Micro Focus Security ArcSight Connectors

SmartConnector for SNMP Unified

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for SNMP Unified

June, 2018

Warranty

Restricted Rights Legend

Trademark Notices

Revision History

Date	Description
10/20/2017	Added support for version 8.2 of both RSA Authentication Manager and RSA Identity Management Service. Removed mappings for RSA Authentication Mappings for older, unsupported versions.
10/17/2017	Added encryption parameters to Global Parameters.
05/15/2017	Added configuration parameter for IP address. Removed support for IBM Lotus Domino versions 7.0 and 8.0 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/30/2016	3DES option for Privacy parameter has been removed. Device Vendor has changed to HPE for HPE Network Node Manager i and HPE ProCurve Ethernet Switch products.
06/30/2016	Added more detail to the description of the Version parameter.
02/15/2016	Removed incorrect Device Vendor and Device Product mappings from HPE NNMi mappings table.
06/30/2015	Added support for RSA Authentication Manager and RSA Identity Management Services release 8.1.
11/14/2014	General availability of this connector.
08/15/2014	First edition of this Configuration Guide.

SmartConnector for SNMP Unified

This guide provides information for installing the SmartConnector for SNMP Unified and configuring the device for event collection. This SmartConnector is supported for installation on Windows and Linux platforms.

Product Overview

SNMP SmartConnectors process received SNMP traps. The SNMP Unified SmartConnector can process traps from multiple devices of different types with various OIDs (object identifiers), and can parse traps from these devices. The following devices are supported with the SmartConnector for SNMP Unified:

- Cisco WIPS version 7.4
- Cisco Wireless LAN Controller MIB version 4
- Cisco Wireless Control System version 7.0
- Extreme Networks (formerly Enterasys) Dragon IDS version 5.0
- HPE Network Node Manager i versions 9.1 and 9.2
- HPE ProCurve Ethernet Switch 4000M devices
- IBM Lotus Domino version 8.5
- McAfee Email Gateway version 7.5
- nCircle Scanner versions 6.0, 6.2, 7.0
- RSA Authentication Manager/Identity Management Service versions 8.0, 8.1, and 8.2
- Websense Web Security Suite versions 6.1, 6.3, 7.0, 7.5, 7.7

Creating a FlexConnector with SNMP Unified

You can select SNMP Unified during connector installation to create an SNMP FlexConnector. Follow the installation procedure given in this guide, then refer to the ArcSight FlexConnector Developer's Guide for the following information:

- For **Security Event Data Format Examples**, "SNMP FlexConnector"
- For **Event Mapping** information, "Tokens Available for SNMP Parsers Only"
- For **Configuration File Examples**, "Configuration Properties for an SNMP FlexConnector"

Note that you must create a folder in which to copy your parser. Under `ARCSIGHT_HOME/current/user/agent`, create a `flexagent/snmp/` subfolder containing subfolders for the various trap OIDs; for example:

`ARCSIGHT_HOME/current/user/agent/flexagent/snmp/<trap OID>`

Configuration

For instructions about forwarding SNMP traps to the ArcSight SmartConnector, see the documentation for your vendor's product.

SNMP Versions

SNMP is a standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates.

The different versions of SNMP are the SNMPv1, SNMPv2c, and SNMPv3. The following is a brief description of each version.

SNMPv1: This is the first version of the protocol, which is defined in RFCs 1155 and 1157. It is easy to set up, requiring only a plaintext community.

SNMPv2c: This is the revised protocol, which includes enhancements of SNMPv1 in the areas of protocol packet types, transport mappings, MIB structure elements but using the existing SNMPv1 administration structure ("community based" and hence SNMPv2c). It is defined in RFC 1901, RFC 1905, RFC 1906, RFC2578. In practical terms, v2c is identical to version 1, except it adds support for 64 bit counters.

