer.</p> <p><local device IP address> - IP address of the local device.</p>

IPsec AH

Message:	<device type>: IPsec using AH failed; time="<timestamp>" source_IP="<IPsec peer IP address>" destination_IP="<local device IP address>" outcome=failure
Interface(s):	IPsec
Syslog severity:	Warning
Explanation:	The processing of a received IPsec AH packet failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <IPsec peer IP address> - IP address of the IPsec peer. <local device IP address> - IP address of the local device.

SNMPv3 decryption

Message:	<device type>: SNMPv3 decryption failed; time="<timestamp>" user="SNMPv3\<user>" source_IP="<client computer IP address>" outcome=failure interface="<interface>"
Interface(s):	SNMPv3
Syslog severity:	Warning
Explanation:	The decryption of a received SNMPv3 packet failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Username specified within the SNMPv3 packet. <client computer IP address> - IP address of the client computer. <interface> - Networking interface on the local device that received the SNMPv3 request.

Job completion

Print

Message:	<device type>: Print job completion; time="<timestamp>" job_name="<job name>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	9100, WS Print, IPP, LPD, FTP
Syslog severity:	Informational
Explanation:	A print driver job was printed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <job name> - Value of the PJO JOBNAME attribute. This value is specified in the print job stream by the print driver at job creation time. <user> - The value of the job attribute JobAcct3, followed by "\" and the value of the job attribute JobAcct8. JobAcct3 specifies the domain name, and JobAcct8 specifies the username. JobAcct3 and JobAcc8 are specified by setting the PJO JOBATTR variable in the print job. JobAcct3 and JobAcc8 are specified in the print job stream by the print driver at job creation time.

	<p>If JobAcct3 and JobAcc8 are missing in the print job stream, the value of <code><user></code> is "Guest."</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the print driver job.</p>
Message:	<code><device type></code> : Print job completion; time=" <code><timestamp></code> " job_name=" <code><job name></code> " user=" <code><user></code> " source_IP=" <code><client computer IP address></code> " outcome=canceled
Interface(s):	9100, WS Print, IPP, LPD, FTP
Syslog severity:	Informational
Explanation:	The printing of a print driver job was canceled.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><job name></code> - Value of the PJI JOBNAME attribute that was specified in the print job. This value is specified in the print job stream by the print driver at job creation time.</p> <p><code><user></code> - The value of the job attribute JobAcct3, followed by "\" and the value of the job attribute JobAcct8.</p> <p>JobAcct3 specifies the domain name, and JobAcct8 specifies the username.</p> <p>JobAcct3 and JobAcc8 are specified by setting the PJI JOBATTR variable in the print job.</p> <p>JobAcct3 and JobAcc8 are specified in the print job stream by the print driver at job creation time.</p> <p>If JobAcct3 and JobAcc8 are missing in the print job stream, the value of <code><user></code> is "Guest."</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the print driver job.</p>
Message:	<code><device type></code> : Print job completion; time=" <code><timestamp></code> " job_name=" <code><job name></code> " user=" <code><user></code> " source_IP=" <code><client computer IP address></code> " outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A print-ready file (.txt, .ps, .pdf, .pcl, .cht, .prn, .tiff, .tif) was printed.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><job name></code> - Name of the job.</p> <p><code><user></code> - User who submitted print-ready file for printing.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the print-ready file.</p>
Message:	<code><device type></code> : Print job completion; time=" <code><timestamp></code> " job_name=" <code><job name></code> " user=" <code><user></code> " source_IP=" <code><client computer IP address></code> " outcome=canceled
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The printing of a print-ready file (.txt, .ps, .pdf, .pcl, .cht, .prn, .tiff, .tif) was canceled.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><job name></code> - Name of the job.</p> <p><code><user></code> - User who submitted the print-ready file for printing.</p>

Copy

<client computer IP address> - IP address of the client computer that sent the print-ready file.

Message:	<device type>: Copy job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A copy job was completed successfully.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the copy job.</p>
Message:	<device type>: Copy job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A copy job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the copy job.</p>

Save to Device Memory

Message:	<device type>: Print and Save to Device Memory job completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	9100, WS-Print, IPP, LPD, FTP, EWS
Syslog severity:	Informational
Explanation:	A non-encrypted printer driver job was printed and stored.
	This message is generated when either a Proof and Hold or Quick Copy job is stored on the device.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - The value of the job attribute JobAcct3, followed by "\ " and the value of the job attribute JobAcct8.</p> <p>JobAcct3 specifies the domain name, and JobAcct8 specifies the username.</p> <p>JobAcct3 and JobAcc8 are specified by setting the PJI JOBATTR variable in the print job.</p> <p>JobAcct3 and JobAcc8 are specified in the print job stream by the print driver at job creation time.</p> <p>If JobAcct3 and JobAcc8 are missing in the print job stream, the value of <user> is "Guest."</p> <p><client computer IP address> - IP address of the client computer that sent the print driver job.</p>
Message:	<device type>: Save to Device Memory job completion; time="<timestamp>" job_type=print user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	9100, WS Print, IPP, LPD, FTP, EWS
Syslog severity:	Informational

Explanation:	A non-encrypted printer driver job was stored.
Variables:	<p>This message is generated when either a Personal Job or Stored Job is stored on the device.</p> <p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - The value of the job attribute JobAcct3 plus “\” plus the value of the job attribute JobAcct8.</p> <p>JobAcct3 specifies the domain name, and JobAcct8 specifies the username.</p> <p>JobAcct3 and JobAcc8 were specified by setting the PJI JOBATTR variable in the print job.</p> <p>If JobAcct3 and JobAcc8 are not specified in the print job, the value of <user> is “Guest.”</p> <p><client computer IP address> - IP address of the client computer that sent the print driver job.</p>
Message:	<device type>: Save to Device Memory job completion; time="<timestamp>" job_type=print user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	9100, WS Print, IPP, LPD, FTP
Syslog severity:	Informational
Explanation:	An encrypted print driver job (Personal Job or Stored Job) was stored.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - The value of the job attribute JobAcct3, followed by “\” and the value of the job attribute JobAcct8.</p> <p>JobAcct3 specifies the domain name, and JobAcct8 specifies the username.</p> <p>JobAcct3 and JobAcc8 are specified by setting the PJI JOBATTR variable in the print job.</p> <p>JobAcct3 and JobAcc8 are specified in the print job stream by the print driver at job creation time.</p> <p>If JobAcct3 and JobAcc8 are missing in the print job stream, the value of <user> is “Guest.”</p> <p><client computer IP address> - IP address of the client computer that sent the print driver job.</p>
Message:	<device type>: Save to Device Memory job completion; time="<timestamp>" job_type=copy user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A copy job was stored.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the storing of the copy job.</p>
Message:	<device type>: Save to Device Memory job completion; time="<timestamp>" job_type=copy user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	The storing of a copy job was canceled.

Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the storing of the copy job.</p>
Message:	<device type>: Save to Device Memory job completion; time=" <timestamp>" job_type=fax user="Guest" outcome=success
Interface(s):	Analog fax
Syslog severity:	Informational
Explanation:	A received fax was stored.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>
Message:	<device type>: Save to Device Memory job completion; time=" <timestamp>" job_type=fax user="Guest" outcome=canceled
Interface(s):	Analog fax
Syslog severity:	Informational
Explanation:	The storing of a received fax was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

Retrieve from Device Memory

Message:	<device type>: Retrieve from Device Memory job completion; time=" <timestamp>" job_type= <job type> user=" <user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A stored job was retrieved and printed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><job type> - Type of stored job. Possible values are:</p> <ul style="list-style-type: none"> • copy • print • fax <p><user> - User who initiated the retrieval and printing of the stored job.</p>
Message:	<device type>: Retrieve from Device Memory job completion; time=" <timestamp>" job_type= <job type> user=" <user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	The retrieval and printing of stored job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><job type> - Type of stored job. Possible values are:</p> <ul style="list-style-type: none"> • copy • print

	<ul style="list-style-type: none"> • fax
	<user> - User who initiated the retrieval and printing of the stored job.
Message:	<device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=<job type> user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	WS*, SNMP
Syslog severity:	Informational
Explanation:	A non-encrypted stored print job or stored copy was retrieved and printed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <job type> - Type of stored job. Possible values are: <ul style="list-style-type: none"> • copy • print <user> - User who initiated the retrieval and printing of the job. <client computer IP address> - IP address of the client computer that sent the request to retrieve and print the stored job.
Message:	<device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=<job type> user="<user>" source_IP="<client computer IP address>" outcome=canceled
Interface(s):	WS*, SNMP
Syslog severity:	Warning
Explanation:	The retrieval and printing of a non-encrypted stored print job or stored copy job was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <job type> - Type of stored job. Possible values are: <ul style="list-style-type: none"> • copy • print <user> - User who initiated the retrieval and printing of the job. <client computer IP address> - IP address of the client computer that sent the request to retrieve and print the stored job.
Message:	<device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=fax user="Guest" outcome=success
Interface(s):	Control panel, EWS, WS*
Syslog severity:	Informational
Explanation:	A stored fax was retrieved and printed per the fax printing schedule.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 .
Message:	<device type>: Retrieve from Device Memory job completion; time="<timestamp>" job_type=fax user="Guest" outcome=canceled
Interface(s):	Control panel, EWS, WS*
Syslog severity:	Informational
Explanation:	The retrieval and printing of a stored fax per the fax printing schedule was canceled.

Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .

Email

Message:	<device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	An email was sent to all recipients successfully.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - User who initiated the email.

Message:	<device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	An email was canceled.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - User who initiated the email.

Message:	<device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=partial_success
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	An email addressed to two or more recipients was sent successfully to at least one recipient but not to all recipients.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - User who initiated the email.

Message:	<device type>: E-mail job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	The processing of an email failed.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - User who initiated the email.

Save to SharePoint

Message:	<device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel

Syslog severity:	Informational
Explanation:	A Save to SharePoint job was completed successfully.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the Save to SharePoint job.</p>
Message:	<device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A Save to SharePoint job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the Save to SharePoint job.</p>
Message:	<device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=partial_success
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	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.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the Save to SharePoint job.</p>
Message:	<device type>: Save to SharePoint job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A Save to SharePoint job failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the Save to SharePoint job.</p>

Save to Network Folder

Message:	<device type>: Save to Network Folder job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control Panel
Syslog severity:	Informational
Explanation:	A Save to Network Folder job was completed successfully.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

<user> - User who initiated the Save to Network Folder job.	
Message:	<device type>: Save to Network Folder job completion; time=" <timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A Save to Network Folder job was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the Save to Network Folder job.
Message:	<device type>: Save to Network Folder job completion; time=" <timestamp>" user="<user>" outcome=partial_success
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	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.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the Save to Network Folder job.
Message:	<device type>: Save to Network Folder job completion; time=" <timestamp>" user="<user>" outcome=failure
Interface(s):	Control Panel
Syslog severity:	Warning
Explanation:	A Save to Network Folder job failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the Save to Network Folder job.
Message:	<device type>: Save to Network Folder job completion; time=" <timestamp>" user="<user>" source_IP=" <client computer IP address>" outcome=success
Interface(s):	OXPD
Syslog severity:	Informational
Explanation:	A Save to Network Folder job was completed successfully.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Control panel user. <client computer IP address> - IP address of the client computer that sent the request to perform the Save to Network Folder job.
Message:	<device type>: Save to Network Folder job completion; time=" <timestamp>" user="<user>" source_IP=" <client computer IP address>" outcome=canceled

Interface(s):	XPd
Syslog severity:	Warning
Explanation:	A Save to Network Folder job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Control panel user.</p> <p><client computer IP address> - IP address of the client computer that sent the request to perform the Save to Network Folder job.</p>
Message:	<device type>: Save to Network Folder job completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=failure
Interface(s):	XPd
Syslog severity:	Warning
Explanation:	A Save to Network Folder job failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Control panel user.</p> <p><client computer IP address> - IP address of the client computer that sent the request to perform the Save to Network Folder job.</p>

Save to HTTP

Message:	<device type>: Save to HTTP job completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	XPd
Syslog severity:	Informational
Explanation:	A Save to HTTP job was completed successfully.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Control panel user.</p> <p><client computer IP address> - IP address of the client computer that sent the request to perform the Save to HTTP job.</p>
Message:	<device type>: Save to HTTP job completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=canceled
Interface(s):	XPd
Syslog severity:	Warning
Explanation:	A Save to HTTP job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Control panel user.</p> <p><client computer IP address> - IP address of the client computer that sent the request to perform the Save to HTTP job.</p>

Message:	<device type>: Save to HTTP job completion; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=failure
Interface(s):	OXPD
Syslog severity:	Warning
Explanation:	A Save to HTTP job failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Control panel user. <client computer IP address> - IP address of the client computer that sent the request to perform the Save to HTTP job.

Fax send

Analog fax

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A fax send job was completed successfully.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the fax send job.

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A fax send job was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the fax send job.

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=partial_success
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A fax send job addressed to multiple fax destinations was sent successfully to at least one fax destination but not to all fax destinations.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the fax send job.

