Technical white paper

HP FutureSmart Printer Integration for HP ArcSight Security Information Event Management Solution

Table of contents

Introduction

HP FutureSmart printers provide event information through the standard Syslog server logging format. Advanced security logging events are now available through the “Enable CCC Logging” setting. This security event information can be sent to an active HP ArcSight Security Information and Event Manger (SIEM) solution using the included SmartConnector for HP Printers Syslog software.

Detailed Description

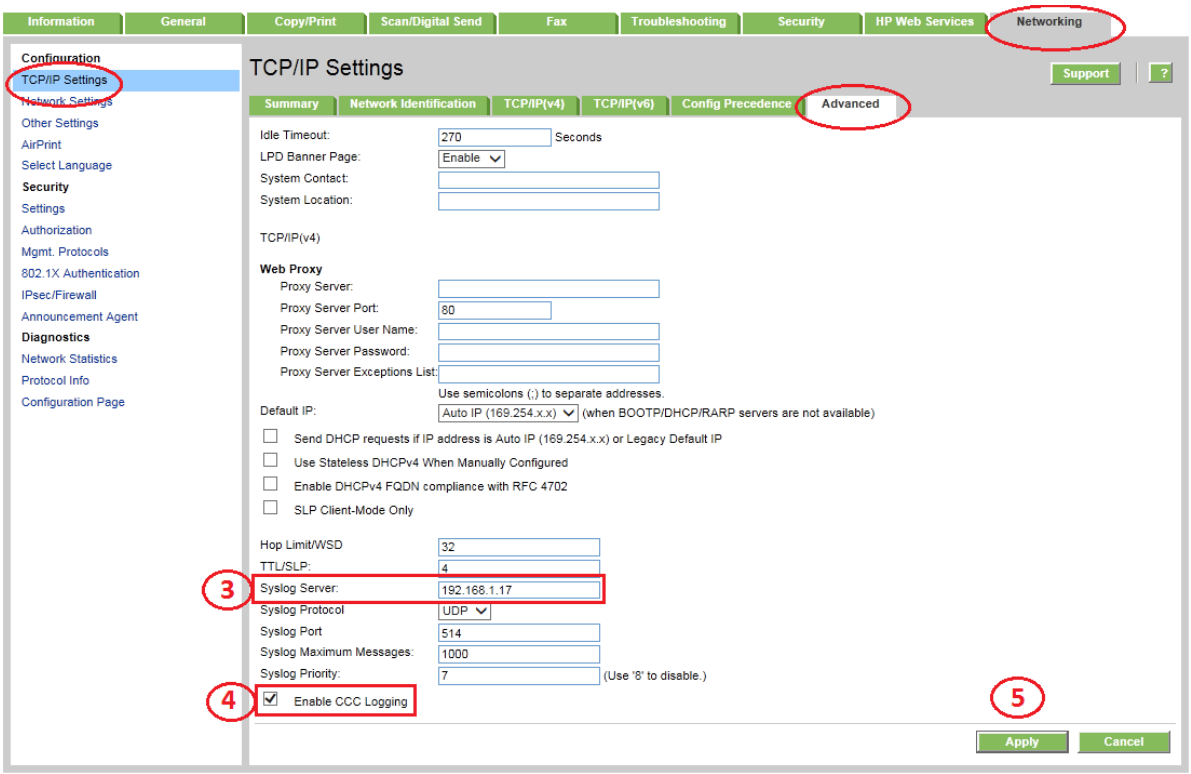
The following components are needed to configure the HP FutureSmart printers to send advanced security logging events to the HP ArcSight SIEM solution.

- An active HP ArcSight SIEM environment consisting of HP ArcSight server(s) and HP ArcSight Console applications
- The SmartConnector for HP Printers Syslog software installed within the HP ArcSight network
- HP FutureSmart printers configured to access the SmartConnector software

HP FutureSmart Printer Configuration

Follow these steps to configure HP FutureSmart printers to send security logging information to the SmartConnector

1. Using the Web interface, access the supported HP printer through any Web browser. For example: http:// <IP address of the printer>.
2. Click the **Networking** tab and the **Advanced** sub-tab.
3. Enter the IP address of the SmartConnector server in the Syslog Server field.
4. Select the Enable CCC Logging checkbox to activate the logging of advanced security events.
5. Click Apply



Supported HP FutureSmart Printers

The following HP FutureSmart printers support the “CCC Logging” setting for integration with HP ArcSight SIEM