SNMPv3: SNMPv3 defines the secure version of the SNMP. SNMPv3 also facilitates remote configuration of the SNMP entities. It is defined by RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415. It adds security to the 64 bit counters with both encryption and authentication, which can be used together or separately. Setup is more complex than just defining a community string.

SNMPv3 security comes primarily in two forms:

- Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the EngineID of the entity. The key is shared with the intended recipient and used to receive the message.
- Privacy is used to encrypt the payload of the SNMP message to ensure that it cannot be read by unauthorized users. Any intercepted traps will be filled with garbled characters and will be unreadable.

Using Zebedee Secure IP Tunnel with SNMP

ArcSight SNMP-based SmartConnectors support Zebedee, an open source UDP tunnel program that provides optional compression and encryption. To configure Zebedee, follow these steps:

1. Use Zebedee to create public and private keys on each of the devices. Create client and server `.zbd` configuration files as described in the Zebedee documentation to refer to the keys.

2. Install the SmartConnector. Start Zebedee in listen server mode on the SmartConnector host, with the command:

   ```
   zebedee -U -f server.zbd -s
   ```

   This prepares Zebedee to listen for connectionless UDP traffic.

3. The client machine is the host that is to send events to the SmartConnector. Run Zebedee on the client with the command:

   ```
   zebedee -U -f client.zbd 162:agent_hostname:162
   ```

   This prepares Zebedee to send UDP traffic to the SmartConnector host, `agent_hostname`.

Unless the device address is included in the SNMP trap, events do not record the host that actually sent the SNMP trap. Using Zebedee makes all SNMP traffic to the SmartConnector appear to come from `localhost`.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

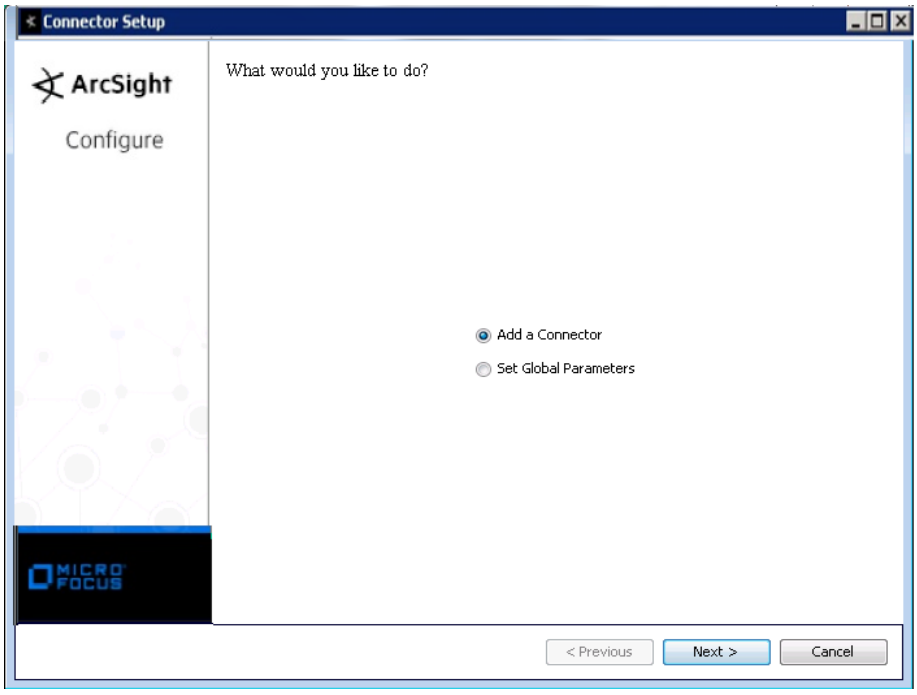
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