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control Panel

Syslog severity:	Warning
Explanation:	A fax send job failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the fax send job.</p>

PC Fax Send

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	9100
Syslog severity:	Informational
Explanation:	A PC Fax Send job was completed successfully.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Username embedded in the job stream by the HP PC Fax Send Driver at job creation time.</p>

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	9100
Syslog severity:	Warning
Explanation:	A PC Fax Send Job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Username embedded in the job stream by the HP PC Fax Send Driver at job creation time.</p>

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	9100
Syslog severity:	Warning
Explanation:	A PC Fax Send job failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Username embedded in the job stream by the HP PC Fax Send Driver at job creation time.</p>

LAN fax

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A LAN fax job was completed successfully.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the LAN fax job.</p>

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

Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A LAN fax job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the LAN fax job.</p>
Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A LAN fax job failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the LAN fax job.</p>

Internet fax

Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	An Internet fax job was completed successfully.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the Internet fax job.</p>
Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	An Internet fax job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the Internet fax job.</p>
Message:	<device type>: Send Fax job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control Panel
Syslog severity:	Warning
Explanation:	An Internet fax job failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the Internet fax job.</p>

Fax receive

Message:	<device type>: Receive Fax job completion; time="<timestamp>" user="Guest" outcome=success
Interface(s):	Analog fax
Syslog severity:	Informational
Explanation:	An analog fax was received and printed.
Variables:	<device type> - see Table 2-2. <timestamp> - see Table 2-2.
Message:	<device type>: Receive Fax job completion; time="<timestamp>" user="Guest" outcome=canceled
Interface(s):	Analog fax
Syslog severity:	Warning
Explanation:	An incoming analog fax was canceled.
Variables:	<device type> - see Table 2-2. <timestamp> - see Table 2-2.
Message:	<device type>: Receive Fax job completion; time="<timestamp>" user="Guest" outcome=partial_success
Interface(s):	Analog fax
Syslog severity:	Warning
Explanation:	At least one page of a multipage incoming analog fax was printed before the fax transmission was interrupted.
Variables:	<device type> - see Table 2-2. <timestamp> - see Table 2-2.
Message:	<device type>: Receive Fax job completion; time="<timestamp>" user="Guest" outcome=failure
Interface(s):	Analog fax
Syslog severity:	Warning
Explanation:	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.
Variables:	<device type> - see Table 2-2. <timestamp> - see Table 2-2.

Fax polling receive

Message:	<device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A fax polling receive job was completed successfully.
Variables:	<device type> - see Table 2-2. <timestamp> - see Table 2-2. <user> - User who initiated the fax polling receive job.
Message:	<device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=canceled

Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A fax polling receive job was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the fax polling receive job.</p>
Message:	<device type>: Receive Fax job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A fax polling receive job failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who initiated the fax polling receive job.</p>

Fax forwarding

Message:	<device type>: Fax Forwarding job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	A received or sent fax was forwarded to one or more fax numbers.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - For the forwarding of a received fax, the value of this variable is "Guest." For the forwarding of a sent fax, the value of this variable is the user who initiated the fax send job at the control panel.</p>
Message:	<device type>: Fax Forwarding job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	The forwarding of a received or sent fax was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - For the forwarding of a received fax, the value of this variable is "Guest." For the forwarding of a sent fax, the value of this variable is the user who initiated the fax send job at the control panel.</p>
Message:	<device type>: Fax Forwarding job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	The forwarding of a received or sent fax failed.

Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - For the forwarding of a received fax, the value of this variable is "Guest." For the forwarding of a sent fax, the value of this variable is the user who initiated the fax send job at the control panel.</p>
-------------------	--

Fax archive

Message:	<device type>: Fax Archive job completion; time="<timestamp>" job_type=sent_fax destination_type=<destination type> user="<user>" outcome=success
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	A sent fax was archived.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><destination type> - Archival destination type. Possible values are:</p> <ul style="list-style-type: none"> • e-mail • network_folder • ftp_server <p><user> - User who initiated the fax send job that was archived.</p>

Message:	<device type>: Fax Archive job completion; time="<timestamp>" job_type=sent_fax destination_type=<destination type> user="<user>" outcome=canceled
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	The archival of a sent fax was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><destination type> - Archival destination type. Possible values are:</p> <ul style="list-style-type: none"> • e-mail • network_folder • ftp_server <p><user> - User who initiated the fax send job that was to be archived.</p>

Message:	<device type>: Fax Archive job completion; time="<timestamp>" job_type=sent_fax destination_type=<destination type> user="<user>" outcome=failure
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	The archival of a sent fax failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><destination type> - Archival destination type. Possible values are:</p> <ul style="list-style-type: none"> • e-mail • network_folder • ftp_server

	<user> - User who initiated the fax send job that was to be archived.
Message:	<device type>: Fax Archive job completion; time="<timestamp>" job_type=received_fax destination_type= <destination type> outcome=success
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	A received fax was archived.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <destination type> - Archival destination type. Possible values are: <ul style="list-style-type: none"> • e-mail • network_folder • ftp_server
Message:	<device type>: Fax Archive job completion; time="<timestamp>" job_type=received_fax destination_type= <destination type> outcome=canceled
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	The archival of a received fax was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <destination type> - Archival destination type. Possible values are: <ul style="list-style-type: none"> • e-mail • network_folder • ftp_server
Message:	<device type>: Fax Archive job completion; time="<timestamp>" job_type=received_fax destination_type= <destination type> outcome=failure
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	The archival of a received fax failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <destination type> - Archival destination type. Possible values are: <ul style="list-style-type: none"> • 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
Syslog severity:	Informational
Explanation:	A Save to USB job was completed successfully.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 .

	<user> - User who initiated the Save to USB job.
Message:	<device type>: Save to USB job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A Save to USB job was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the Save to USB job.
Message:	<device type>: Save to USB job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A Save to USB job failed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the Save to USB job.

Retrieve from USB

Message:	<device type>: Retrieve from USB job completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	A Retrieve from USB job was completed successfully.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the Retrieve from USB job.
Message:	<device type>: Retrieve from USB job completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A Retrieve from USB job was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who initiated the Retrieve from USB job.
Message:	<device type>: Retrieve from USB job completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	A Retrieve from USB job failed.

Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - User who initiated the Retrieve from USB job.

Job notification

Message:	<device type>: Job Notification completion; time="<timestamp>" user="<user>" outcome=success
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	A job notification report was delivered by email.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - If the job notification report is for a received fax, the value of this variable is "Guest." Otherwise, the value of this variable is the user who initiated the job that resulted in the job notification report.

Message:	<device type>: Job Notification completion; time="<timestamp>" user="<user>" outcome=canceled
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	A job notification sent via email was canceled.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - If the job notification report is for a received fax, the value of this variable is "Guest." Otherwise, the value of this variable is the user who initiated the job that resulted in the job notification report.

Message:	<device type>: Job Notification completion; time="<timestamp>" user="<user>" outcome=failure
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	A job notification sent via email failed.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<user> - If the job notification report is for a received fax, the value of this variable is "Guest." Otherwise, the value of this variable is the user who initiated the job that resulted in the job notification report.

Message:	<device type>: Print job completion; time="<timestamp>" job_name="Notification Job" user="<user>" outcome=success
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	A job notification report was printed.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .

	<user> - If the job notification report is for a received fax, the value of this variable is "Guest." Otherwise, the value of this variable is the user who initiated the job that resulted in the job notification report.
Message:	<device type>: Print job completion; time="<timestamp>" job_name="Notification Job" user="<user>" outcome=canceled
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	The printing of a job notification report was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - If the job notification report is for a received fax, the value of this variable is "Guest." Otherwise, the value of this variable is the user who initiated the job that resulted in the job notification report.

Internal reports/tests

Message:	<device type>: Print job completion; time="<timestamp>" job_name="<report name>" user="<user>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	An internal report or test was printed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <report name> - Name of the report/test. <user> - User who initiated the printing of the report/test.
Message:	<device type>: Print job completion; time="<timestamp>" job_name="<report name>" user="<user>" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	The printing of an internal report or test was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <report name> - Name of the report/test. <user> - User who initiated the printing of the report/test.
Message:	<device type>: Print job completion; time="<timestamp>" job_name="" user="Guest" source_IP="0.0.0.0" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	The HP Jetdirect Security Report was printed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 .

Message:	<device type>: Print job completion; time="<timestamp>" job_name="" user="Guest" source_IP="0.0.0.0" outcome=canceled
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	The printing of the HP Jetdirect Security Report was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 .
Message:	<device type>: Print job completion; time="<timestamp>" job_name="<report name>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, SNMP
Syslog severity:	Informational
Explanation:	An internal report or test was printed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <report name> - Name of the report/test. <user> - User who initiated the printing of the report/test. <client computer IP address> - IP address of the client computer that sent the request to print the report/test.
Message:	<device type>: Print job completion; time="<timestamp>" job_name="<report name>" user="<user>" source_IP="<client computer IP address>" outcome=canceled
Interface(s):	EWS, SNMP
Syslog severity:	Warning
Explanation:	The printing of an internal report or test was canceled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <report name> - Name of the report/test. <user> - User who initiated the printing of the report/test. <client computer IP address> - IP address of the client computer that sent the request to print the report/test.
Message:	<device type>: Print job completion; time="<timestamp>" job_name="<report name>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	A fax report was printed.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <report name> - Name of the fax report. <user> - User who initiated the printing of the fax report.

	<client computer IP address> - IP address of the client computer that sent the request to print the fax report.
Message:	<device type>: Print job completion; time="<timestamp>" job_name="<report name>" user="<user>" source_IP="<client computer IP address>" outcome=canceled
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	The printing of a fax report was canceled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><report name> - Name of the fax report.</p> <p><user> - User who initiated the printing of the fax report.</p> <p><client computer IP address> - IP address of the client computer that sent the request to print the fax report.</p>

Back up and restore

Backup device data

Message:	<p><device type>: Device Data Backup Completion; time="<timestamp>" source_IP="<client computer IP address>" outcome=success</p> <p><device type>: Device Data Backup Exported; time="<timestamp>" destination="<shared folder path>" source_IP="<client computer IP address>" outcome=success</p>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	Device data on the device was backed up.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><shared folder path> - Shared folder path the backup file was placed on.</p> <p><client computer IP address> - IP address of the client computer that sent the request to back up the device data.</p>

Restore device data

Message:	<device type>: Device Data Restore Completion; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	Device data from a backup was restored on the device.
	NOTE: Depending on the device data restored, additional messages can be generated.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><client computer IP address> - IP address of the client computer that sent the request to restore device data on the device.</p>

Device configuration

Syslog

Message:	<i><device type></i> : Syslog settings modified; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS, SNMP
Syslog severity:	Warning
Explanation:	<p>A syslog setting was modified.</p> <p>This message is generated when any of the following syslog settings are modified:</p> <ul style="list-style-type: none">• Syslog server IP address• Syslog protocol• Syslog port• Syslog maximum messages• Syslog priority• Syslog facility
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><user></i> - User who modified the syslog setting.</p> <p><i><client computer IP address></i> - IP address of the computer that sent the request to modify the syslog setting.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the syslog setting. Possible values are:</p> <ul style="list-style-type: none">• Wired• AP• STA

Jetdirect logging

Message:	<i><device type></i> : Jetdirect logging started; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Notice
Explanation:	<p>Jetdirect logging was enabled.</p> <p>This message is generated when the syslog server IP address is set and enhanced security event logging is enabled.</p>
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><user></i> - User who set the syslog server IP address and enabled enhanced security event logging.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to set the syslog server IP address and enable enhanced security event logging.</p> <p><i><interface></i> - Networking interface on the local device that received the request to set the syslog server IP address and enable enhanced security event logging. Possible values are:</p> <ul style="list-style-type: none">• Wired• AP• STA

Message:	<i><device type></i> : Jetdirect logging stopped; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	Jetdirect logging was disabled. This message is generated when the syslog server IP address is cleared and enhanced security event logging is disabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - User who cleared the syslog server IP address and disabled enhanced security event logging. <i><client computer IP address></i> - IP address of the client computer that sent the request to clear the syslog server IP address and disable enhanced security event logging. <i><interface></i> - Networking interface on the local device that received the request to clear the syslog server IP address and disable enhanced security event logging. Possible values are: <ul style="list-style-type: none"> • Wired • AP • STA

Enhanced security event logging

Message:	<i><device type></i> : CCC logging started; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS, SNMP
Syslog severity:	Notice
Explanation:	Enhanced security event logging was enabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - User who enabled enhanced security event logging. <i><client computer IP address></i> - IP address of the client computer that sent the request to enable enhanced security event logging. <i><interface></i> - Networking interface on the local device that received the request to enable enhanced security event logging. Possible values are: <ul style="list-style-type: none"> • Wired • AP • STA

Message:	<i><device type></i> : CCC logging stopped; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS, SNMP
Syslog severity:	Warning
Explanation:	Enhanced security event logging was disabled. This message is logged when enhanced security event logging is disabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 .

<user> - User who disabled enhanced security event logging.

<client computer IP address> - IP address of the client computer that sent the request to disable enhanced security event logging.