Printer Type	Model Number
HP Color LaserJet Enterprise	M651
HP Color LaserJet Enterprise	MFP M680
HP Color LaserJet Enterprise	CP5520 Series
HP Color LaserJet Enterprise	CP5525
HP Color LaserJet Enterprise Flow	MFP M575
HP Color LaserJet Enterprise Flow	MFP M680
HP Color LaserJet Enterprise Flow	MFP M880
HP Color LaserJet	M750
HP Color LaserJet	M855
HP Color LaserJet	CM4540 MFP
HP LaserJet	M4555 MFP
HP LaserJet	500 COLOR M551
HP LaserJet	500 COLOR MFPM575
HP LaserJet	500 MFP M525
HP LaserJet	600 M601
HP LaserJet	600 M602
HP LaserJet	600 M603
HP LaserJet	MFP M630
HP LaserJet	700 COLOR MFPM775
HP LaserJet	700 M712
HP LaserJet	700 MFPM725
HP LaserJet	MFPM725
HP LaserJet	M806
HP LaserJet Enterprise Flow	MFP M525
HP LaserJet Enterprise Flow	MFP M630
HP LaserJet Enterprise Flow	MFP M830
HP OfficeJet Enterprise Color	MFP X585
HP OfficeJet Enterprise Color Flow	MFP X585
HP Digital Sender Flow	8500 fn1 Document Capture Workstation
HP Scanjet Enterprise	8500 fn1
HP Scanjet Enterprise	8500 fn1 Document Capture Workstation

Supported Syslog Security Events

Stored Job Syslog Events

- Kerberos authentication retrieving a PIN protected print job at control panel
- LDAP authentication retrieving a PIN protected print job at control panel
- User PIN authentication retrieving a PIN protected print job at control panel
- PIN protected stored copy job can be created with Kerberos Authentication
- PIN protected stored copy job can be created with LDAP Authentication
- PIN protected stored copy job can be created with User PIN Authentication
- Kerberos authentication retrieving stored fax job at control panel
- LDAP authentication retrieving stored fax job at control panel
- User PIN authentication retrieving stored fax job at control panel
- Non-PIN protected stored copy job created when authenticating via Kerberos
- Non-PIN protected stored copy job created when authenticating via LDAP
- Non-PIN protected stored copy job created when authenticating via User PIN

Control Panel Syslog Events

- User is successfully identified and authenticated via User PIN at control panel

- User is successfully identified and authenticated via Kerberos at control panel
- User is successfully identified and authenticated via LDAP at control panel
- User is NOT successfully identified and authenticated via User PIN at control panel
- User is NOT successfully identified and authenticated via Kerberos at control panel
- User is NOT successfully identified and authenticated via LDAP at control panel
- User is successfully identified and authenticated via User PIN when attempting copy at control panel
- User is successfully identified and authenticated via LDAP when attempting copy at control panel

Fax Syslog Events

- Outgoing fax sent after authenticating via Kerberos
- Outgoing fax sent after authenticating via LDAP
- Outgoing fax sent after authenticating via User PIN
- Outgoing fax archived to an email address
- Outgoing fax archived to a fax number

Fax Polling Syslog Events

- Completion of fax polling job after logging onto the control panel via Kerberos authentication
- Completion of fax polling job after logging onto the control panel via LDAP authentication
- Completion of fax polling job after logging onto the control panel via User PIN authentication

Fax Stored Job Syslog Events

- Receipt and storage of incoming fax job

Copy Syslog Events

- Copy job executed after logging on to the control panel via Kerberos authentication
- Copy job executed after logging on to the control panel via LDAP authentication
- Copy job executed after logging on to the control panel via User PIN authentication

Digital Send Syslog Events

- Document sent to e-mail after logging on to the control panel via Kerberos
- Document sent to e-mail after logging on to the control panel via LDAP
- Document sent to e-mail after logging on to the control panel via User PIN
- Document sent to a network folder after logging on to the control panel via Kerberos
- Document sent to a network folder after logging on to the control panel via LDAP
- Document sent to a network folder after logging on to the control panel via User PIN

Inactivity Timeout Syslog Events

- Inactivity timeout – User PIN authenticated
- Inactivity timeout – LDAP authenticated
- Inactivity timeout – Kerberos authenticated
- Inactivity timeout with large copy job
- Inactivity Timeout with ADF pick error condition
- Inactivity Timeout with Out of Paper error condition

User PIN Syslog Events

- New user PIN record added via EWS
- Edit User PIN record via EWS
- Delete User PIN record via EWS
- Remove all PIN records via the EWS
- Add of User PIN records by importing address book via EWS