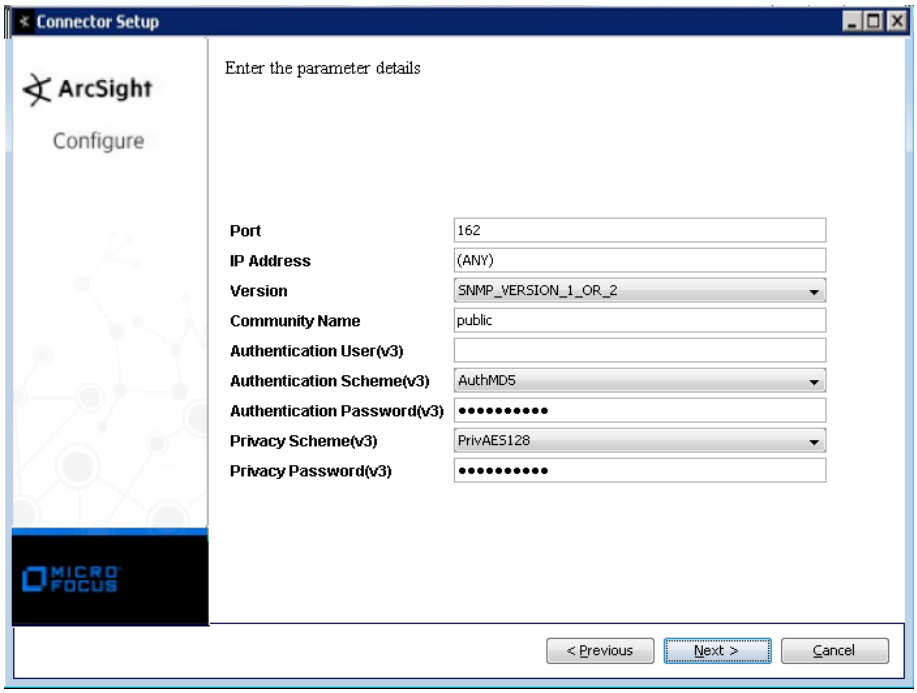
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2 Select **SNMP Unified** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Port	Enter the port number to which SNMP traps are sent. The default is 162.
IP Address	Specify a local IP address from which the connector will listen for incoming SNMP trap messages (accept the default (ANY) to bind to a local default IP address assigned by the OS).
Version	The SNMP version being used. Select SNMP_VERSION_1_OR_2 or SNMP_VERSION_3. SNMP_VERSION_1_OR_2 is the default. When you select SNMP_VERSION_1_OR_2, you need not enter values for the Authentication User, Authentication Scheme, Authentication Password, Privacy Scheme, or Privacy Password parameters as these are valid only for SNMP v3. If your SNMP Unified SmartConnector is receiving SNMP trap version 1 or 2, then you need only one SNMP Unified SmartConnector to listen to traps on port 162 from multiple device vendors like RSA, Cisco, and so on. If your SNMP Unified SmartConnector listens for SNMP version 3 traps, then you must use the same Authentication User(v3), Authentication Scheme(v3), Authentication Password(v3), Privacy Scheme(v3), and Privacy Password(v3) on all end source devices that forward SNMP version 3 to one SNMP Unified SmartConnector. If you do not want to use the same connector listening for v3 traps, install another SNMP Unified connector and choose a different SNMP listener port (if installed on the same host with the other SNMP Unified connector). Configure different Authentication User(v3), Authentication Scheme(v3), Authentication Password(v3), Privacy Scheme(v3), and Privacy Password(v3) for that other connector.