<interface> - Networking interface on the local device that received the request to disable enhanced security event logging. Possible values are:

- Wired
 - AP
 - STA
-

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>" outcome=success interface= <interface>
Interface(s):	EWS, SNMP
Syslog severity:	Warning
Explanation:	The Jetdirect security settings were reset to factory defaults.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who reset the Jetdirect security settings to factory defaults.</p> <p><client computer IP address> - IP address of the client computer that sent the request to reset the Jetdirect security settings to factory defaults.</p> <p><interface> - Networking interface on the local device that received the request to reset the Jetdirect security settings to factory defaults. Possible values are:</p> <ul style="list-style-type: none">• Wired• AP• STA

Message:	<device type>: Jetdirect security settings reset to factory defaults; time=" <timestamp>" outcome=success interface= <interface>
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	The Jetdirect security settings were reset to factory defaults.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><interface> - Networking interface on the local device. Possible values are:</p> <ul style="list-style-type: none">• Wired• AP• STA

SNMPv3 user accounts

Message:	<device type>: SNMPv3 user account added; time=" <timestamp>" user=" <user>" SNMPv3_user_account=" <user account>" source_IP=" <client computer IP address>" outcome=success interface= <interface>
Interface(s):	EWS, SNMPv3
Syslog severity:	Informational

Explanation:	An SNMPv3 user account was added.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who added the SNMPv3 user account.</p> <p><user account> - User name of SNMPv3 user account that was added.</p> <p><client computer IP address> - IP address of the client computer that sent the request to add the SNMPv3 user account.</p> <p><interface> - Networking interface on the local device that received request to add the SNMPv3 account. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: SNMPv3 user account deleted; time="<timestamp>" user="<user>" SNMPv3_user_account="<user account>" source_IP="<client computer IP address>" outcome=success interface="<interface>"
Interface(s):	EWS, SNMPv3
Syslog severity:	Informational
Explanation:	An SNMPv3 user account was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who deleted the SNMPv3 user account.</p> <p><username> - User name of the SNMPv3 user account that was deleted.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete the SNMPv3 user account.</p> <p><interface> - Networking interface on the local device that received the request to delete the SNMPv3 account. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

Inactivity timeout

Message:	<device type>: Control Panel Inactivity Timeout Changed; time="<timestamp>" value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*, control panel
Syslog severity:	Informational
Explanation:	The inactivity timeout setting was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p>

	<p><user> - Authenticated user who modified the inactivity timeout setting. If an unauthenticated user modified the inactivity timeout setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the inactivity timeout setting.</p>
Message:	<device type>: Control Panel Inactivity Timeout Changed; time="<timestamp>" value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	Control panel
Syslog severity:	Informational
Explanation:	The inactivity timeout setting was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the inactivity timeout setting. If an unauthenticated user modified the inactivity timeout setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the inactivity timeout setting.</p>

Account policy

Account lockout policy for device administrator account

Message:	<device type>: Account Lockout Policy enabled; time="<timestamp>" account=local_administrator user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The account lockout policy for the device administrator account was enabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who enabled the account policy. If an unauthenticated user enabled the account lockout policy, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to enable the account lockout policy.</p>
Message:	<device type>: Account Lockout Policy disabled; time="<timestamp>" account=local_administrator user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The account lockout policy for the device administrator account was disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

	<p><user> - Authenticated user who disabled the account lockout policy. If an unauthenticated user disabled the account lockout policy, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to disable the account lockout policy.</p>
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=<account> item=maximum_login_attempts value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The maximum attempts setting for the device administrator account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the account lockout policy. If an unauthenticated user modified the account lockout policy, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p>
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=<account> item=default_lockout_time value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The lockout interval setting for the device administrator account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the account lockout policy. If an unauthenticated user modified the account lockout policy, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p>
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=<account> item=counter_reset_time value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The reset lockout interval setting for the device administrator account lockout policy was modified.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<value> - New setting value.

<old value> - Old setting value.

<user> - Authenticated user who modified the account lockout policy. If an unauthenticated user modified the account lockout policy, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.

Account lockout policy for remote configuration account

Message:	<device type>: Account Lockout Policy enabled; time="<timestamp>" account=remote_configuration user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The account lockout policy for the remote configuration account was enabled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <value> - New setting value. <old value> - Old setting value. <user> - Authenticated user who enabled the account lockout policy. If an unauthenticated user enabled the account lockout policy, the user key-value pair is not contained within the message. <client computer IP address> - IP address of the client computer that sent the request to enable the account lockout policy.
Message:	<device type>: Account Lockout Policy disabled; time="<timestamp>" account=remote_configuration user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The account lockout policy for the remote configuration account was disabled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authenticated user who disabled the account lockout policy. If an unauthenticated user disabled the account lockout policy, the user key-value pair is not contained within the message. <client computer IP address> - IP address of the client computer that sent the request to disable the account lockout policy.
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=remote_configuration item=maximum_login_attempts value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational

Explanation:	The maximum attempts setting for the remote configuration account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the account lockout policy. If an unauthenticated user modified the account lockout policy, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p>
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=remote_configuration item=default_lockout_time value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The lockout interval setting for the remote configuration account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the account lockout policy. If an unauthenticated user modified the account lockout policy, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p>
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=remote_configuration item=counter_reset_time value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The reset lockout interval setting for the remote configuration account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the account lockout policy. If an unauthenticated user modified the account lockout policy, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p>

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>" outcome=success interface= <interface>
Interface(s):	SNMP
Syslog severity:	Informational
Explanation:	The account lockout policy for SNMPv3 user accounts was enabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who enabled the account lockout policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to enable the account lockout policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the account lockout policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Account Lockout Policy disabled; time=" <timestamp>" account=SNMPv3 user=" <user>" source_IP=" <client computer IP address>" outcome=success interface= <interface>
Interface(s):	SNMP
Syslog severity:	Informational
Explanation:	The account lockout policy for SNMPv3 user accounts was disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who disabled the account lockout policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to disable the account lockout policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the account lockout policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Account Lockout Policy setting modified; time=" <timestamp>" account=SNMPv3 item=maximum_login_attempts value=" <value>" old_value=" <old value>" user=" <user>" source_IP=" <client computer IP address>" outcome=success interface= <interface>
Interface(s):	SNMP
Syslog severity:	Informational
Explanation:	The maximum attempts setting for the SNMPv3 user account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p>

	<p><user> - User who modified the account lockout policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the account lockout policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=SNMPv3 item=default_lockout_time value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success interface="<interface>"
Interface(s):	SNMP
Syslog severity:	Informational
Explanation:	The lockout interval setting for the SNMPv3 user account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - User who modified the account lockout policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the account lockout policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Account Lockout Policy setting modified; time="<timestamp>" account=SNMPv3 item=counter_reset_time value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success interface="<interface>"
Interface(s):	SNMP
Syslog severity:	Informational
Explanation:	The reset lockout interval setting for the SNMPv3 user account lockout policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - User who modified the account lockout policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the account lockout policy.</p>

<interface> - Networking interface on the local device that received the request to modify the account lockout policy. Possible values are:

- Wired
 - AP
 - STA
-

Password complexity policy for device administrator password

Message:	<i><device type></i> : Password Complexity Policy enabled; time=" <i><timestamp></i> " account= <i><account></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The password complexity policy for the device administrator password was enabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Authenticated user who enabled the password complexity policy. If an unauthenticated user enabled the password complexity policy, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to enable the password complexity policy.
Message:	<i><device type></i> : Password Complexity Policy disabled; time=" <i><timestamp></i> " account=local_administrator user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The password complexity policy for the device administrator password was disabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Authenticated user who disabled the password complexity policy. If an unauthenticated user disabled the password complexity policy, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to disable the password complexity policy.

Password complexity policy for remote configuration password

Message:	<i><device type></i> : Password Complexity Policy enabled; time=" <i><timestamp></i> " account=remote_configuration user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The password complexity policy for the remote configuration password was enabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Authenticated user who enabled the password complexity policy. If an unauthenticated user enabled the password complexity policy, the user key-value pair is not contained within the message.

	<client computer IP address> - IP address of the client computer that sent the request to enable the password complexity policy.
Message:	<device type>: Password Complexity Policy disabled; time=" <timestamp>" account=remote_configuration user=" <user>" source_IP=" <client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The password complexity policy for the remote configuration password was disabled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authenticated user who disabled the password complexity policy. If an unauthenticated user disabled the password complexity policy, the user key-value pair is not contained within the message. <client computer IP address> - IP address of the client computer that sent the request to disable the password complexity policy.

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>" outcome=success interface= <interface>
Interface(s):	SNMPv3
Syslog severity:	Informational
Explanation:	The password complexity policy for the SNMPv3 authentication passphrase was enabled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authenticated user who enabled the password complexity policy. If an unauthenticated user enabled the password complexity policy, the user key-value pair is not contained within the message. <client computer IP address> - IP address of the client computer that sent the request to enable the password complexity policy. <interface> - Networking interface on the local device that received the request to enable the password complexity policy. Possible values are: <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Password Complexity Policy disabled; time=" <timestamp>" account=SNMPv3 user=" <user>" source_IP=" <client computer IP address>" outcome=success interface= <interface>
Interface(s):	SNMPv3
Syslog severity:	Informational
Explanation:	The password complexity policy for the SNMPv3 authentication passphrase was disabled.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authenticated user who disabled the password complexity policy. If an unauthenticated user disabled the password complexity policy, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to disable the password complexity policy.

<interface> - Networking interface on the local device that received the request to disable the password complexity policy. Possible values are:

- Wired
 - AP
 - STA
-

Minimum password length policy for device administrator password

Message:	<i><device type></i> : Minimum Password Length Policy setting modified; time=" <i><timestamp></i> " account=local_administrator item=minimum_password_length value=" <i><value></i> " old_value=" <i><old value></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The minimum password length policy for the device administrator password was modified.
Variables:	

<device type> - see [Table 2-2](#).

<timestamp> - see [Table 2-2](#).

<value> - New setting value.

NOTE: New setting value of zero (0) indicates the minimum password policy was disabled.

<old value> - Old setting value.

<user> - Authenticated user who modified the minimum password length policy. If an unauthenticated user modified the minimum password length policy, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the minimum password length policy.

Minimum password length policy for remote configuration password

Message:	<i><device type></i> : Minimum Password Length Policy setting modified; time=" <i><timestamp></i> " account=remote_configuration item=minimum_password_length value=" <i><value></i> " old_value=" <i><old value></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The minimum password length policy for the remote configuration password was modified.
Variables:	

<device type> - see [Table 2-2](#).

<timestamp> - see [Table 2-2](#).

<value> - New setting value.

NOTE: New setting value of zero (0) indicates the minimum password policy was disabled.

<old value> - Old setting value.

<user> - Authenticated user who modified the minimum password length policy. If an unauthenticated user modified the minimum password length policy, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the minimum password length policy.

Minimum password length policy for 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>" outcome=success interface="<interface>"
Interface(s):	SNMPv3
Syslog severity:	Informational
Explanation:	The minimum password length policy for the SNMPv3 authentication passphrase was modified.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<value> - New setting value.

NOTE: New setting value of zero (0) indicates the minimum password policy was disabled.

<old value> - Old setting value.

<user> - Authenticated user who modified the minimum password length policy. If an unauthenticated user modified the minimum password length policy, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the minimum password length policy.

<interface> - Networking interface on the local device that received the request to modify the minimum password length policy. Possible values are:

- Wired
 - AP
 - STA
-

Date and time settings

DST settings

Message:	<device type>: Date and Time configuration modified; time="<timestamp>" item=adjust_for_daylight_savings value=enabled old_value=disabled user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*, CP, SNMPv3
Syslog severity:	Informational
Explanation:	Date and time settings were configured to adjust for daylight savings.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<user> - Authenticated user who enabled adjust for daylight savings. If an unauthenticated user enabled adjust for daylight savings, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to enable adjust for daylight savings.

Message:	<device type>: Date and Time configuration modified; time="<timestamp>" item=adjust_for_daylight_savings value=disabled old_value=enabled user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*, CP, SNMPv3

Syslog severity:	Informational
Explanation:	Date and time settings were configured to not adjust for daylight savings.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who disabled adjust for daylight savings. If an unauthenticated user disabled adjust for daylight savings, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to disable adjust for daylight savings.</p>
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>" outcome=success
Interface(s):	EWS, WS*, CP, SNMPv3
Syslog severity:	Informational
Explanation:	A daylight savings time setting was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><item> - Setting that was modified. Possible values are:</p> <ul style="list-style-type: none"> • DST_start_occurrence • DST_start_week_day • DST_start_month • DST_start_hour • DST_end_occurrence • DST_end_week_day • DST_end_month • DST_end_hour • DST_offset_minutes <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the setting. If an unauthenticated user modified the setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the setting.</p>
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>" outcome=success
Interface(s):	EWS, WS*, CP, SNMPv3
Syslog severity:	Informational
Explanation:	The daylight savings time settings were reset to factory defaults.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who reset the daylight savings time settings to factory defaults. If an unauthenticated user reset the daylight savings time settings to factory defaults, the user key-value pair is not contained within the message.</p>

<client computer IP address> - IP address of the client computer that sent the request to reset the daylight savings time settings to factory defaults.

NTS settings

Message:	<i><device type></i> : Date and Time configuration modified; time=" <i><timestamp></i> " item=automatically_synchronize_with_network_time_server value=enabled old_value=disabled user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	Automatic time synchronization with the Network Time Server was enabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Authenticated user who enabled automatic time synchronization with the Network Time Server. If an unauthenticated user enabled automatic time synchronization with the Network Time Server, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to enabled automatic time synchronization with the Network Time Server.
Message:	<i><device type></i> : Date and Time configuration modified; time=" <i><timestamp></i> " item=automatically_synchronize_with_network_time_server value=disabled old_value=enabled user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	Automatic time synchronization with the Network Time Server was disabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Authenticated user who disabled automatic time synchronization with the Network Time Server. If an unauthenticated user disabled automatic time synchronization with the Network Time Server, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to disable automatic time synchronization with the Network Time Server.
Message:	<i><device type></i> : Date and Time configuration modified; time=" <i><timestamp></i> " item= <i><item></i> value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The Network Time Server settings were modified.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><item></i> - Setting that was modified. Possible values are: <ul style="list-style-type: none">• network_time_server_address• local_port_to_receive_time_from_network_time_server• frequency_of_time_synchronization_with_network_time_server_in_hours <i><user></i> - Authenticated user who modified the setting. If an unauthenticated user modified the setting, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to modify the setting.

Message:	<i><device type></i> : System Time Use Default; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The Network Time Server settings were reset to factory defaults.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><user></i> - Authenticated user who reset the Network Time Server settings to factory defaults. If an unauthenticated user reset the Network Time Server settings to factory defaults, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to reset the Network Time Server settings to factory defaults.</p>

Fax settings

Fax archive

Message:	printer: Fax setting modified; time=" <i><timestamp></i> " item=fax_archive value= <i><value></i> old_value= <i><old value></i> source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The fax archive setting was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> do_not_archive archive_only archive_and_print <p><i><old value></i> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> do_not_archive archive_only archive_and_print <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the fax archive setting.</p>

Fax forwarding

Message:	printer: Fax setting modified; time=" <i><timestamp></i> " item=fax_forwarding value= <i><value></i> old_value= <i><old value></i> source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	Fax forwarding was either enabled or disabled.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New enable or disable setting value. Possible values are:</p> <ul style="list-style-type: none"> enable disable

<old value> - New enable or disable setting value. Possible values are:

- enable
- disable

<client computer IP address> - IP address of the client computer that sent the request to enable or disable fax forwarding.

