HP ArcSight Port and Protocol Information

Important Notice

The information (data) contained on all sheets of this document constitutes confidential information of Hewlett-Packard Company or its affiliates (collectively hereinafter “HP”) and is provided for evaluation purposes only. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and to not reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, unless otherwise authorized by HP in writing. There is no obligation to maintain the confidentiality of any such information which was known to recipient without restriction prior to receipt of this document as evidenced by written business records; which becomes publicly known through no fault of recipient; or which is rightfully received by recipient from a third party without restriction.

This document includes information about current HP products, sales, and service programs that may be enhanced or discontinued at HP's sole discretion. HP has endeavored to include in this document the materials that are believed to be reliable and relevant for the purpose of recipient's evaluation. Neither HP nor its representatives make any warranties as to the accuracy or completeness of the information. Accordingly, this document is provided for information purposes only in the hope that HP may be considered to receive your business. Neither HP nor its representatives shall have any liability to recipient or any of its representatives as a result of the use of the information provided. Only a mutually agreed-upon written definitive agreement, signed by the authorized representatives of the parties, shall be binding on HP or its affiliates.

The term “solution” in the context of this proposal is defined as the products and services proposed herein. Since additional information may be required from you in order to develop the appropriate configuration for your project, the term “solution” does not imply that those products or services as proposed are guaranteed to, or will, meet your requirements.

The use of the terms “partner” or “partnership” in this proposal does not imply a formal, legal, or contractual partnership, but rather a mutually beneficial relationship arising from the teamwork between the parties.

If there are any concerns, questions, or issues regarding this notice, please contact your sales representative.

HP ArcSight Ports and Protocols

This document describes the most commonly used ports and protocols used by HP ArcSight ESM, Express, Logger, ArcSight Management Center, Connector Appliance, SmartConnectors, Model Import Connectors, and Network Synergy Platform.

HP ArcSight ESM & Express (v6.X/v4.X)

Source Device	Destination Device	Destination Port	Notes
Workstation	ESM/Express Manager	TCP 8443	Console to ESM/Express Manager communication.
Workstation	Express/ESM Manager	TCP 22	SSH access for troubleshooting and diagnostics.
Workstation	DNS Server(s)	UDP/TCP 53	Console to DNS server communication (nslookup tool). Host resolution of ESM/Express Manager during Console login.
Workstation	Whois Server(s)	UDP/TCP 43	Console to Whois server communication (whois tool).
Workstation	Selected Destination/Target in Console	ICMP	Console to target communication (ping tool).
Workstation	HP ArcSight Web	TCP 9443	Web browser to HP ArcSight Web communication.
ESM/Express Manager	NTP Server(s)	UDP 123	ESM/Express Manager to NTP server (for time synchronization).
ESM/Express Manager	DNS Server(s)	UDP/TCP 53	ESM/Express Manager to DNS server communication (nslookup tool).
ESM/Express Manager	SMTP Server(s)	TCP 25	ESM/Express Manager to SMTP server (for notifications).
ESM/Express Manager	POP3 Server(s)	TCP 110	ESM/Express Manager to POP3 server (for notifications, if applicable).
ESM/Express Manager	IMAP Server(s)	TCP 143	ESM/Express Manager to IMAP server (for notifications, if applicable).
ESM/Express Manager	SNPP Server(s)	TCP 444	ESM/Express Manager to SNPP server (for notifications, if applicable).
ESM/Express Manager	LDAP Server(s)	TCP 389 or 636	ESM/Express Manager to LDAP server (if applicable). TCP 389 without SSL; TCP 636 with SSL.
ESM/Express Manager	RADIUS Server(s)	UDP 1645 or 1812	ESM/Express Manager to RADIUS server (if applicable).

Source Device	Destination Device	Destination Port	Notes
Connector Appliance SmartConnectors, Logger SmartConnectors, and SmartConnectors	ESM/Express Manager	TCP 8443	SmartConnector to ESM/Express Manager secure and encrypted event channel.
ESM/Express Manager	Logger	TCP 443	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination (Forwarding Connector).
ESM/Express Manager	ESM/Express Manager	TCP 8443	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination (Forwarding Connector).
ESM/Express Manager	Syslog Server(s)	UDP/TCP 514	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination (Forwarding Connector).
ESM/Express Manager	McAfee ePolicy Orchestrator	TCP 1433	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination (Forwarding Connector).
Web Service Client	ESM/Express Manager	TCP 9090	The ESM/Express Service Layer is available and exposes functionalities as Web Services. By consuming the exposed Web Services, you can integrate ESM/Express functionality in your own applications.
	Express Manager	TCP 9001	Remote Connector Management listening port.
	Express Manager	TCP 9002	Remote Connector Management listening port.
	Express Manager	TCP 6443	Connector Management.
	ESM 6.5c Manager	TCP 8443, 9443, 9000	These TCP ports are used for external incoming connections.