Parameter	Description
Community Name	Enter the community name to which SNMP trap messages are sent. The default is public.
Authentication User(v3)	Enter the name that identifies the SNMP v3 user.
Authentication Scheme(v3)	The type of authentication being used. Select AuthMD5 or AuthSHA. AuthMD5 is the default.
Authentication Password(v3)	Enter the authentication password.
Privacy Scheme(v3)	The type of privacy being used. Select PrivAES128, PrivAES192, PrivAES256, or PrivDES.
Privacy Password(v3)	Enter the privacy password.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Cisco WIPS Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Critical; High = Major; Medium = Warning, minor; Low = Cleared, info
Base Event Count	eventCount
Device Custom Date 1	alarmCreationTime
Device Custom Date 2	Created
Device Custom String 1	AP Interface Name
Device Custom String 2	Wireless Controller IP
Device Custom String 3	authEntityId
Device Custom String 4	applicationSpecificAlarmID
Device Custom String 5	generatedBy
Device Custom String 6	displayName

ArcSight ESM Field	Device-Specific Field
Device Event Category	cWNotificationCategory (1=unknown, 2=accessPoints, 3=adhocRogue, 4=clients, 5=controllers, 9=meshLinks, 10=mobilityService, 11=performance, 12=rogueAP, 13=rrm, 14=security, 15=wcs, 16=switch, 17=ncs)
Device Event Class Id	Both (eventType, cWNotificationSeverity)
Device Product	'WIPS'
Device Receipt Time	Time Stamp
Device Severity	cWNotificationSeverity "1=cleared","2=indeterminate","3=critical","4=major","5=minor","6=warning","7=info"
Device Vendor	'CISCO'
External ID	instanceId
Message	cWNotificationDescription
Name	cWNotificationSubCategory or applicationCategoryData (if cWNotificationSubCategory doesn't exist, extract from cWNotificationSpecialAttributes)
Source User Name	Network User

Cisco Wireless LAN Controller Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = malicious; High = unclassified; Medium = pending; Low = friendly
Destination MAC Address	One of(bsnStationAPMacAddr, bsnAPDot3MacAddressTrapType70, bsnStationAPMacAddrGeneral, bsnRogueAPAirespaceAPMacAddress)
Device Custom String 1	The rogue on wired network
Device Custom String 2	The rogue on Adhoc mode
Device Custom String 3	AP Name
Device Custom String 5	Station AP If Slot Id
Device Custom String 6	Signature Type
Device Event Class Id	One of(_SNMP_TRAP_TYPE, bsnSignatureName when SNMP_TRAP_TYPE is 70)
Device Inbound Interface	One of ((bsnRogueAPRadioType, bsnAPIfType, bsnAPIfTypeGeneral) ("1=dot11b", "2=dot11a", "3=unknown","4=uwb", "5=dot11g", "6=dot11n24", "7=dot11n5")
Device Product	'Airespace'
Device Severity	bsnRogueAPClassType("0=pending", "1=friendly", "2=malicious", "3=unclassified")
Device Vendor	'CISCO'
Flex String 1	_SNMP_TRAP_TYPE
Name	bsnSignatureDescription when SNMP_TRAP_TYPE is 70
Reason	One of (bsnStationReasonCode, bsnStationReasonCodeGeneral, bsnApFunctionalityDisableReasonCode, bsnAPIfUpDownCause)
Source Address	One of(bsnUserIpAddress,bsnUserIpAddressGeneral)
Source MAC Address	One of(bsnStationMacAddress, bsnAPDot3MacAddressTrapType13, bsnAPDot3MacAddressTrapType13, bsnSignatureAttackerMacAddress, bsnAPDot3MacAddressTrapType39, bsnStationMacAddressGeneral, bsnAPMacAddrTrapVariable, bsnRogueAPDot11MacAddress, bsnRogueAPDot11MacAddressGeneral)
Source Port	One of (bsnAPPortNumber, bsnAPPortNumberTrapVariable)
Source User Name	One of (bsnStationUserName, bsnStationUserNameGeneral)