- Remove all User PIN records by clearing Authorized User List address book via EWS
- Add of User PIN record via DSMP (DbAddRec)
- Modification of User PIN record via DSMP (DbModifyRec)
- Deletion of User PIN record via DSMP (DbDeleteRec)
- Deletion of User PIN record via DSMP (DbClearRec)
- Deletion of all User PIN records when clearing User PIN address book via DSMP (ClearMFPAddressBook)
- Address book imported with User PIN records via the DSMP - ImportAddressBooks command

Authentication Manager Syslog Events

- Modification of the Authentication Manager settings via the EWS - Walk Up
- Modification of the Authentication Manager settings via the EWS – Copy
- Modification of the Authentication Manager settings via the EWS - Color Copy
- Modification of the Authentication Manager settings via the EWS - "Send to Email"
- Modification of the Authentication Manager settings via the EWS - "Send Fax"
- Modification of the Authentication Manager settings via the EWS - "Send to Folder"
- Modification of the Authentication Manager settings via the EWS - "Job Storage"
- Modification of the Authentication Manager settings via the EWS - "Create Stored Job”
- Modification of the Authentication Manager settings via the EWS - "DSS Secondary Email”
- Modification of the Authentication Manager settings via the EWS - "DSS Workflow"
- Modification of the Authentication Manager settings via the EWS - "Newly Installed Functions"
- Modification of the Authentication Manager settings via DSMP - SetAuthentication
- Disabling/Enabling of Jetdirect logging via SNMP request

Auditing Syslog Events

- Disable/Enable Oz Logging & Auditing from the EWS
- Disable/Enable Jetdirect Logging & Auditing from the EWS

Stored Job Syslog Events

- Printing of PIN-protected stored job via SNMP wrapped PML with the correct pin

PJL Password Syslog Events

- Deletion of PJL Password via the EWS
- Set PJL Password via the EWS

File Erase Mode Syslog Events

- Modification of the File Erase Mode (Non-secure Fast Erase) via the EWS
- Modification of the File Erase Mode (Secure Fast Erase) via the EWS
- Modification of the File Erase Mode (Secure Sanitize Erase) via the EWS
- Modification of the File Erase Mode via DMCMD PJL command (Non-Secure Fast Erase)
- Modification of the File Erase Mode via DMCMD PJL command (Secure Fast Erase)
- Modification of the File Erase Mode via DMCMD PJL command (Secure Sanitize Erase)
- Modification of the File Erase Mode via DMINFO PJL command (Non-Secure Fast Erase)
- Modification of the File Erase Mode via DMINFO PJL command (Secure Fast Erase)
- Modification of the File Erase Mode via DMINFO PJL command (Secure Sanitize Erase)
- Modification of the File Erase Mode via SNMP wrapped PML request (Non -Secure Fast Erase)
- Modification of the File Erase Mode via SNMP wrapped PML request (Secure Fast Erase)
- Modification of the File Erase Mode via SNMP wrapped PML request (Secure Sanitize Erase)

Wipe Flag Syslog Events

- Secure Storage Erase function initiated via the EWS
- Modification of the Disk Wipe Flag via DMCMD PJL command
- Modification of the Disk Wipe Flag via DMINFO PJL command

- Modification of the Disk Wipe Flag via SNMP wrapped PML request

Fax Pin Syslog Events

- Set Fax PIN via the EWS
- Modification of the Fax PIN via the EWS
- Modification of the Fax PIN via DSMP (SetMfpRecordInDevice)

Certificates Syslog Events

- Deletion of a CA certificate via the EWS
- Installation of a CA certificate via the EWS
- Self-signed Jetdirect certificate generated via the EWS
- PFX certificate imported via the EWS