General security

Device administrator password

Message:	<device type>: Device Administrator Password modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The device administrator password was set, cleared, or modified.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authenticated user who set, cleared, or modified the device administrator password. If an unauthenticated user set, cleared, or modified the device administrator password, the user key-value pair is not contained within the message. <client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the device administrator password.
Message:	<device type>: Device Administrator Password modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=failure
Interface(s):	EWS, WS*
Syslog severity:	Warning
Explanation:	An attempt to set, clear, or modify the device administrator password was unsuccessful.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - Authenticated user who attempted to set, clear or modify the device administrator password. If an unauthenticated user attempted to set, clear, or modify the device administrator password, the user key-value pair is not contained within the message. <client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the device administrator password.
Message:	<device type>: Device Administrator Password modified; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success interface="<interface>"
Interface(s):	SNMP
Syslog severity:	Warning
Explanation:	The device administrator password was set, cleared, or modified.
Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <user> - User who set, cleared, or modified the device administrator password.

<client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the device administrator password.

<interface> - Device networking interface on which the device configuration request was received. Possible values are:

- Wired
 - AP
 - STA
-

Service access code

Message:	<i><device type></i> : Service User PIN modified; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The service user PIN (a.k.a. service access code) was modified.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><client computer IP address></i> - IP address of the client computer that sent the request to modify the service access code.
Message:	<i><device type></i> : Service User PIN modified; time=" <i><timestamp></i> " source_IP=" <i><client IP address></i> " outcome=failure
Interface(s):	EWS, WS*
Syslog severity:	Warning
Explanation:	An attempt to modify the service user PIN (a.k.a. service access code) was unsuccessful.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><client computer IP address></i> - IP address of the client computer that sent the request to modify the service access code.

Remote configuration password

Message:	<i><device type></i> : Remote Configuration Password modified; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The remote configuration password was set, cleared, or modified.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Authenticated user who set, cleared, or modified the remote configuration password. If an unauthenticated user set, cleared, or modified the remote configuration password, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to set, clear, or modify the remote configuration password.
Message:	<i><device type></i> : Remote Configuration Password modified; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=failure

Interface(s):	EWS, WS*
Syslog severity:	Warning
Explanation:	An attempt to set, clear, or modify the remote configuration password was unsuccessful.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who attempted to set, clear, or modify the remote configuration password. If an unauthenticated user attempted to set, clear, or modify the remote configuration password, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the remote configuration password.</p>

Cross-site request forgery (CRSF) prevention

Message:	<device type>: Cross-site Request Forgery (CRSF) prevention modified; time="<timestamp>" value=<value> old_value=<old value> user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	Cross-site request forgery prevention was either enabled or disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><old value> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><user> - Authenticated user who enabled or disabled cross-site request forgery prevention. If an unauthenticated user enabled or disabled cross-site request forgery, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to enable or disable cross-site request forgery.</p>

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>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The EWS session timeout setting was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p>

<user> - Authenticated user who modified the EWS session timeout. If an unauthenticated user modified the EWS session timeout, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the EWS session timeout.

PJL password

Message:	printer: PJL Password modified; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome=success
-----------------	---

Interface(s):	EWS, WS*, PJL
----------------------	---------------

Syslog severity:	Informational
-------------------------	---------------

Explanation:	The PJL password was set, cleared, or modified.
---------------------	---

Variables:	<i><device type></i> - see Table 2-2 .
-------------------	--

<timestamp> - see [Table 2-2](#).

<client computer IP address> - IP address of the client computer that sent the request to modify the PJL password.

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

Interface(s):	EWS, WS*
----------------------	----------

Syslog severity:	Warning
-------------------------	---------

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

Variables:	<i><device type></i> - see Table 2-2 .
-------------------	--

<timestamp> - see [Table 2-2](#).

<client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the PJL password.

Firmware upgrade security

Message:	<i><device type></i> : Allow Firmware Upgrade as Print Job Changed; time=" <i><timestamp></i> " value= <i><value></i> old value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
-----------------	--

Interface(s):	EWS, WS*
----------------------	----------

Syslog severity:	Informational
-------------------------	---------------

Explanation:	The "Allow firmware upgrades sent as print jobs (port 9100)" setting was either enabled or disabled.
---------------------	--

Variables:	<i><device type></i> - see Table 2-2 .
-------------------	--

<timestamp> - see [Table 2-2](#).

<value> - New setting value. Possible values are:

- enable
- disable

<old value> - Old setting value. Possible values are:

- enable
- disable

<user> - Authenticated user who enabled or disabled the "Allow firmware upgrades sent as print jobs (port 9100)" setting. If an unauthenticated user enabled or disabled the "Allow firmware upgrades sent as print jobs (port 9100)" setting, the user key-value pair is not contained within the message.

	<i><client computer IP address></i> - IP address of the client computer that sent the request to enable or disable the “Allow firmware upgrades sent as print jobs (port 9100)” setting.
Message:	<i><device type></i> : Allow Installation of Legacy Packages with SHA-1 Changed; time=" <i><timestamp></i> " value= <i><value></i> old value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The “Allow installation of legacy packages signed with SHA-1 Hashing algorithm” setting was either enabled or disabled.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><i><old value></i> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><i><user></i> - Authenticated user who enabled or disabled the “Allow installation of legacy packages signed with SHA-1 Hashing algorithm” setting. If an unauthenticated user enabled or disabled the “Allow firmware upgrades sent as print jobs (port 9100)” setting, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to enable or disable the “Allow installation of legacy packages signed with SHA-1 Hashing algorithm” setting.</p>

Bootloader administrator password

Message:	<i><device type></i> : Boot Administrator Password modified; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	The pre-boot menu administrator password was set, cleared, or modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to set, clear, or modify the pre-boot menu administrator password.</p>
Message:	<i><device type></i> : Boot Administrator Password modified; time=" <i><timestamp></i> " source_IP=" <i><client computer IP address></i> " outcome=failure
Interface(s):	WS*
Syslog severity:	Warning
Explanation:	An attempt to set, clear, or modify the pre-boot menu administrator password was unsuccessful.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to set, clear, or modify the pre-boot menu administrator password.</p>

Drive-lock password

Message:	<i><device type></i> : Encrypted Drives Random Password Set; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A new random drive-lock password was generated.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Authenticated user who generated the new random drive-lock password. If an unauthenticated user generated the new random drive-lock password, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to generate a new random drive-lock password.

File erase mode

Message:	<i><device type></i> : File Erase Mode for erasing temporary job files modified; time=" <i><timestamp></i> " value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The file erase mode used to erase temporary job files was modified.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><value></i> - New setting value. Possible values are: <ul style="list-style-type: none">• non_secure_fast_erase• secure_fast_erase• secure_sanitize_erase <i><old value></i> - Old setting value. Possible values are: <ul style="list-style-type: none">• non_secure_fast_erase• secure_fast_erase• secure_sanitize_erase <i><user></i> - Authenticated user who modified the file erase mode. If an unauthenticated user modified the file erase mode, the user key-value pair is not contained within the message. <i><client computer IP address></i> - IP address of the client computer that sent the request to modify the file erase mode.

Access control

LDAP Sign In

Message:	<i><device type></i> : LDAP Sign In enabled; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	LDAP Sign In was enabled.
Variables:	<i><device type></i> - see Table 2-2 .

	<p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who enabled LDAP Sign In. If an unauthenticated user enabled LDAP Sign In, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to enable LDAP Sign In.</p>
Message:	<device type>: LDAP Sign In disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	LDAP Sign In was disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who disabled LDAP Sign In. If an unauthenticated user disabled LDAP Sign In, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to disable LDAP Sign In.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=LDAP_server_address value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The LDAP server address setting for LDAP Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the LDAP server address. If an unauthenticated user set, cleared, or modified the LDAP server address, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the LDAP server address.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=LDAP_server_port value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The LDAP server port setting for LDAP Sign In was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

	<p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who modified the LDAP server port setting. If an unauthenticated user modified the LDAP server port, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the LDAP server port.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=use_a_secure_connection_SSL value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Use a secure connection (SSL)" setting for LDAP Sign In was either enabled or disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><old value> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><user> - Authenticated user who enabled or disabled the "Use a secure connection (SSL)" setting. If an unauthenticated user enabled or disabled the "Use a secure connection (SSL)" setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to enable or disable "Use a secure connection (SSL)" setting.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=bind_prefix value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The bind prefix setting for LDAP Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the bind prefix setting. If an unauthenticated user set, cleared, or modified the bind prefix setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the bind prefix setting.</p>

Message:	<code><device type>: LDAP Sign In configuration modified; time="<timestamp>" item=LDAP_administrator_password user="<user>" source_IP="<client computer IP address>" outcome=success</code>
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The administrator's password for binding to the LDAP server for LDAP Sign In was set, cleared, or modified.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><user></code> - Authenticated user who set, cleared, or modified the administrator's password. If an unauthenticated user set, cleared, or modified the administrator's password, the user key-value pair is not contained within the message.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to set, clear, or modify the administrator's password.</p>
Message:	<code><device type>: LDAP Sign In configuration modified; time="<timestamp>" item=server_connection_credentials_to_use value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success</code>
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Server credentials to use" option for LDAP Sign In was modified.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><value></code> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> • UserCredentials • AdministratorCredentials <p><code><old value></code> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> • UserCredentials • AdministratorCredentials <p><code><user></code> - Authenticated user who modified the "Server credentials to use" option. If an unauthenticated user modified the "Server credentials to use" option, the user key-value pair is not contained within the message.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to modify the "Server credentials to use" option.</p>
Message:	<code><device type>: LDAP Sign In configuration modified; time="<timestamp>" item=LDAP_administrator_DN value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success</code>
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The administrator's Distinguished Name for LDAP Sign In was set, cleared, or modified.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><value></code> - New administrator Distinguished Name.</p> <p><code><old value></code> - Old administrator Distinguished Name.</p>

	<p><user> - Authenticated user who set, cleared, or modified the administrator's Distinguished Name. If an unauthenticated user set, cleared, or modified the administrator's Distinguished Name, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the administrator's Distinguished Name.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=name_entered_match_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Match the name entered with this attribute" setting for LDAP Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the "Match the name entered with this attribute" setting. If an unauthenticated user set, cleared, or modified the "Match the name entered with this attribute" setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the "Match the name entered with this attribute" setting.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=email_address_retrieve_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Retrieve the user's email address using this attribute" setting for LDAP Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the "Retrieve the user's email address using this attribute" setting. If an unauthenticated user set, cleared, or modified the "Retrieve the user's email address using this attribute" setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the "Retrieve the user's email address using this attribute" setting.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=email_address_retrieve_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*

Syslog severity:	Informational
Explanation:	The “Retrieve the user’s email address using this attribute” setting for LDAP Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the “Retrieve the user’s email address using this attribute” setting. If an unauthenticated user set, cleared, or modified the “Retrieve the user’s email address using this attribute” setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the “Retrieve the user’s email address using this attribute” setting.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=name_retrieve_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The “Retrieve the device user’s name using this attribute” setting for LDAP Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the “Retrieve the device user’s name using this attribute” setting. If an unauthenticated user set, cleared, or modified the “Retrieve the device user’s name using this attribute” setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the “Retrieve the device user’s name using this attribute” setting.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" item=group_retrieve_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The “Retrieve the device user’s group using this attribute” setting for LDAP Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p>

	<p><i><user></i> - Authenticated user who set, cleared, or modified the “Retrieve the device user’s group using this attribute” setting. If an unauthenticated user set, cleared, or modified the “Retrieve the device user’s group using this attribute” setting, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to set, clear, or modify the “Retrieve the device user’s group using this attribute” setting.</p>
Message:	<i><device type></i> : LDAP Sign In configuration modified; time=" <i><timestamp></i> " item=exact_match_on_group_attribute value=" <i><value></i> " old_value=" <i><old value></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The “Exact match on Group attribute” setting for LDAP Sign In was either enabled or disabled.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><i><old value></i> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><i><user></i> - Authenticated user who enabled or disabled the “Exact match on Group attribute” setting. If an unauthenticated user enabled or disabled the “Exact match on Group attribute” setting, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to enable or disable the “Exact match on Group attribute” setting.</p>
Message:	<i><device type></i> : LDAP Sign In configuration modified; time=" <i><timestamp></i> " action=bind_and_search_root_added value=" <i><value></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A search root for looking up the user’s name and email for LDAP Sign In was added.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - Bind and search root that was added.</p> <p><i><user></i> - Authenticated user who added the search root. If an unauthenticated user added the search root, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to add the search root.</p>
Message:	<i><device type></i> : LDAP Sign In configuration modified; time=" <i><timestamp></i> " action=bind_and_search_root_deleted value=" <i><value></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational

Explanation:	A search root for looking up the user's name and email for LDAP Sign In was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - Bind and search root that was deleted.</p> <p><user> - Authenticated user who deleted the search root. If an unauthenticated user deleted the search root, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete the search root.</p>
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>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The order of the search roots used for looking up the user's name and email for LDAP Sign In was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who modified the order of the search roots. If an unauthenticated user modified the order of the search roots, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the order of the search roots.</p>
Message:	<device type>: LDAP Sign In configuration modified; time="<timestamp>" action=LDAP_sign_in_configuration_deleted user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	The LDAP Sign In configuration was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who deleted the LDAP Sign In configuration. If an unauthenticated user deleted the LDAP Sign In configuration, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete the LDAP Sign In configuration.</p>
Message:	<device type>: LDAP Authentication Test; time="<timestamp>" username="<username>" server="<server address>" port="<server port>" admin_name="<administrator DN>" bind_prefix="<bind prefix>" search_root="<search roots>" name_match_attribute="<name match attribute>" email_attribute="<email match attribute>" group_attribute="<group match attribute>" group_exact_match="<group exact match>" source_IP="<client computer IP address>" outcome=<test result>
Interface(s):	EWS
Syslog severity:	Informational