Cisco WCS Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional Data	alertType
Additional Data	classificationType
Additional Data	cWNotificationTimestamp
Additional Data	cWNotificationUpdatedTimestamp
Additional Data	detectingAPRadioType
Additional Data	numOfDetectingAps
Additional Data	on80211A
Additional Data	on80211B
Additional Data	onNetwork
Additional Data	radioType
Additional Data	rogueApType
Additional Data	RSSI
Additional Data	SNR
Additional Data	sptStatus
Additional Data	state
Additional Data	totalRogueClients
Additional Data	Xcoordinate
Additional Data	Ycoordinate
Agent (Connector) Severity	High=critical,major; Medium=warning; Low=minor,clear,info,unknown
Application Protocol	802.11b/g
Destination Address	cWNotificationManagedObjectAddress, Controller
Destination Host Name	Controller Name
Destination Mac Address	Rogue AP, Adhoc Rogue, rogueApMacAddr
Destination Nt Domain	cWNotificationVirtualDomains
Device Custom Number1	channelNumber
Device Custom String 2	ssId
Device Custom String 3	cWNotificationManagedObjectAddressType ("0=unknown","1=IPv4","2=IPv6","3=IPv4z","4=IPv6z","16=DNS")
Device Custom String 5	cWNotificationSourceDisplayName
Device Custom String 6	"Access Points"
Device Event Category	cWNotificationCategory (1=unknown, 2=accessPoints, 3=adhocRogue, 4=clients, 5=controllers, 6=coverageHole, "7=interference, 8=contextAwareNotifications, 9=meshLinks, 10=mobilityService, 11=performance, 12=rogueAP, 13=rrm, 14=security, 15=wcs)
Device Event Class Id	cWNotificationKey
Device Product	Wireless Control System
Device Severity	cWNotificationSeverity (1=critical,2=major,3=minor,4=warning,5=clear,6=info,7=unknown)
Device Vendor	'CISCO'

ArcSight ESM Field	Device-Specific Field
Message	cWNotificationDescription
Name	cWNotificationSubCategory

Extreme Networks Dragon Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional Data	DragonAlertName
Additional Data	DragonDirection
Additional Data	DragonSensor
Agent (Connector) Severity	Low (<25), Medium (<50), High (<100), Very-High (>=100)
Device Host Name	If the relevant field in the logs appear as <name>-nids or <name>-hids, then <name> is used. Otherwise, the entire field is used. The former is the default behavior unless Dragon is configured to use a custom name in that field.
Device Severity	Dragon Severity
Event Name	Dragon Event Name
Protocol	Protocol (not populated for Dragon Squire events)
Source Address	Dragon Source Address (not populated for Dragon Squire events)
Source Port	Dragon Source Port (not populated for Dragon Squire events)
Target Address	Dragon Target IP (not populated for Dragon Squire events)
Target Port	Dragon Target Port (not populated for Dragon Squire events)

HPE Network Node Manager i Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High=critical,major; Medium=warning; Low=minor,clear,info,unknown
Application Protocol	802.11b/g
Destination Address	nnmiIncidentOtherNodeMgmtAddr
Destination Address	cWNotificationManagedObjectAddress, Controller
Destination Host Name	nnmiIncidentOtherNodeHostname
Destination Host Name	Controller Name
Destination Mac Address	Rogue AP, Adhoc Rogue, rogueApMacAddr
Destination Nt Domain	cWNotificationVirtualDomains
Device Address	nnmiIncidentSourceNodeMgmtAddr
Device Custom Date 1	nnmiIncidentDbCreateTime
Device Custom Date 2	nnmiIncidentDbModifiedTime
Device Custom Number 1	nnmiIncidentDupCount
Device Custom String 1	One of (nnmiIncidentLifecycleState, nnmiIncidentLifecycleStateCurrentValue) (1 = registered, 2 = inprogress, 3 = completed, 4 = closed, 5 = dampened)