Date/Time Syslog Events

- Modification of the date/time settings via the EWS – date/time
- Modification of the date/time settings via the EWS – Time Zone
- Modification of the date/time settings via the EWS – Automatically adjust clock for DST
- Modification of the date/time settings via the EWS – DST Start Date
- Modification of the date/time settings via the EWS – DST End Date
- Modification of the date/time settings via the EWS – DST Offset
- Modification of the date/time settings via the EWS – DST Use Defaults
- Modification of the date/time settings via DMCMD PJL command – Date & Time
- Modification of the date/time settings via DMINFO PJL command – Date & Time
- Modification of the date/time settings via DMCMD PJL command – Time Zone
- Modification of the date/time settings via DMINFO PJL command – Time Zone
- Modification of the date/time settings via DMCMD PJL command – Automatically adjust clock for DST
- Modification of the date/time settings via DMINFO PJL command – Automatically adjust clock for DST
- Modification of the date/time settings via DMCMD PJL command – DST Start Date
- Modification of the date/time settings via DMINFO PJL command – DST Start Date
- Modification of the date/time settings via DMCMD PJL command – DST End Date
- Modification of the date/time settings via DMINFO PJL command – DST End Date
- Modification of the date/time settings via DMCMD PJL command – DST Offset
- Modification of the date/time settings via DMINFO PJL command – DST Offset
- Modification of the date/time settings via DMCMD PJL command – DST Reset
- Modification of the date/time settings via DMINFO PJL command – DST Reset
- Modification of the date/time settings via an SNMP wrapped PML request – Date & Time
- Modification of the date/time settings via an SNMP wrapped PML request – Time Zone
- Modification of the date/time settings via an SNMP wrapped PML request – Automatically adjust clock for DST
- Modification of the date/time settings via an SNMP wrapped PML request – DST Start Date
- Modification of the date/time settings via an SNMP wrapped PML request – DST End Date
- Modification of the date/time settings via an SNMP wrapped PML request – DST Offset
- Modification of the date/time settings via an SNMP wrapped PML request – DST Reset

IPSec – Service Template Syslog Events

- Addition of IPSec Service Template via the EWS
- Modification of IPSec Service Template via the EWS
- Deletion of IPSec Service Template via the EWS

IPSec – IPSec Policy Syslog Events

- Addition of an IPsec Policy (Certificates)
- Modification of an IPsec Policy via the EWS
- Deletion of an IPsec Policy via the EWS

IPSec - Address Template Syslog Events

- Addition of an Address Template via the EWS
- Modification of an Address Template via the EWS
- Deletion of an Address Template via the EWS

IPSec – Action on Match for Default Rule Syslog Events

- Modification of the action-on-match for the Default IPsec/Firewall rule via the EWS

IPSec – IPSec/Firewall Rule Syslog Events

- Addition of an IPsec/Firewall rule via the EWS
- Disable an IPsec/Firewall rule via the EWS
- Enable an IPsec/Firewall rule via the EWS
- Deletion of IPsec/Firewall rule via the EWS

IPSec – Advanced Settings

- Modification of IPSec/Firewall advanced settings via the EWS
- Modification of IPsec/Firewall advanced settings via the EWS - DHCPv4/BOOTP
- Modification of IPsec/Firewall advanced settings via the EWS - DHCPv6
- Modification of IPsec/Firewall advanced settings via the EWS - NTP
- Modification of IPsec/Firewall advanced settings via the EWS - ICMPv4
- Modification of IPsec/Firewall advanced settings via the EWS - ICMPv6
- Modification of IPsec/Firewall advanced settings via the EWS - IGMPv2
- Modification of IPsec/Firewall advanced settings via the EWS - Bonjour
- Modification of IPsec/Firewall advanced settings via the EWS – SLP
- Modification of IPsec/Firewall advanced settings via the EWS - WS-Discovery

PJL Password Syslog Events

- Modification of PJL Password via the EWS
- PJL Password is modified (using PJL command default) with PASSWORD option of JOB command

IPSec Syslog Events

- IPSec IKE Phase 1 & 2 complete success fully and MFP is responder
- Connection to device with IPSec using Diffie Hellman Group 2
- Connection to device with IPsec using Diffie Hellman Group 14
- Linux Administrative Computer connection to device using AES 128 bit encryption with a SHA1 hash algorithm
- Failure of IKE phase 1 when device is initiating communication with a computer using unsupported algorithms for Main Mode
- Failure of IKE phase 2 when device is initiating communication with a computer using unsupported algorithms for Quick Mode
- IKE phase 1 and phase 2 success when device is initiating communication with a computer using supported algorithms for both Main Mode and Quick Mode
- Failure of IKE phase 1 when device is responding to communication with a computer using unsupported algorithms for Main Mode
- Failure of IKE phase 2 when device is responding to communication with a computer using unsupported algorithms for Quick Mode
- Connect to the device via IPsec using 3DES for the encryption algorithm

For more information

To read more about HP ArcSight solution, go to: **hp.com/go/arcsight**

hp.com/go/support

Current HP driver, support, and security alerts
delivered directly to your desktop

4AA4-xxxxENW, Updated March 2016
Public