Explanation:	The LDAP Sign In test was performed.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><username></i> - User name that was used to test user authentication.</p> <p><i><server address></i> - IP address or hostname of the LDAP server.</p> <p><i><administrator DN></i> - If the option to use the LDAP administrator's credentials to bind to the LDAP server was selected in the LDAP Sign In configuration, the value of this variable is the LDAP administrator's Distinguished Name.</p> <p><i><bind prefix></i> - If the option to use device user's credentials to bind to the LDAP server was selected in the LDAP Sign In configuration, the value of this variable is the bind prefix that was used to construct the user's Distinguished Name.</p> <p><i><search root></i> - Search roots that were used to lookup the user's name and email in the LDAP directory.</p> <p><i><name match attribute></i> - Attribute that was used to match <i><username></i>.</p> <p><i><email attribute></i> - Attribute that was used to retrieve the user's email address.</p> <p><i><group match attribute></i> - Attribute that was used to retrieve the user's groups.</p> <p><i><group exact match></i> - Setting that determines whether the group match attribute must have an exact match on the user's groups. Possible values are:</p> <ul style="list-style-type: none"> • enabled • disabled <p><i><client computer IP address></i> - IP address of the client computer that sent the request to perform the LDAP Sign In test.</p> <p><i><test result></i> - Result of the LDAP Sign In test. Possible values are:</p> <ul style="list-style-type: none"> • success • failure

Windows Sign In

Message:	<i><device type></i> : Windows Sign In enabled; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	Windows Sign In was enabled.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><user></i> - Authenticated user who enabled Windows Sign In. If an unauthenticated user enabled Windows Sign In, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to enable Windows Sign In.</p>
Message:	<i><device type></i> : Windows Sign In disabled; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational

Explanation:	Windows Sign In was disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who disabled Windows Sign In. If an unauthenticated user disabled Windows Sign In, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to disable Windows Sign In.</p>
Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" action=trusted_domain_added value="<value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A trusted domain for Windows Sign In was added.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - Trusted domain that was added.</p> <p><user> - Authenticated user who added the trusted domain configuration. If an unauthenticated user added the trusted domain, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to add the trusted domain.</p>
Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" action=trusted_domain_deleted value="<value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A trusted domain for Windows Sign In was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - Trusted domain that was deleted.</p> <p><user> - Authenticated user who deleted the trusted domain. If an unauthenticated user modified deleted the trusted domain, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete the trusted domain.</p>
Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" item=default_windows_domain value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The default Windows domain setting for Windows Sign In was modified.
Variables:	<device type> - see Table 2-2 .

	<p><timestamp> - see Table 2-2.</p> <p><value> - New default Windows domain.</p> <p><old value> - Old default Windows domain</p> <p><user> - Authenticated user who set a new default Windows domain. If an unauthenticated user set a new default Windows domain, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set a new default Windows domain.</p>
Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" item=name_entered_match_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The “Match the name entered with this attribute” setting for Windows Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the “Match the name entered with this attribute” setting. If an unauthenticated user set, cleared, or modified the “Match the name entered with this attribute” setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the “Match the name entered with this attribute” setting.</p>
Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" item=email_address_retrieve_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The “Retrieve the user’s email using this attribute” setting for Windows Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the “Retrieve the user’s email using this attribute” setting. If an unauthenticated user set, cleared, or modified the “Retrieve the user’s email using this attribute” setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the “Retrieve the user’s email using this attribute” setting.</p>

Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" item=name_retrieve_attribute value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Retrieve the device user's name using this attribute" setting for Windows Sign In was set, cleared, or modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - Authenticated user who set, cleared, or modified the "Retrieve the device user's name using this attribute" setting. If an unauthenticated user modified the Windows Sign In configuration, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to set, clear, or modify the "Retrieve the device user's name using this attribute" setting.</p>
Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" item=reverse_DNS_lookups value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Enable reverse DNS lookups" setting for Windows Sign In was either enabled or disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><old value> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> • enable • disable <p><user> - Authenticated user who enabled or disabled the "Enable reverse DNS lookups" setting. If an unauthenticated user enabled or disabled the "Enable reverse DNS lookups" setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to enable or disable the "Enable reverse DNS lookups" setting.</p>
Message:	<device type>: Windows Sign In configuration modified; time="<timestamp>" item=use_a_secure_connection value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Use a secure connection (SSL)" setting for Windows Sign In was either enabled or disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

<value> - New setting value. Possible values are:

- enable
- disable

<old value> - Old setting value. Possible values are:

- enable
- disable

<user> - Authenticated user who enabled or disabled the "Use a secure connection (SSL)" setting. If an unauthenticated user enabled or disabled the "Use a secure connection (SSL)" setting, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to enable or disable the "Use a secure connection (SSL)" setting.

Message:	<device type>: Windows Authentication Test; time="<timestamp>" domain="<domain>" username="<username>" reverse_DNS="<reverse DNS>" name_attribute="<name attribute>" email_attribute="<email attribute>" source_IP="<client computer IP address>" outcome="<test result>"
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The Windows Sign In test was performed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><domain> - Windows domain.</p> <p><username> - Username that was specified in the Windows Sign In test to authenticate.</p> <p><reverse DNS> - Enable or disable setting for performing reverse DNS lookups. Possible values are:</p> <ul style="list-style-type: none">• enabled• disabled <p><name attribute> - Attribute that was used to match the value of <username>.</p> <p><email attribute> - Attribute that was used to retrieve the user's email address.</p> <p><client computer IP address> - IP address of the client computer that sent the request to perform the Windows Sign In test.</p> <p><test result> - Result of the Windows Sign In test. Possible values are:</p> <ul style="list-style-type: none">• success• failure

Device user accounts

Message:	<device type>: Device User Account added; time="<timestamp>" user="<display name attribute>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A device user account was added.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

	<display name attribute> - Display name attribute of the device user account.
	<client computer IP address> - IP address of the client computer that sent the request to add the device user account.
Message:	<device type>: Device User Accounts imported; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	One or more device user accounts were imported.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<client computer IP address> - IP address of the client computer that sent the request to import the device user accounts.
Message:	<device type>: Device User Accounts exported; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	One or more device user accounts were exported.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<client computer IP address> - IP address of the client computer that sent the request to export the device user accounts.
Message:	<device type>: Device User Account deleted; time="<timestamp>" all_users_deleted source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	All device user accounts were deleted.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<client computer IP address> - IP address of the client computer that sent the request to delete all device user accounts.
Message:	<device type>: Device User Account deleted; time="<timestamp>" user="<display name attribute>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A device user account was deleted.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<display name attribute> - Display name attribute of the device user account that was deleted.

	<client computer IP address> - IP address of the client computer that sent the request to delete the device user account.
Message:	<device type>: Device User Account modified; time="<timestamp>" user="<display name attribute>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A device user account was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><display name attribute> - Display name attribute of the device user account.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the device user account.</p>
Message:	<device type>: Default Permission Set for sign-in method modified; time="<timestamp>" sign-in_method=local_device permission_set="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The default permission set for new device user accounts was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New default permission set. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><old value> - Old default permission set. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><user> - Authenticated user who modified the default permission set for new device user accounts. If an unauthenticated user modified the default permission set for new device user accounts, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the default permission set for new device user accounts.</p>

Default sign-in method for 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>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The default sign-in method for the control panel was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p>

<value> - New setting value. Possible values are:

- local_device
- ldap
- windows
- smartcard

Possible values also include the names of third-party authentication agents that have been installed on the device.

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

- local_device
- ldap
- windows
- smartcard

Possible values also include the names of third-party authentication agents that have been installed on the device.

<user> - Authenticated user who modified the default sign-in method for the control panel. If an unauthenticated user modified the default sign-in method for the control panel, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the default sign-in method for the control panel.

Default sign-in method for EWS

Message:	<i><device type></i> : Default Sign In Method for EWS tabs modified; time=" <i><timestamp></i> " value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The default sign-in method for EWS was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New setting value. Possible values are:</p> <ul style="list-style-type: none">• local_device• ldap• windows• smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p> <p><i><old value></i> - Previous default sign-in method. Possible values are:</p> <ul style="list-style-type: none">• local_device• ldap• windows• smartcard <p>Possible values also include the names of third-party authentication agents installed on the device.</p> <p><i><user></i> - Authenticated user who modified the default sign-in method for the EWS. If an unauthenticated user modified the default sign-in method for the EWS, the user key-value pair is not contained within the message.</p>

<client computer IP address> - IP address of the client computer that sent the request to modify the default sign-in method for the EWS.

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>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A new sign-in method was assigned to a control panel application.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><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.</p> <p><value> - New sign-in method. Possible values are:</p> <ul style="list-style-type: none">• local_device• ldap• windows• smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p> <p><old value> - Old sign-in method. Possible values are:</p> <ul style="list-style-type: none">• local_device• ldap• windows• smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p> <p><user> - Authenticated user who modified the sign-in method assigned to the control panel application. If an unauthenticated user modified the sign-in method assigned to the application, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the sign-in method assigned to the application.</p>

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>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The sign-in method assigned to an EWS tab was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><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.</p> <p><value> - New sign-in method. Possible values are:</p>

- local_device
- ldap
- windows
- smartcard

Possible values also include the names of third-party authentication agents that have been installed on the device.

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

- local_device
- ldap
- windows
- smartcard

Possible values also include the names of third-party authentication agents that have been installed on the device.

<user> - Authenticated user who modified the sign-in method assigned to the EWS tab. If an unauthenticated user modified the sign-in method assigned to the EWS tab, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the sign-in method assigned to the EWS tab.

Custom permission sets

Message:	<i><device type></i> : Permission Set added; time=" <i><timestamp></i> " permission_set=" <i><permission set></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A custom permission set was added.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><permission set></i> - Custom permission set added.</p> <p><i><user></i> - Authenticated user who added the custom permission set. If an unauthenticated user added the permission set, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to add the custom permission set.</p>
Message:	<i><device type></i> : Permission Set modified; time=" <i><timestamp></i> " permission_set=" <i><permission set></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The name of a custom permission set was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><permission set></i> - Custom permission set modified.</p> <p><i><user></i> - Authenticated user who modified the custom permission set. If an unauthenticated user modified the custom permission set, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the custom permission set.</p>

Message:	<code><device type>: Permission Set copied; time="<timestamp>" permission_set="<permission set>" copied_from_permission_set="<base permission set>" user="<user>" source_IP="<client computer IP address>" outcome=success</code>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A custom permission set was added by copying an existing permission set.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><permission set></code> - Custom permission set added.</p> <p><code><base permission set></code> - Base permission set for the custom permission set that was added. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><code><user></code> - Authenticated user who added the custom permission set. If an unauthenticated user added the custom permission set, the user key-value pair is not contained within the message.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to add the custom permission set.</p>
Message:	<code><device type>: Permission Set deleted; time="<timestamp>" permission_set="<permission set>" user="<user>" source_IP="<client computer IP address>" outcome=success</code>
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A custom permission set was deleted.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><permission set></code> - Custom permission set that was deleted.</p> <p><code><user></code> - Authenticated user who deleted the custom permission set. If an unauthenticated user deleted the custom permission set, the user key-value pair is not contained within the message.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to delete the custom permission set.</p>

Permissions associated with permission sets

Message:	<code><device type>: Permission Set modified; time="<timestamp>" permission_set="<permission set>" permission="<permission>" value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success</code>
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A permission was either granted or denied to a permission set.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><permission set></code> - Permission set. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator

- Device User

Possible values also include any custom permission sets that have been added.

<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_granted
- access_denied

<user> - Authenticated user who modified the permission set. If an unauthenticated user modified the permission set, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to modify the permission set.

Message:	<i><device type></i> : Permission Set modified; time=" <i><timestamp></i> " permission_set=" <i><permission set></i> " permission=all_permissions value=access_denied old_value=access_granted user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	All permissions were denied to a permission set.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><permission set></i> - Permission set.</p> <p><i><user></i> - Authenticated user who denied all permissions to the permission set. If an unauthenticated user denied all permissions to the permission set, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to deny all permissions to the permission set.</p>

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

Message:	<i><device type></i> : Sign In and Permission Policy settings modified; time=" <i><timestamp></i> " item=allow_users_to_choose_alternate_sign-in_methods value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The "Allow users to choose alternate sign-in methods at the product control panel" setting was either enabled or disabled.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New setting value. Possible values are:</p> <ul style="list-style-type: none"> • enabled • disabled <p><i><old value></i> - Old setting value. Possible values are:</p> <ul style="list-style-type: none"> • enabled • disabled

<user> - Authenticated user who enabled or disabled the “Allow users to choose alternate sign-in methods at the product control panel” setting. If an unauthenticated user enabled or disabled the “Allow users to choose alternate sign-in methods at the product control panel” setting, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to enable or disable the “Allow users to choose alternate sign-in methods at the product control panel” setting.