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	nnmiIncidentNature
Device Custom String 2	ssId
Device Custom String 3	nnmiIncidentPriority
Device Custom String 3	cWNotificationManagedObjectAddressType ("0=unknown","1=IPv4","2=IPv6","3=IPv4z","4=IPv6z","16=DNS")
Device Custom String 4	nnmiIncidentClosedReason
Device Custom String 5	nnmiIncidentLifecycleStatePreviousValue (1 = registered, 2 = inprogress, 3 = completed, 4 = closed, 5 = dampened)
Device Custom String 5	cWNotificationSourceDisplayName
Device Custom String 6	"Access Points"
Device Event Category	nnmiIncidentCategory
Device Event Category	cWNotificationCategory (1=unknown, 2=accessPoints, 3=adhocRogue, 4=clients, 5=controllers, 6=coverageHole, "7=interference, 8=contextAwareNotifications, 9=meshLinks, 10=mobilityService, 11=performance, 12=rogueAP, 13=rrm, 14=security, 15=wcs)
Device Event Class Id	cWNotificationKey
Device Event Class ID	_SNMP_TRAP_TYPE
Device Facility	nnmiIncidentFamily
Device Host Name	'nnmiIncidentSourceNodeHostname'
Device Process Name	nnmiApplicationId
Device Product	'NNMi'
Device Receipt Time	nnmiIncidentOriginTime
Device Severity	nnmiIncidentSeverity
Device Severity	cWNotificationSeverity "1=critical","2=major","3=minor","4=warning","5=clear","6=info","7=unknown"
Device Vendor	'HPE'
External ID	nnmiIncidentUuid
Message	nnmiIncidentFmtMessage
Message	cWNotificationDescription
Name	nnmiIncidentName
Name	cWNotificationSubCategory
Request URL	nnmiNmsUrl
Source Service Name	nnmiIncidentOrigin

HPE ProCurve Ethernet Switch SNMP Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = Critical; Medium = debug Warning; Low = Information
Application Protocol	Application Protocol

ArcSight ESM Field	Device-Specific Field
Device Custom Number1	Updated Time in seconds
Device Custom String1	Switch Port Number
Device Event Class Id	System Module
Device Receipt Time	Date and Time
Device Severity	Severity
Event Name	Event Message
Raw Event	Line that is logged in HPE Procurve Switch
Source Address	Source IP Address

IBM Lotus Domino SNMP Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 0, 1, or 2; Medium = 3 or 4; Low = 5
Application Protocol	Application Protocol
Destination Address	Destination Address
Destination Dns Domain	Destiantion Dns Domain
Destination Host Name	Destination Host Name
Destination User Name	Destination User Name
Device Custom Number 1	Message size
Device Custom Number 2	Message Count
Device Custom Number 3	Disk Short
Device Custom String 1	Reason
Device Custom String 2	Message IDs
Device Custom String 3	Destination Email Domain
Device Custom String 4	Source Email Domain
Device Custom String 5	File Size
Device Custom String 6	Hop Count
Device Event Class Id	lnEvtType
Device External Id	lnEvtSeq
Device Product	'Domino'
Device Receipt Time	lnEvtWhen
Device Severity	lnEvtSeverity
Device Vendor	'IBM'
External Id	lnEvtSeq
File Name	File Name
File Size	File Size
Message	lnEvtData
Name	lnEvtData
Source Address	Source Address
Source Host Name	Source Host Name
Source User Name	Source User Name
Transport Protocol	Transport Protocol

McAfee Email Gateway Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	megEventHost
Destination Host Name	megEventHost
Device Custom Date 1	GMT Timestamp
Device Custom String 2	Meg Event Additional Message
Device Event Class Id	megEventID
Device Product	'Email Gateway'
Device Receipt Time	megEventLocalDateTime
Device Vendor	'McAfee'
Reason	megEventReason

nCircle Scanner SNMP Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
EventCategory	'nspMdAttackType' or 'nspMdVulnerabilityType', depending on the trap type
EventName	One of the following, depending on the trap type: 'DB Fault [<nspDBFaultDescription>]', 'Rogue Host Detected [<nspMdIPAddress>]', 'Score Exceeded [<nspMdScore>]', 'Ua User Lockout [<nspUaLockedOutUserName>]', 'Vulnerablity Detected [<nspMdVulnerabilityName>]', <nspMdAttackName>, 'AS Appliance Not responding', 'Con NTP Failure'
Filename	nspDbFaultLogLocation
TargetAddress	nspAsApplianceIPAddress
TargetHostName	nspMdName
TargetUserId	nspUaLockedOutUserName