Source Device	Destination Device	Destination Port	Notes
	ESM 6.5c Manager	TCP 1976, 2812, 3306, 5555, 6005, 6009, 6443, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8808, 8880, 8888, 8889, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9123, 9124, 9999, 45450	These TCP ports are used internally for inter-component communication by ESM 6.5c.
	ESM 6.5c Manager	TCP 6060, 9005, 9009, 1099	Risk Insight
	ESM 6.5c Manager	TCP 8081, 6005, 8444, 6410, 6400	Risk Insight (BusinessObjects)

HP ArcSight Logger (v5.X)

Source Device	Destination Device	Destination Port	Notes
Workstation	Logger	TCP 443	Web browser to Logger communication.
Workstation	Logger	TCP 22	SSH access for troubleshooting and diagnostics.
Logger	NTP Server(s)	UDP 123	Logger to NTP server (for time synchronization).
Logger	DNS Server(s)	UDP/TCP 53	Logger to DNS server communication.
Logger	SMTP Server(s)	TCP 25	Logger to SMTP server (for notifications).
Logger	Syslog Server(s)	UDP/TCP 514	Logger to syslog server (for notifications).
Logger	SNMP Server(s)	UDP 162	Logger to SNMP server (for notifications).
Logger	RADIUS Server(s)	UDP 1645 or 1812	Logger to RADIUS server (when Logger is configured to use RADIUS password authentication).
Logger	NFS Server(s)	TCP 111 UDP 111 TCP 2049 UDP 2049 TCP 2219 UDP 2219	Allows Logger to connect to servers via NFS for event archiving and search export.
Logger	CIFS Server(s)	TCP 445	Allows Logger to connect to servers via CIFS for event archiving and search export.
Logger	NFS Server(s)	TCP 111 UDP 111 TCP 2049 UDP 2049 TCP 2219 UDP 2219	Allows Logger File Receivers to read log files from NFS servers. Allows Logger SmartConnectors (L3500) to read logs from NFS servers.
Logger	CIFS Server(s)	TCP 445	Allows Logger File Receivers to read log files from CIFS servers. Allows Logger SmartConnectors (L3500) to read logs from CIFS servers.
Logger	SCP, SFTP, FTP Server(s)	TCP 22 (SCP, SFTP) TCP 20 & 21 (FTP)	Allows Logger File Transfer Receiver to read remote log files using SCP, SFTP or FTP protocols.
Syslog Event Sources	Logger	UDP 514 & 8514	Used by Logger syslog Receivers over UDP.
Syslog Event Sources	Logger	TCP 515 & 8515	Used by Logger syslog Receivers over TCP.

Source Device	Destination Device	Destination Port	Notes
Connector Appliance SmartConnectors, Logger SmartConnectors, and SmartConnectors	Logger	TCP 443	SmartConnector to Logger secure and encrypted event channel (SmartMessage Receiver).
Logger	ESM/Express Manager	TCP 8443	Used to forward audit events from Logger to the ESM/Express Manager.
Logger	ESM/Express Manager and/or Syslog Server(s)	TCP 8443 (ESM/Express Manager), UDP/TCP 514	Used to send all events, or events which match a particular filter, on to a particular host.
Logger	SCP Server	TCP 22 (SCP)	Allows backup of Logger configuration to remote host.

HP ArcSight Management Center (v2.X)

Source Device	Destination Device	Destination Port	Notes
Workstation	ArcMC	TCP 443 (when installed as root) TCP 9000 when installed as non-root user)	Web browser to ArcMC communication.
Workstation	ArcMC	TCP 22	SSH access for troubleshooting and diagnostics.
ArcMC	ArcMC/Logger/Connector Appliance	TCP 443 (when installed as root) TCP 9000 (when installed as non-root user)	Managing ArcMC/Logger/Connector Appliance
ArcMC	NTP Server(s)	UDP 123	ArcMC to NTP server (for time synchronization).
ArcMC	DNS Server(s)	UDP/TCP 53	ArcMC to DNS server communication (for IP/hostname resolution)
ArcMC	SMTP Server(s)	TCP 25	ArcMC to SMTP server (for notifications).
ArcMC	RADIUS Server(s)	UDP 1645 or 1812	ArcMC to RADIUS server (for external authentication).
ArcMC	LDAP Server(s)	TCP 389 or 636	ArcMC to LDAP server (for external authentication). TCP 389 without SSL; TCP 636 with SSL.
ArcMC	SCP Server	TCP 22	Allows backup of ArcMC configuration to a remote host.
ArcMC	ArcMC local syslog SmartConnector	UDP/TCP 514	Used for audit forwarding from ArcMC to the ArcMC local syslog SmartConnector.
ArcMC SmartConnectors	ESM/Express Manager	TCP 8443	ArcMC SmartConnectors to ESM/Express Manager secure and encrypted event channel.
ArcMC SmartConnectors	Logger	TCP 443	ArcMC SmartConnectors to Logger SmartMessage secure and encrypted event channel.
ArcMC local syslog SmartConnector	ESM/Express Manager	TCP 8443	Used for audit forwarding from the ArcMC local syslog SmartConnector to ESM/Express Manager secure and encrypted event channel.
ArcMC local syslog SmartConnector	Logger	TCP 443	Used for audit forwarding from ArcMC local syslog SmartConnector to Logger SmartMessage secure and encrypted event channel.