Default permission set for network users

Message:	<i><device type></i> : Default Permission Set for sign-in method modified; time=" <i><timestamp></i> " sign-in_method= <i><sign-in method></i> permission_set=" <i><permission set></i> " old_value=" <i><old value></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	The default permission set for a sign-in method modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><sign-in method></i> - Sign-in method whose permission set was modified. Possible values are:</p> <ul style="list-style-type: none">• local_device• windows• ldap• smartcard <p><i><permission set></i> - Permission set. Possible values are:</p> <ul style="list-style-type: none">• Device Administrator• Device User <p>Possible values also include any custom permission sets that have been added.</p> <p>Possible values also include the names of third-party authentication agents installed on the device.</p> <p><i><user></i> - Authenticated user who modified the permission set assigned to the sign-in method. If an unauthenticated user modified the permission set assigned to the sign-in method, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the permission set assigned to the sign-in method.</p>

Network user to permission set relationships

Message:	<i><device type></i> : User to Permission Set Relationship added; time=" <i><timestamp></i> " network_user_name=" <i><username></i> " permission_set=" <i><permission set></i> " sign_in_method= <i><sign-in method></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A network user to permission set relationship was added.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><username></i> - Network user name specified in the network user to permission set relationship.</p>

	<p><i><permission set></i> - Permission set specified in the network user to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><i><sign-in method></i> - Sign-in method specified in the user to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p> <p><i><user></i> - Authenticated user who added the network user to permission set relationship. If an unauthenticated user added the network user to permission set relationship, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to add the network user to permission set relationship.</p>
Message:	<i><device type></i> : User to Permission Set Relationship modified; time=" <i><timestamp></i> " network_user_name=" <i><user name></i> " permission_set=" <i><permission set></i> " sign_in_method= <i><sign-in method></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	A network user to permission set relationship was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><user name></i> - Network user name specified in the network user to permission set relationship.</p> <p><i><permission set></i> - Permission set specified in the network user to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><i><sign-in method></i> - Sign-in method specified in the network user to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p> <p><i><user></i> - Authenticated user who modified the network user to permission set relationship. If an unauthenticated user modified the network user to permission set relationship, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the network user to permission set relationship.</p>

Message:	<device type>: User to Permission Set Relationship deleted; time="<timestamp>" network_user_name="<username>" permission_set="<permission set>" sign_in_method="<sign-in method>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A network user to permission set relationship was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><username> - Network user name specified in the user to permission set relationship.</p> <p><permission set> - Permission set specified in the user to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><sign-in method> - Sign-in method specified in the user to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p> <p><user> - Authenticated user who deleted the user to permission set relationship. If an unauthenticated user deleted the user to permission set relationship, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to the delete the user to permission set relationship.</p>
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>" outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	All network user to permission set relationships for a specific remote sign-in method were deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><sign-in method> - Sign-in method specified in the user to permission set relationships. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p>

<user> - Authenticated user who deleted all user to permission set relationships. If an unauthenticated user deleted all user to permission set relationships, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to delete all network user to permission set relationships.

Network group to permission set relationships

Message:	<i><device type></i> : Group to Permission Set Relationship added; time=" <i><timestamp></i> " network_group_name=" <i><group name></i> " permission_set=" <i><permission set></i> " sign_in_method= <i><sign-in method></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A network group to permission set relationship was added.
Variables:	<i><device type></i> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<group name> - Network group name specified in the network group to permission set relationship.

<permission set> - Permission set specified in the network group to permission set relationship. Possible values are:

- Device Administrator
- Device User

Possible values also include any custom permission sets that have been added.

<sign-in method> - Sign-in method specified in the network group to permission set relationship. Possible values are:

- local_device
- windows
- ldap
- smartcard

Possible values also include the names of third-party authentication agents that have been installed on the device.

<user> - Authenticated user who added the network group to permission set relationship. If an unauthenticated user added the network to permission set relationship, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to add the network group to permission set relationship.

Message:	<i><device type></i> : Group to Permission Set Relationship modified; time=" <i><timestamp></i> " network_group_name=" <i><group name></i> " permission_set=" <i><permission set></i> " sign_in_method= <i><sign-in method></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	A network group to permission set relationship was modified.
Variables:	<i><device type></i> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

	<p><i><group name></i> - Network group name specified in the network group to permission set relationship.</p> <p><i><permission set></i> - Permission set specified in the network group to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><i><sign-in method></i> - Sign-in method that was used to perform authentication. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents that have been installed on the device.</p> <p><i><user></i> - Authenticated user who modified the network group to permission set relationship. If an unauthenticated user modified the network group to permission set relationship, the user key-value pair is not contained within the message.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the network group to permission set relationship.</p>
Message:	<i><device type></i> : Group to Permission Set Relationship deleted; time=" <i><timestamp></i> " network_group_name=" <i><group name></i> " permission_set=" <i><permission set></i> " sign_in_method= <i><sign-in method></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A network group to permission set relationship was deleted.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><group name></i> - Network group name.</p> <p><i><permission set></i> - Permission set specified in the network group to permission set relationship. Possible values are:</p> <ul style="list-style-type: none"> • Device Administrator • Device User <p>Possible values also include any custom permission sets that have been added.</p> <p><i><sign-in method></i> - Sign-in method that was used to perform authentication. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents installed on the device.</p> <p><i><user></i> - Authenticated user who deleted the network group to permission set relationship. If an unauthenticated user attempted to delete the network group to permission set relationship, the user key-value pair is not contained within the message.</p>

	<client computer IP address> - IP address of the client computer that sent the request to delete the network group to permission set relationship.
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>" outcome=success
Interface(s):	WS*
Syslog severity:	Informational
Explanation:	All group to permission set relationships for a specific remote sign-in method were deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><sign-in method> - Sign-in method that was specified in network group to permission set relationships. Possible values are:</p> <ul style="list-style-type: none"> • local_device • windows • ldap • smartcard <p>Possible values also include the names of third-party authentication agents installed on the device.</p> <p><user> - Authenticated user who deleted all the network group to permission set relationships. If an unauthenticated user deleted all network group to permission set relationships, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete all network group to permission set relationships.</p>

Certificates

CA certificates

Message:	<device type>: Device CA certificate installed; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*, OXPd
Syslog severity:	Informational
Explanation:	A device CA certificate was installed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who installed the device CA certificate. If an unauthenticated user installed the device CA certificate, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to install the device CA certificate.</p>
Message:	<device type>: Device CA certificate deleted; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*, OXPd
Syslog severity:	Informational
Explanation:	A device CA certificate was deleted.
Variables:	<device type> - see Table 2-2 .

	<timestamp> - see Table 2-2 .
	<user> - Authenticated user who deleted the device CA certificate. If an unauthenticated user deleted the device CA certificate, the user key-value pair is not contained within the message.
	<client computer IP address> - IP address of the client computer that sent the request to delete the device CA certificate.
Message:	<device type>: CA certificate installed; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS (Networking tab)
Syslog severity:	Warning
Explanation:	A CA certificate was installed.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<client computer IP address> - IP address of the client computer that sent the request to install the CA certificate.
Message:	<device type>: CA certificate deleted; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS (Networking tab)
Syslog severity:	Warning
Explanation:	A CA certificate was deleted.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<client computer IP address> - IP address of the client computer that sent the request to delete the CA certificate.

Identity certificates

Message:	<device type>: Self-signed device Identity certificate created; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A new self-signed device identity certificate was generated.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .
	<client computer IP address> - IP address of the client computer that sent the request to generate a new self-signed device identity certificate.
Message:	<device type>: Device Identity CSR created; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A device identity certificate signing request was generated.
Variables:	<device type> - see Table 2-2 .
	<timestamp> - see Table 2-2 .

<client computer IP address> - IP address of the client computer that sent the request to generate a device identity certificate signing request.	
Message:	<device type>: Device Identity certificate from CSR installed; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A device identity certificate generated from a certificate signing request was installed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><client computer IP address> - IP address of the client computer that sent the request to install the device identity certificate.</p>
Message:	<device type>: Device Identity certificate installed; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	A device identity certificate was installed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who installed the device identity certificate. If an unauthenticated user installed the device identity certificate, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to install the device identity certificate.</p>
Message:	<device type>: Device Identity certificate and private key installed; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A device identity certificate with private key was installed.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who installed the device identity certificate with private key. If an unauthenticated user installed the device identity certificate with private key, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to install the device identity certificate with private key.</p>
Message:	<device type>: Device Identity certificate deleted; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A device identity certificate was deleted.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<user> - Authenticated user who deleted the device identity certificate. If an unauthenticated user deleted the device identity certificate, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to delete the device identity certificate.

Message:	<device type>: Device Identity certificate for network identity selected; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A new device identity certificate was selected for network identity.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<user> - Authenticated user who selected the new device identity certificate for network identity. If an unauthenticated user who selected the new device identity certificate for network identity, the user key-value pair is not contained within the message.

<client computer IP address> - IP address of the client computer that sent the request to select a new device identity certificate for network identity.

Message:	<device type>: Device Identity certificate for e-mail selected; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS, WS*
Syslog severity:	Informational
Explanation:	A new device identity certificate was selected for email signing.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<client computer IP address> - IP address of the client computer that sent the request to select a new device identity certificate for email signing.

Message:	<device type>: Jetdirect Identity certificate modified; time="<timestamp>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS (Networking tab)
Syslog severity:	Warning
Explanation:	An identity certificate was installed or a self-signed certificate was created.
Variables:	<device type> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<client computer IP address> - IP address of the client computer that sent the request to install the identity certificate or generate the self-signed identity certificate.

Kerberos server certificate validation

Message:	<device type>: Online Certificate Status Protocol URL added; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational

Explanation:	An Online Certificate Status Protocol URL was added for Kerberos server certificate validation.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who added the Online Certificate Status Protocol URL. If an unauthenticated user added the Online Certificate Status Protocol URL, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to add the Online Certificate Status Protocol URL.</p>
Message:	<device type>: Online Certificate Status Protocol URL deleted; time=" <timestamp>" user=" <user>" source_IP=" <client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	An Online Certificate Status Protocol URL for Kerberos server certificate validation was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who deleted the Online Certificate Status Protocol URL. If an unauthenticated user deleted the Online Certificate Status Protocol URL, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete the Online Certificate Status Protocol URL.</p>
Message:	<device type>: Certification Validation settings modified; time=" <timestamp>" user=" <user>" source_IP=" <client computer IP address>" outcome=success
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	<p>A certificate validation setting for Kerberos server certificate validation was modified.</p> <p>This message is generated when any one of the following setting modifications are made:</p> <ul style="list-style-type: none"> Switching between "Do not validate server certificate", "Perform OCSP Validation On the certificate trust chain", and "Perform CDP Validation on the certificate trust chain." Enabling or disabling the "Treat unknown certificate status as valid" function.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - Authenticated user who modified the certificate validation setting. If an unauthenticated user modified the certificate validation setting, the user key-value pair is not contained within the message.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the certificate validation setting.</p>

HP Connection Inspector

Message:	<device type>: HP Connection Inspector enabled; time=" <timestamp>" user=" <user>" source_IP=" <client computer IP address>" outcome=success interface= <interface>
Interface(s):	EWS
Syslog severity:	Informational

Explanation:	HP Connector Inspector feature was enabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who enabled the HP Connection Inspector.</p> <p><client computer IP address> - IP address of the client computer from which the request to the enable HP Connection Inspector feature was received.</p> <p><interface> - Networking interface on the local device that received the request to enable HP Connection Inspector feature. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: HP Connection Inspector disabled; time="<timestamp>" user="<user>" source_IP="<client computer IP address>" outcome=success interface= <interface>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	HP Connector Inspector feature was disabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><user> - User who disabled the HP Connection Inspector.</p> <p><client computer IP address> - IP address of the client computer from which the request to the disable HP Connection Inspector feature was received.</p> <p><interface> - Networking interface on the local device that received the request to disable HP Connection Inspector feature. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: HP Connection Inspector Protected Mode settings modified; time="<timestamp>" item=dns_failure_threshold value= <value> old_value= <old value> user="<user>" source_IP="<client computer IP address>" outcome=success interface= <interface>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The DNS failure threshold setting for the HP Connection Inspector feature was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - User who modified the DNS failure threshold setting.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the DNS failure threshold setting.</p> <p><interface> - Networking interface on the local device that received the request to modify the DNS failure threshold setting. Possible values are:</p>

	<ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : HP Connection Inspector Protected Mode settings modified; time=" <i><timestamp></i> " item=monitoring_window value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The monitoring window setting for the HP Connection Inspector feature was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New setting value.</p> <p><i><old value></i> - Old setting value.</p> <p><i><user></i> - User who modified the monitoring window setting.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the monitoring window setting.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the monitoring window setting. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : HP Connection Inspector Protected Mode settings modified; time=" <i><timestamp></i> " item=protected_mode_duration value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The protected mode duration setting for the HP Connection Inspector feature was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New setting value.</p> <p><i><old value></i> - Old setting value.</p> <p><i><user></i> - User who modified the protected mode duration setting.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the protected mode duration setting.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the protected mode duration setting. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : HP Connection Inspector Protected Mode settings modified; time=" <i><timestamp></i> " item=number_of_times_in_protected_mode value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success

Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The number of times in protected mode setting for the HP Connection Inspector feature was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - User who modified the number of times in protected mode setting.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the number of times in protected mode setting.</p>
Message:	<device type>: HP Connection Inspector Protected Mode settings modified; time=" <timestamp>" item=cumulative_protected_mode_duration value= <value> old_value= <old value> user=" <user>" source_IP=" <client computer IP address>" outcome=success interface= <interface>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	The cumulative protected mode duration setting for the HP Connection Inspector feature was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><value> - New setting value.</p> <p><old value> - Old setting value.</p> <p><user> - User who modified the number of times in protected mode setting.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the cumulative protected mode duration setting.</p> <p><interface> - Networking interface on the local device that received the request to modify the cumulative protected mode duration setting. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: HP Connection Inspector Advanced settings modified; time=" <timestamp>" action=whitelist-exception_list_entry_added value=" <entry>" user=" <user>" source_IP=" <client computer address>" outcome=success interface= <interface>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	An entry was added to the whitelist / exception list for the HP Connection Inspector feature.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><entry> - Entry added to the whitelist / exception list.</p> <p><user> - User who added the entry to the whitelist / exception list.</p>

	<p><i><client computer IP address></i> - IP address of the client computer that sent the request to add the entry to the whitelist / exception list.</p> <p><i><interface></i> - Networking interface on the local device that received the request to add the entry to the whitelist / exception list. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : HP Connection Inspector Advanced settings modified; time=" <i><timestamp></i> " action=whitelist-exception_list_entry_deleted value=" <i><entry></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	An entry was deleted from the whitelist / exception list for the HP Connection Inspector feature.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><entry></i> - Entry deleted from the whitelist / exception list.</p> <p><i><user></i> - User who deleted the entry from the whitelist / exception list.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to delete the entry from the whitelist / exception list.</p> <p><i><interface></i> - Networking interface on the local device that received the request to delete the entry from the whitelist / exception list. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : HP Connection Inspector settings modified; time=" <i><timestamp></i> " action=factory_defaults_restored user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Informational
Explanation:	HP Connection Inspector feature settings were restored to factory defaults.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><user></i> - User who restored factor defaults.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to restore factory defaults.</p> <p><i><interface></i> - Networking interface on the local device that received the request to restore factor defaults. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

IPsec/Firewall

IPsec/Firewall policy

Message:	<i><device type></i> : IPsec/Firewall enabled; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The IPsec/Firewall policy was enabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - User who enabled the IPsec/Firewall policy. <i><client computer IP address></i> - IP address of the client computer that sent the request to enable the IPsec/Firewall policy <i><interface></i> - Networking interface on the local device that received the request to enable the IPsec/Firewall policy. Possible values are: <ul style="list-style-type: none">• Wired• AP• STA

Message:	<i><device type></i> : IPsec/Firewall disabled; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS, telnet
Syslog severity:	Warning
Explanation:	IPsec/Firewall policy was disabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - User who disabled the IPsec/Firewall policy. <i><client computer IP address></i> - IP address of the client computer that sent the request to disable the IPsec/Firewall policy <i><interface></i> - Networking interface on the local device that received the request to disable the IPsec/Firewall policy. Possible values are: <ul style="list-style-type: none">• Wired• AP• STA

Message:	<i><device type></i> : IPsec/Firewall disabled; time=" <i><timestamp></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	SNMP
Syslog severity:	Warning
Explanation:	The IPsec/Firewall policy was disabled.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><user></i> - Current EWS user.