RSA Authentication Manager/Identity Management General Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	client
Device Action	action
Device Event Class ID	action id
Device Payload ID	ID
Device Receipt Time	time
Event Outcome	result
File Hash	One of (Security Domain id, security domain ID)
File ID	ID
File Name	One of (name, Name)
File Path	One of (Identity source ID, identity source ID)
File Permission	arguments
File Type	One of (type, Domain Object Type)
Message	reason
Name	action
Old File Hash	Security Domain Id
Old File ID	ID

ArcSight ESM Field	Device-Specific Field
Old File Name	Name
Old File Path	Identity Source Id
Old File Type	Domain Object Type

RSA Authentication Manager/Identity Management Trap Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	ERROR, SYSTEM = Medium; INFO = Low
Device Product	'Identity Management Service'
Device Severity	Severity
Device Vendor	'RSA'
Message	Message
Name	Name

RSA Authentication Manager/Identity Management Policy Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	policy ID
Device Custom String 5	method name
Device Custom String 6	policy expression

RSA Authentication Manager/Identity Management User Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	ID
Destination User Name	login name
Device Custom String 1	session ID
Device Custom String 2	first name, last name (User Full Name)
Device Custom String 3	security domain ID

Websense SNMP Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Low when Device Severity = Information; Medium when Device Severity = Warning; High when Device Severity = Error
Application Protocol	valueofCategoryOrProtocol
Destination Address	destIP
Destination Port	destPort
Device Action	valueOfDispsotionOrAction
Device Custom Number 1	threshold
Device Custom String 1	One of (alertCount, alertCount1)
Device Event Category	valueOfCategoryOrProtocol

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	snmpTrapType plus one of (eventName, eventName1)
Device Process Name	source
Device Product	'Websense Enterprise and Policy Server'
Device Receipt Time	optional timestamp
Device Severity	One of ("Warning",type)
Device Vendor	'Websense'
Flex String 1	_SNMP_TRAP_TYPE
Message	concatenate(_SNMP_TRAP_TYPE, __oneOf(message0-message23))
Name	One of (eventName, eventName1)
Request URL	url
Source Address	userIP
Source User Name	user

Websense SNMP Trap Type 1000 Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Low when Device Severity = Information, Low; Medium when Device Severity = Warning, Medium; High when Device Severity = Error, High
Device Custom String 5	filteringService
Device Custom String 6	subscriptionKey
Device Event Class ID	concatenate(snmpTrapType,"I",eventName)
Device Process Name	source
Device Product	'Websense Enterprise and Policy Server'
Device Receipt Time	date
Device Severity	type
Device Vendor	'Websense'
Message	message
Name	eventName

Websense SNMP Trap Type 2002 Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Low when Device Severity = Information, Low; Medium when Device Severity = Warning, Medium; High when Device Severity = Error, High
Destination Address	destinationAddress
Destination Port	destinationPort
Device Action	action
Device Custom Number 1	threshold
Device Custom String 1	alertCount
Device Custom String 2	alert
Device Custom String 3	threatDetails
Device Custom String 4	webSecurityUrl
Device Event Category	category

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	concatenate(snmpTrapType,"|",eventName)
Device Process Name	source
Device Product	'Websense Enterprise and Policy Server'
Device Receipt Time	date
Device Severity	One of("Warning",type)
Device Vendor	'Websense'
Message	message
Name	eventName
Request URL	url
Source Address	sourceAddress
Source Host Name	sourceHostName