Source Device	Destination Device	Destination Port	Notes
ArcMC	SmartConnectors	TCP 9001-9020	Allows ArcMC to manage remote SmartConnectors (appliance and/or software).
ArcMC	NFS Server(s)	UDP/TCP 111 TCP 2049 UDP 2049 TCP 2219 UDP 2219	Allows SmartConnectors to read logs from NFS servers.
ArcMC	CIFS Server(s)	TCP 445	Allows SmartConnectors to read logs from CIFS servers.

HP ArcSight Connector Appliance (v6.X)

Source Device	Destination Device	Destination Port	Notes
Workstation	Connector Appliance	TCP 443	Web browser to Connector Appliance communication.
Workstation	Connector Appliance	TCP 22	SSH access for troubleshooting and diagnostics.
Connector Appliance	NTP Server(s)	UDP 123	Connector Appliance to NTP server (for time synchronization).
Connector Appliance	DNS Server(s)	UDP/TCP 53	Connector Appliance to DNS server communication.
Connector Appliance	SMTP Server(s)	TCP 25	Connector Appliance to SMTP server (for notifications).
Connector Appliance	RADIUS Server(s)	UDP 1645 or 1812	Connector Appliance to RADIUS server (when Connector Appliance is configured to use RADIUS password authentication).
Connector Appliance SmartConnectors or SmartConnectors	ESM/Express Manager	TCP 8443	SmartConnector to ESM/Express Manager secure and encrypted event channel.
Connector Appliance SmartConnectors or SmartConnectors	Logger	TCP 443	SmartConnector to Logger SmartMessage secure and encrypted event channel.
Connector Appliance	NFS Server(s)	TCP 111 UDP 111 TCP 2049 UDP 2049 TCP 2219 UDP 2219	Allows SmartConnectors to read logs from NFS servers.
Connector Appliance	CIFS Server(s)	TCP 445	Allows SmartConnectors to read logs from CIFS servers.
Connector Appliance	Connector Appliance SmartConnectors and SmartConnectors	TCP 9001 (SmartConnector) TCP 9001-9004 (C3500) TCP 9001-9008 (C5500)	Allows Connector Appliance to manage remote SmartConnectors (appliance and/or software).
Connector Appliance	Syslog Server(s)	UDP/TCP 514	Used to forward audit events from Connector Appliance to syslog server(s).
Connector Appliance	SCP Server	TCP 22 (SCP)	Allows backup of Connector Appliance configuration to remote host.

HP ArcSight SmartConnectors

Source Device	Destination Device	Destination Port	Notes
SmartConnector	DNS Server(s)	UDP/TCP 53	SmartConnector to DNS server communication.
Connector Appliance SmartConnectors or SmartConnectors	ESM/Express Manager	TCP 8443	SmartConnector to ESM/Express Manager secure and encrypted event channel.
Connector Appliance SmartConnectors or SmartConnectors	Logger	TCP 443	SmartConnector to Logger SmartMessage secure and encrypted event channel.
Connector Appliance	SmartConnectors	TCP 9001	Allows Connector Appliance to manage remote SmartConnectors (appliance and/or software).
Forwarding Connector	ESM/Express Manager	TCP 8443	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination.
Forwarding Connector	Logger	TCP 443	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination.
Forwarding Connector	Syslog Server(s)	UDP/TCP 514	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination.
Forwarding Connector	McAfee ePolicy Orchestrator	TCP 1433	Allows you to receive events from a source ESM/Express Manager installation and send them to a secondary destination.
Syslog Event Sources	SmartConnector	UDP/TCP 514	All products that send events via syslog.
SNMP Event Sources	SmartConnector	UDP 162	All products that send events via SNMP.
Windows Unified (WUC)	Windows Servers and Workstations	TCP 445	This SmartConnector can connect to local or remote machines, inside a single domain or from multiple domains, to retrieve events from all types of event logs.
Windows Domain (Legacy)	Windows Servers	TCP 135, 139, 445 UDP 137,138	The Windows Domain SmartConnector will use RPC and Remote Registry to connect to the server and poll the Windows Event Log. This SmartConnector requires domain privileges and domain membership.