	<p><i><client computer IP address></i> - IP address of the client computer that sent the request to disable the IPsec/Firewall policy.</p> <p><i><interface></i> - Networking interface on the local device that received the request to disable the IPsec/Firewall policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : IPsec/Firewall disabled; time=" <i><timestamp></i> " user="Guest" source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	Control panel
Syslog severity:	Warning
Explanation:	The IPsec/Firewall policy was disabled.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><interface></i> - Networking interface on the local device. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

IPsec/Firewall rules

Message:	<i><device type></i> : IPsec/Firewall rule added; time=" <i><timestamp></i> " rule= <i><rule index></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall rule was added.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><rule index></i> - Index of rule in the rules list. Possible values are: 1 - 10</p> <p><i><user></i> - User who added the IPsec/Firewall rule.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to add the IPsec/Firewall rule.</p> <p><i><interface></i> - Networking interface on the local device that received the request to add the IPsec/Firewall rule. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : IPsec/Firewall rule position changed; time=" <i><timestamp></i> " rule_ <i><old index></i> _moved_to_ <i><new index></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	Index of an IPsec/Firewall rule in the rules list was modified.
Variables:	<i><device type></i> - see Table 2-2 .

	<p><timestamp> - see Table 2-2.</p> <p><old index> - Old index of the rule in the rules list. Possible values are: 1 - 10</p> <p><new index> - New index of the rule in the rules list. Possible values are: 1 - 10</p> <p><user> - User who modified the index of the rule in the rules list.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the index of the rule.</p> <p><interface> - Networking interface on the local device that received the request to modify the index of the rule. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: IPsec/Firewall rule deleted; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall rule was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><rule index> - Index of rule in the rules list. Possible values are: 1 - 10</p> <p><user> - User who deleted the IPsec/Firewall rule.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete the IPsec/Firewall rule.</p> <p><interface> - Networking interface on the device that received the request to delete the IPsec/Firewall rule. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: IPsec/Firewall rule enabled; time="<timestamp>" rule=<rule index> user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall rule was enabled.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><rule index> - Index of rule in the rules list. Possible values are: 1 - 10</p> <p><user> - User who enabled the IPsec/Firewall rule.</p> <p><client computer IP address> - IP address of the client computer that sent the request to enable the IPsec/Firewall rule.</p> <p><interface> - Networking interface on the device that received the request to enable the IPsec/Firewall rule. Possible values are:</p> <ul style="list-style-type: none"> • Wired

	<ul style="list-style-type: none"> • AP • STA
Message:	<i><device type></i> : IPsec/Firewall rule disabled; time=" <i><timestamp></i> " rule= <i><rule number></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall rule was disabled.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><rule index></i> - Index of rule in the rules list. Possible values are: 1 - 10</p> <p><i><user></i> - User who disabled the IPsec/Firewall rule.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to disable the IPsec/Firewall rule.</p> <p><i><interface></i> - Networking interface on the device that received the request to disable the IPsec/Firewall rule. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : IPsec/Firewall default rule action modified; time=" <i><timestamp></i> " value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The action-on-match for the default IPsec/Firewall rule was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><value></i> - New action-on-match. Possible values are:</p> <ul style="list-style-type: none"> • allow • drop <p><i><old value></i> - Old action-on-match. Possible values are:</p> <ul style="list-style-type: none"> • allow • drop <p><i><user></i> - User who modified the action-on-match for the default IPsec/Firewall rule.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the action-on-match for the default IPsec/Firewall rule.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the action-on-match for the default IPsec/Firewall rule. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

IPsec/Firewall address templates

Message:	<code><device type>: IPsec/Firewall address policy added; time="<timestamp>" policy_name="<name>" user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall address template was added.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><name></code> - Template name.</p> <p><code><user></code> - User who added the IPsec/Firewall address template.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to add the IPsec/Firewall address template.</p> <p><code><interface></code> - Networking interface on the local device that received the request to add the IPsec/Firewall address template. Possible values are:</p> <ul style="list-style-type: none">• Wired• AP• STA
Message:	<code><device type>: IPsec/Firewall address policy modified; time="<timestamp>" policy_name="<name>" user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall address template was modified.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><name></code> - Template name.</p> <p><code><user></code> - User who modified the IPsec/Firewall address template.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to modify the IPsec/Firewall address template.</p> <p><code><interface></code> - Networking interface on the local device that received the request to modify the IPsec/Firewall address template. Possible values are:</p> <ul style="list-style-type: none">• Wired• AP• STA
Message:	<code><device type>: IPsec/Firewall address policy deleted; time="<timestamp>" policy_name="<name>" user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall address template was deleted.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p>

<name> - Template name.

<user> - User who deleted the IPsec/Firewall address template.

<client computer IP address> - IP address of the client computer that sent the request to delete the IPsec/Firewall address template.

<interface> - Networking interface on the local device that received the request to delete the IPsec/Firewall address template. Possible values are:

- Wired
 - AP
 - STA
-

IPsec/Firewall service templates

Message:	<device type>: IPsec/Firewall service policy added; time="<timestamp>" policy_name="<name>" user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall service template was added.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - Template name.</p> <p><user> - User who added the IPsec/Firewall service template.</p> <p><client computer IP address> - IP address of the client computer that sent the request to add the IPsec/Firewall service template.</p> <p><interface> - Networking interface on the local device that received the request to add the IPsec/Firewall service template. Possible values are:</p> <ul style="list-style-type: none">• Wired• AP• STA

Message:	<device type>: IPsec/Firewall service policy modified; time="<timestamp>" policy_name="<name>" user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall service template was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - Template name.</p> <p><user> - User who modified the IPsec/Firewall service template.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec/Firewall service template.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec/Firewall service template. Possible values are:</p> <ul style="list-style-type: none">• Wired

	<ul style="list-style-type: none"> • AP • STA
Message:	<code><device type></code> : IPsec/Firewall service policy deleted; time=" <code><timestamp></code> " policy_name=" <code><name></code> " user=" <code><user></code> " source_IP=" <code><client computer IP address></code> " outcome=success interface= <code><interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall service template was deleted.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><name></code> - Template name.</p> <p><code><user></code> - User who deleted the IPsec/Firewall address template.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to delete the IPsec/Firewall address template.</p> <p><code><interface></code> - Networking interface on the local device that received the request to delete the IPsec/Firewall address template. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

IPsec/Firewall advanced options

Message:	<code><device type></code> : IPsec/Firewall configuration change; time=" <code><timestamp></code> " item=advanced_settings value= <code><advanced option></code> user=" <code><user></code> " source_IP=" <code><client computer IP address></code> " outcome=success interface= <code><interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IPsec/Firewall policy advanced option was modified.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><advanced option></code> - IPsec/Firewall policy advanced option that was modified. Possible values are:</p> <ul style="list-style-type: none"> • 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 <p><code><user></code> - User who modified the IPsec/Firewall policy advanced option.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to modify the IPsec/Firewall policy advanced option.</p>

<interface> - Networking interface on the local device that received the request to modify the IPsec/Firewall policy advanced option. Possible values are:

- Wired
 - AP
 - STA
-

IPsec policy with manual keying

Message:	<i><device type></i> : IPsec policy added; time=" <i><timestamp></i> " policy_name=" <i><name></i> " item=authentication_method value=Manual_keys user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
-----------------	--

Interface(s):	EWS
----------------------	-----

Syslog severity:	Warning
-------------------------	---------

Explanation:	A manual keys IPsec policy was added.
---------------------	---------------------------------------

Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><name></i> - Policy name. <i><user></i> - User who added the IPsec policy. <i><client computer IP address></i> - IP address of the client computer that sent the request to add the IPsec policy.
-------------------	--

<interface> - Networking interface on the local device that received the request to add the IPsec policy. Possible values are:

- Wired
 - AP
 - STA
-

Message:	<i><device type></i> : IPsec policy Modified ; time=" <i><timestamp></i> " policy_name=" <i><name></i> " item=authentication_method value=IKEv1 old_value=Manual_Keys identity_authentication_option= <i><identity authentication option></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
-----------------	--

Interface(s):	EWS
----------------------	-----

Syslog severity:	Warning
-------------------------	---------

Explanation:	A manual keys IPsec policy was modified and converted into an IKEv1 IPsec policy.
---------------------	---

Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><name></i> - IPsec policy name. <i><identity authentication option></i> - Authentication method that will be used to mutually authenticate both endpoints. Possible values are: <ul style="list-style-type: none">• Pre-shared_key• Certificates• Kerberos <i><user></i> - User who modified the IPsec policy. <i><client computer IP address></i> - IP address of the client computer that sent the request to modify the IPsec policy. <i><interface></i> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are: <ul style="list-style-type: none">• Wired
-------------------	--

	<ul style="list-style-type: none"> • AP • STA
Message:	<p><device type>: IPsec policy Modified; time=" <timestamp>" policy_name=" <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>" source_IP=" <client computer IP address>" outcome=success interface= <interface></p>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	A manual keys IPsec policy was modified and converted into an IKEv2 IPsec policy.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><local identity authentication option> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><remote identity authentication option> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><user> - User who modified the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<p><device type>: IPsec policy modified; time=" <timestamp>" policy_name=" <name>" item=authentication_method value=Manual_keys old_value=IKEv1 user=" <user>" source_IP=" <client computer IP address>" outcome=success interface= <interface></p>
Interface(s):	EWS

Syslog severity:	Warning
Explanation:	An IKEv1 IPsec policy was modified and converted into a manual keys IPsec policy.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><user> - User who modified the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: IPsec policy modified; time="<timestamp>" policy_name="<name>" item=authentication_method value=Manual_keys old_value=IKEv2 user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IKEv2 IPsec policy was modified and converted into manual keys IPsec policy.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><user> - User who modified the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: IPsec policy deleted; time="<timestamp>" policy_name="<name>" item=authentication_method value=Manual_keys user="<user>" source_IP="<client computer IP address>" outcome=success interface=<interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	A manual keys IPsec policy was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><user> - User who deleted the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to delete the IPsec policy.</p>

<interface> - Networking interface on the local device that received the request to delete the IPsec policy. Possible values are:

- Wired
 - AP
 - STA
-

IPsec policy with IKEv1

Message:	<i><device type></i> : IPsec policy added; time=" <i><timestamp></i> " policy_name=" <i><name></i> " item=identity_authentication_option value= <i><value></i> user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IKEv1 IPsec policy was added.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><name></i> - IPsec policy name. <i><value></i> - Authentication method that will be used by both endpoints to perform mutual authentication. Possible values are: <ul style="list-style-type: none">• Pre-shared_key• Certificates• Kerberos <i><user></i> - User who added the IPsec policy. <i><client computer IP address></i> - IP address of the client computer that sent the request to add the IPsec policy. <i><interface></i> - Networking interface on the local device that received the request to add the IPsec policy. Possible values are: <ul style="list-style-type: none">• Wired• AP• STA

Message:	<i><device type></i> : IPsec policy modified; time=" <i><timestamp></i> " policy_name=" <i><name></i> " item=identity_authentication_option value= <i><value></i> old_value= <i><old value></i> user=" <i><user></i> " source_IP=" <i><client computer address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IKEv1 IPsec policy was modified.
Variables:	<i><device type></i> - see Table 2-2 . <i><timestamp></i> - see Table 2-2 . <i><name></i> - IPsec policy name. <i><value></i> - Authentication method that will be used by both endpoints to perform mutual authentication. Possible values are: <ul style="list-style-type: none">• Pre-shared_key• Certificates• Kerberos <i><old value></i> - Previous authentication method used by both endpoints to perform mutual authentication. Possible values are: <ul style="list-style-type: none">• Pre-shared_key

	<ul style="list-style-type: none"> • Certificates • Kerberos <p><user> - User who modified the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: IPsec policy modified; time="<timestamp>" policy_name="<name>" item=authentication_type value=IKEv1 old_value=IKEv2 identity_authentication_option value="<value>" user="<user>" source_IP="<client computer IP address>" outcome=success interface="<interface>"
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IKEv2 IPsec policy was modified and converted into an IKEv1 IPsec policy.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><value> - Authentication method that will be used by both endpoints to perform mutual authentication. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates • Kerberos <p><user> - User who modified the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: IPsec policy deleted; time="<timestamp>" policy_name="<name>" item=identity_authentication_option value="<value>" user="<user>" source_IP="<client computer IP address>" outcome=success interface="<interface>"
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IKEv1 IPsec policy was deleted.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><value> - Authentication method that was used by both endpoints to perform mutual authentication. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key

- Certificates
- Kerberos

<user> - User who deleted the IPsec policy.

<client computer IP address> - IP address of the client computer that sent the request to delete the IPsec policy.

<interface> - Networking interface on the local device that received the request to delete the IPsec policy. Possible values are:

- Wired
- AP
- STA

IPsec policy with IKEv2

Message:	<i><device type></i> : IPsec policy added; time=" <i><timestamp></i> " policy_name=" <i><name></i> " local_identity_authentication_option= <i><local identity authentication option></i> local_identityType=" <i><local identity type></i> " remote_identity_authentication_option= <i><remote identity authentication option></i> remote_identity_type=" <i><remote identity type></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
-----------------	---

Interface(s):	EWS
----------------------	-----

Syslog severity:	Warning
-------------------------	---------

Explanation:	An IKEv2 IPsec policy was added.
---------------------	----------------------------------

Variables:	<i><device type></i> - see Table 2-2 .
-------------------	--

<timestamp> - see [Table 2-2](#).

<name> - IPsec/Firewall template name.

<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

<user> - User who added the IPsec policy.

<client computer IP address> - IP address of the client computer that sent the request to add the IPsec policy.

	<p><i><interface></i> - Networking interface on the local device that received the request to add the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<p><i><device type></i>: IPsec policy modified; time="<i><timestamp></i>" policy_name="<i><name></i>" item=local_identity_type value="<i><value></i>" old_value="<i><old value></i>" local_identity_authentication_option= <i><local identity authentication option></i> user="<i><user></i>" source_IP="<i><client computer IP address></i>" outcome=success interface= <i><interface></i></p>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The local identity type in an IKEv2 IPsec policy was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><name></i> - IPsec policy name.</p> <p><i><value></i> - Identity type the IPsec peer will use to identify the local device. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><i><old value></i> - Previous identity type that was used by the IPsec peer to identify the local device. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><i><local identity authentication option></i> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><i><user></i> - User who modified the IPsec policy.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<p><i><device type></i>: IPsec policy modified; time="<i><timestamp></i>" policy_name="<i><name></i>" item=Identity local_identity_authentication_option= <i><local identity authentication option></i> local_identity_type="<i><local identity type></i>" user="<i><user></i>" source_IP="<i><client computer IP address></i>" outcome=success interface= <i><interface></i></p>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The local identity in an IKEv2 IPsec policy was modified.
Variables:	<i><device type></i> - see Table 2-2 .

<timestamp> - see [Table 2-2](#).

<name> - IPsec policy name.

<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

<user> - User who modified the IPsec policy.

<client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.

<interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:

- Wired
 - AP
 - STA
-

Message:	<device type>: IPsec policy modified; time="<timestamp>" policy_name="<name>" item=Key local_identity_authentication_option=Pre-Shared_Key local_identity_type="<local identity type>" user="<user>" source_IP="<client computer IP address>" outcome=success interface="<interface>"
-----------------	---

Interface(s):	EWS
----------------------	-----

Syslog severity:	Warning
-------------------------	---------

Explanation:	The pre-shared key contained in an IKEv2 IPsec policy was modified.
---------------------	---

Variables:	<device type> - see Table 2-2 . <timestamp> - see Table 2-2 . <name> - IPsec policy name. <local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are: <ul style="list-style-type: none">• Distinguished_Name• FQDN• E-mail• IP_Address• Key-ID <client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy. <interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are: <ul style="list-style-type: none">• Wired• AP• STA
-------------------	--

Message:	<device type>: IPsec policy modified; time="<timestamp>" policy_name="<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>" outcome=success interface= <interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The local identity authentication option in an IKEv2 IPsec policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><value> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><old value> - Previous local identity authentication that was used by the IPsec peer to authentication the local device. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><user> - User who modified the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

Message:	<device type>: IPsec policy modified; time="<timestamp>" policy_name="<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>" outcome=success interface= <interface>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The remote identity type in an IKEv2 IPsec policy was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec/Firewall template name.</p> <p><value> - Identity type the local device will use to identify the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address

	<ul style="list-style-type: none"> • Key-ID <p><i><old value></i> - Previous identity type the local device used to identify the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><i><remote identity authentication option></i> - Authentication method the local device will use to authentication the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Certificates • Pre-Shared_Key <p><i><user></i> - User who modified the IPsec policy.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : IPsec policy modified; time=" <i><timestamp></i> " policy_name=" <i><name></i> " item=Identity remote_identity_authentication_option= <i><remote identity authentication option></i> remote_identity_type=" <i><remote identity type></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The remote identity in an IKEv2 IPsec policy was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><name></i> - IPsec policy name.</p> <p><i><remote identity authentication option></i> - Authentication method the local device will use to authentication the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Certificates • Pre-Shared_Key <p><i><remote identity type></i> - Identity type the local device will use to authenticate the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><i><user></i> - User who modified the IPsec policy.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP

	<ul style="list-style-type: none"> • STA
Message:	<i><device type></i> : IPsec policy modified; time=" <i><timestamp></i> " policy_name=" <i><name></i> " item=Key remote_identity_authentication_option=Pre-Shared_Key remote_identity_type=" <i><remote identity type></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The pre-shared key contained in an IKEv2 IPsec policy was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><name></i> - IPsec policy name.</p> <p><i><remote identity type></i> - Identity type the local device will use to identify the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><i><user></i> - User who modified the IPsec policy.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<i><device type></i> : IPsec policy modified; time=" <i><timestamp></i> " policy_name=" <i><name></i> " item=remote_identity_authentication_option value= <i><value></i> old_value= <i><old value></i> remote_identity_type=" <i><remote identity type></i> " user=" <i><user></i> " source_IP=" <i><client computer IP address></i> " outcome=success interface= <i><interface></i>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The remote identity authentication option in an IKEv2 IPsec policy was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><name></i> - IPsec policy name.</p> <p><i><value></i> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Pre-Shared_Key • Certificates <p><i><old value></i> - Previous authentication method the local device used to authenticate the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Pre-Shared_Key • Certificates <p><i><remote identity type></i> - Identity type the local device will use to identify the IPsec peer. Possible values are:</p>

	<ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><user> - User who modified the IPsec policy.</p> <p><client computer IP address> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><interface> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<p><device type>: IPsec policy modified; time="<timestamp>" policy_name="<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>" outcome=success interface= <interface></p>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IKEv1 IPsec policy was modified and converted into an IKEv2 IPsec policy.
Variables:	<p><device type> - see Table 2-2.</p> <p><timestamp> - see Table 2-2.</p> <p><name> - IPsec policy name.</p> <p><local identity authentication option> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><local identity type> - Identity type the IPsec peer will use to identify the local device. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><remote identity authentication option> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><remote identity type> - Identity type the local device will use to identify the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><user> - User who modified the IPsec policy.</p>

	<p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<p><i><device type></i>: IPsec policy deleted; time="<i><timestamp></i>" policy_name="<i><name></i>" local_identity_authentication_option=<i><local identity authentication option></i> local_identityType="<i><local identity type></i>" remote_identity_authentication_option=<i><remote identity authentication option></i> remote_identity_type="<i><remote identity type></i>" user="<i><user></i>" source_IP="<i><client computer IP address></i>" outcome=success interface=<i><interface></i></p>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	An IKEv2 IPsec policy was deleted.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><name></i> - IPsec policy name.</p> <p><i><local identity authentication option></i> - Authentication method the IPsec peer will use to authenticate the local device. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><i><local identity type></i> - Identity type the IPsec peer will use to identify the local device. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><i><remote identity authentication option></i> - Authentication method the local device will use to authenticate the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Pre-shared_key • Certificates <p><i><remote identity type></i> - Identity type the local device will use to identify the IPsec peer. Possible values are:</p> <ul style="list-style-type: none"> • Distinguished_Name • FQDN • E-mail • IP_Address • Key-ID <p><i><user></i> - User who modified the IPsec policy.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the IPsec policy.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the IPsec policy. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

IPsec policy with IKEv1 using Kerberos

Message:	<code><device type>: IPsec configuration change; time="<timestamp>" item=Kerberos_settings value>manual_configuration user = "<user>" source_IP="<client computer IP address>" outcome=success interface= <interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The manual configuration for Kerberos was modified.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><user></code> - User who modified the manual configuration.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to modify the manual configuration.</p> <p><code><interface></code> - Networking interface on the local device that received the request to modify the manual configuration. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<code><device type>: IPsec configuration change; time="<timestamp>" item=Kerberos_settings user = "<user>" value=conf_file source_IP="<client computer IP address>" outcome=success interface= <interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	A conf file was imported for the Kerberos.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><user></code> - User who imported the conf file.</p> <p><code><client computer IP address></code> - IP address of the client computer that sent the request to import the conf file.</p> <p><code><interface></code> - Networking interface on the local device that received the request to import the conf file. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<code><device type>: IPsec configuration change; time="<timestamp>" item=Kerberos_settings value=keytab_file user = "<user>" source_IP="<client computer IP address>" outcome=success interface= <interface></code>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	A keytab file was imported for Kerberos.
Variables:	<p><code><device type></code> - see Table 2-2.</p> <p><code><timestamp></code> - see Table 2-2.</p> <p><code><user></code> - User who imported the keytab file.</p>

	<p><i><client computer IP address></i> - IP address of the client computer that sent the request to import the keytab file.</p> <p><i><interface></i> - Networking interface on the local device that received the request to import the keytab file. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<p><i><device type></i>: IPsec configuration change; time="<i><timestamp></i>" item=Kerberos_settings value=SNTP_info user = "<i><user></i>" source_IP="<i><client computer IP address></i>" outcome=success interface= <i><interface></i></p>
Interface(s):	EWS
Syslog severity:	Warning
Explanation:	The SNTP server address for Kerberos was modified.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><timestamp></i> - see Table 2-2.</p> <p><i><user></i> - User who modified the SNTP server address.</p> <p><i><client computer IP address></i> - IP address of the client computer that sent the request to modify the SNTP server address.</p> <p><i><interface></i> - Networking interface on the local device that received the request to modify the SNTP server address. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

3 Basic logging

Message:	<i><device type></i> : IPv6 warning: Address Cache Overflow. Address: <i><IPv6 address></i> interface= <i><interface></i>
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	Configuration of IPv6 address failed.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><interface></i> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

Message:	<i><device type></i> : registered system name <i><system name></i> with WINS server <i><WINS server IP address></i> interface= <i><interface></i>
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	System name was registered with the WINS server.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><system name></i> - System name.</p> <p><i><WINS server IP address></i> - IP address of the WINS server.</p> <p><i><interface></i> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

Message:	<i><device type></i> : WINS: registration successful, inconsistency with JD database and WINS server database. interface= <i><interface></i>
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	Registration response from WINS server contained the wrong IP Address and time-to-live.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><interface></i> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

Message:	<i><device type></i> : failed to register system name <i><system name></i> with primary WINS server <i><WINS server IP address></i> interface= <i><interface></i>
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	Registration of system name with the primary WINS server failed.
Variables:	<p><i><device type></i> - see Table 2-2.</p> <p><i><system name></i> - System name.</p>

	<p><WINS server IP address> - IP address of the WINS server.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: failed to register system name <name> with secondary WINS server <WINS IP address> interface= <interface>
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	Registration of the system name with the secondary WINS server failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><system name> - System name.</p> <p><WINS server IP address> - IP address of the WINS server.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Security: Security settings reset interface= <interface>
Interface(s):	EWS, SNMP
Syslog severity:	Warning
Explanation:	JDI security settings were reset to factory defaults.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server.</p>
Message:	<device type>: network peripheral interface fatal error: <error number>
Interface(s):	N/A
Syslog severity:	Critical
Explanation:	JDI backplane state error occurred and was disconnected.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: Device assessment with configuration server failed interface= <interface>
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	Announcement agent failed to register with HP JetdAdvantage Security Manager.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA

Message:	<device type>: Security: Snmpv1/v2 get community name is not set interface= <interface>
Interface(s):	EWS, SNMP
Syslog severity:	Informational
Explanation:	SNMPv1/v2c Get community name was cleared.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Security: Snmpv1/v2 set community name is not set interface= <interface>
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	SNMPv1/v2c Set community name was cleared.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Security: Snmpv1/v2 get community name is set interface= <interface>
Interface(s):	EWS, SNMP
Syslog severity:	Informational
Explanation:	SNMPv1/v2c Get community name was set.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Security: Snmpv1/v2 set community name is set interface= <interface>
Interface(s):	EWS, SNMP
Syslog severity:	Informational
Explanation:	SNMPv1/v2c Get community name was set.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: Security: Security Configuration modified through the use of WebUI by <client computer IP address> interface= <interface>
Interface(s):	EWS

Syslog severity:	Informational
Explanation:	Jetdirect security configuration was modified.
Variables:	<p><device type> - see Table 2-2.</p> <p><client computer IP address> - IP address of the client computer that sent the configuration request.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: peripheral low-power state
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	The device entered sleep mode.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: IPv6 error: Duplicate Address Detection Failed (Manual). Address: <IPv6 address> interface= <interface>
Interface(s):	N/A
Syslog severity:	Error
Explanation:	IPv6 Duplicate Address Detection failed.
Variables:	<p><device type> - see Table 2-2.</p> <p><interface> - Networking interface on the local device that was used to send the message to the syslog server. Possible values are:</p> <ul style="list-style-type: none"> • Wired • AP • STA
Message:	<device type>: toner/ink low
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	Toner/ink low.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: paper out
Interface(s):	N/A
Syslog severity:	Error
Explanation:	Paper out.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: cover/door open

Interface(s):	N/A
Syslog severity:	Error
Explanation:	Cover/door open.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: offline or intervention needed
Interface(s):	N/A
Syslog severity:	Error
Explanation:	Offline or intervention needed.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: error cleared
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	Error cleared.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: not ready to print
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	Not ready to print.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: ready to print
Interface(s):	N/A
Syslog severity:	Informational
Explanation:	Ready to print.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: powered up
Interface(s):	N/A
Syslog severity:	Warning
Explanation:	Powered up.
Variables:	<device type> - see Table 2-2 .
Message:	<device type>: syslog started
Interface(s):	N/A
Syslog severity:	Debug
Explanation:	Syslog was started.
	This message is generated when syslog is started during system initialization.
Variables:	<device type> - see Table 2-2 .

© Copyright 2018 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.

April 2018