Source Device	Destination Device	Destination Port	Notes
Check Point	Check Point Provider-1 (configure for each CMA)	TCP 18184	The Check Point SmartConnector will connect to Provider-1 using Log Export API (LEA) using SSLCA and OPSEC will need to be configured per CMA.
Check Point	Check Point Provider-1 or Smart Center	TCP 18210	Allows SmartConnector to pull OPSEC SSL certificate.
Oracle	Oracle Server	TCP 1521	The SmartConnector establishes connectivity to the database.
Microsoft SQL Server	Microsoft SQL Server	TCP 1433 TCP 139, 445 UDP 135, 139, 445	The SmartConnector establishes connectivity to the database and reads audit trace logs simultaneously. Trace files are not a requirement with some products reporting to Microsoft SQL Server.
MySQL	MySQL Server	TCP 3306	The SmartConnector establishes connectivity to the database.
Blue Coat	Server hosting Blue Coat SmartConnector and FTP server	TCP 20 TCP 21	Allows Blue Coat to send logs to server hosting Blue Coat SmartConnector over FTP and FTP-Data.
Sourcefire	Sourcefire Defense Center Server	TCP 8302	SSL connection for the Defense Center eStreamer protocol.
The third-party SmartConnector types listed above are some of the most common SmartConnectors deployed. For any third-party SmartConnector not listed, please refer to the “SmartConnector Configuration Guide” for information on the ports and protocols used.			

HP ArcSight Model Import Connectors

Source Device	Destination Device	Destination Port	Notes
Model Import Connector for Reputation Security Monitor	tmc.tippingpoint.com d.tippingpoint.com	TCP 443	A component of Reputation Security Monitor which retrieves reputation data from the threat intelligence service (powered by HP DVLabs), processes this data, and forwards it to ESM/Express.
Model Import Connector for IdentityView	Active Directory	TCP 389 or 636	The Model Import Connector for Microsoft Active Directory extracts the user identity information (or Actor data) from the Active Directory LDAP, and then uses that data to populate HP ArcSight ESM/Express Manager with resources.
Model Import Connector	ESM/Express Manager	TCP 8443	Model Import Connector to ESM/Express Manager secure and encrypted channel.

HP ArcSight Network Synergy Platform (v5.X)

Source Device	Destination Device	Destination Port	Notes
Workstation	NSP	TCP 443	Web browser to NSP communication.
NSP	Managed devices	TCP 20 & 21 (FTP)	Configuration file transfer.
NSP	Managed devices	TCP 22 (SSH, SCP, SFTP)	Securely copy or transfer files.
NSP	Managed devices	TCP 23 (telnet)	Managed device access through the appliance only as needed.
NSP	Managed devices	UDP 69 (TFTP)	Configuration file transfer.
NSP	Managed devices	ICMP	Device discovery.
NSP	Managed devices	Multiple ports	Device discovery, if OS fingerprinting is selected.
Managed devices	NSP	TCP 20 & 21 (FTP)	Configuration file transfer.
Managed devices	NSP	TCP 22 (SSH, SCP)	Securely copy or transfer files (SSH proxy; SCP on demand only).
Managed devices	NSP	UDP 69 (TFTP)	Configuration file transfer (TFTP on demand only).
NSP	SMTP Server(s)	TCP 25 (SMTP)	E-mail notifications (if enabled on your appliance).
NSP	SNMP Server(s)	UDP 161 & 162 (SNMP)	SNMP notifications (if your appliance is configured to send them).
NSP	Syslog Server(s)	UDP 514 (syslog)	Syslog messages (if your appliance is configured to send them).
NSP	WINS Server(s)	UDP/TCP 1512	NSP to WINS server communication to resolve Windows NETBIOS names.
NSP	NTP Server(s)	UDP 123	NSP to NTP server (for time synchronization).
NSP	DNS Server(s)	UDP/TCP 53	NSP to DNS server communication.
NSP	ESM/Express Manager	TCP 8443	TRM Connector configured to integrate NSP with ESM/Express and take TRM actions on managed devices through the NSP appliance.
NSP	Syslog SmartConnector (running on Connector Appliance or as a SmartConnector)	UDP 514 (syslog)	The NSP appliance forwards the notification messages it generates to an HP ArcSight Common Event Format (CEF) Syslog SmartConnector that sends the events on to the ESM/Express Manager.

Source Device	Destination Device	Destination Port	Notes
The information that resides on your NSP appliance is well protected. Any port, except 443, is opened only for the length of time it takes to perform the action related to that port. After the action has been performed, the port is closed. The appliance opens no unnecessary ports or third-party software vulnerabilities that might compromise the security of the information.