Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft DHCP File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Microsoft DHCP File

October 17, 2017

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
08/14/2015	Removed Windows Server 2003 support due to vendor support change. Modified mapping for DHCP IPv6 Event Mappings table.
05/15/2015	Added support for Windows Server 2012 R2.
02/15/2013	Added information about read/write acces to the DHCP folder.
11/15/2012	Added information about CIFS mount for Connector Appliance to Installation section.
05/15/2012	Added new installation procedure.
02/15/2012	Added troubleshooting information regarding Windows 2003 support.
03/30/2011	Added troubleshooting information regarding Windows 2008 support.

Contents

SmartConnector for Microsoft DHCP File

This guide provides information for installing and configuring the SmartConnector for Microsoft DHCP File for log file event collection. This SmartConnector is supported on Windows 2008 and 2012 R2 Server platforms, and should be installed on the Windows machine where the DHCP server resides. IPv4 and IPv6 are supported for Windows 2008 and 2012 R2.

Product Overview

The Dynamic Host Configuration Protocol (DHCP) is an Internet Engineering Task Force (IETF) standard designed to reduce the administration burden and complexity of configuring hosts on a TCP/IP-based network. When you deploy DHCP servers on your network, you can provide client computers and other TCP/IP-based network devices with valid IP addresses automatically. You also can provide the additional configuration parameters these clients and devices need (DHCP options) that let them connect to other network resources, such as DNS servers, WINS servers, and routers.

Configuring DHCP

The user the connector is running as requires read/write access to the DHCP folder to read the DHCP files. If the connector is running as a service, the SYSTEM user requires read/write access to the DHCP folder.

Rotating Log Format

The rotating log format used by the new multiple-instance is different from the previous single-instance connector. The new time-based format is based upon that of the Java 1.6 SimpleDateFormat. For more information, see http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html. Some examples:

Log Format	Rotating Logs
/var/log/'MMddyyyy'.log	/var/log/07082009.log
	/var/log/07092009
	/var/log/07102009
/var/log/'yyyy/MMdd'/access.log	/var/log/2009/0708/access.log
	/var/log/2009/0709/access.log
	/var/log/2009/0710/access.log
/var/log/'yyyy/MMdd'/access-'HHmm'.log	/var/log/2009/0708/access-0900.log
	/var/log/2009/0708/access-1000.log
	/var/log/2009/0708/access-1100.log

The log format can also be specified for index-based rotating logs. Here are some examples:

Log Format	Rotating Logs
/var/log/access.'%02d.01,99'.log	/var/log/access.01.log
	/var/log/access.02.log
	/var/log/access.03.log

Audit Logging

The following can be specified for DHCP servers running Windows Server 2008, and 2012 R2:

- The directory path in which the DHCP server stores audit log files. DHCP audit logs are located by default at `%windir%\System32\Dhcp`.
- A maximum size restriction (in megabytes) for the total amount of disk space available for all audit log files created and stored by the DHCP service.
- An interval for disk checking that is used to determine how many times the DHCP server writes audit log events to the log file before checking for available disk space on the server.
- A minimum size requirement (in megabytes) for server disk space used during disk checking to determine whether sufficient space exists for the server to continue audit logging.

Notes:

- The user the connector is running as requires read/write access to the DHCP folder to read the DHCP files. If the connector is running as a service, the SYSTEM user requires read/write access to the DHCP folder.
- You can selectively enable or disable the audit logging feature at each DHCP server. For more information, see "Enabling Audit Logging."
- Only the directory path in which the DHCP server stores audit log files can be modified using the DHCP console. To do so, first select the applicable DHCP server in the console tree. On the **Action** menu, click **Properties**. Next, click the **Advanced** tab and edit **Audit log file path** as necessary. Other audit logging parameters are adjusted through registry-based configuration changes.

Naming of Audit Log Files

The audit logging behavior discussed in this section applies only to Windows Server 2008, and 2012 R2 DHCP. In Windows NT and Windows 2000, the file name format differed.

The DHCP server bases the name of the audit log file on the current day of the week, as determined by checking the current date and time at the server. For example, when the DHCP server starts, if the current date and time are the following:

```
Monday, April 7, 2003, 04:56:42 P.M.
```

The server audit log file is named:

```
DhcpSrvLog-Mon.Log
```

When a DHCP server starts or a new day begins (when the local time on the computer is 12:00 A.M.), the server writes a header message in the audit log file, indicating that logging has started. Then, depending upon whether the audit log file is a new or existing file, the following actions occur:

- If the file already existed without modification for more than a day, it is overwritten.
- If the file already existed but was modified within the previous 24 hours, the file is not overwritten. Instead, new logging activity is appended to the end of the existing file.

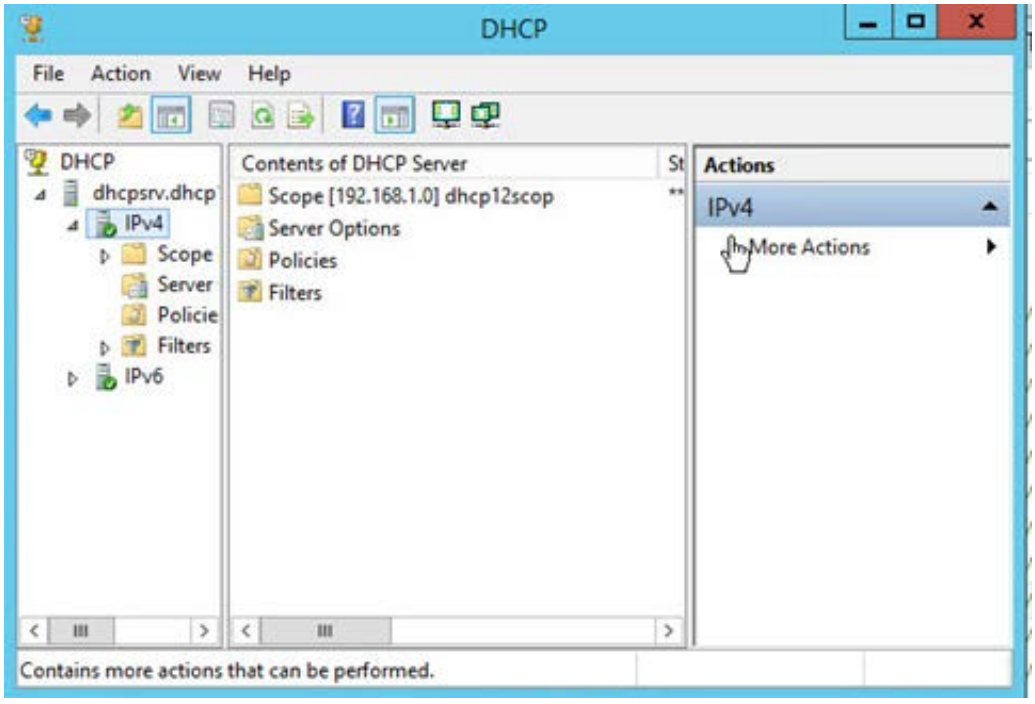
After audit logging starts, the DHCP server performs disk checks at regular intervals, to ensure both the ongoing availability of server disk space and that the current audit log file does not become too large or grow too quickly.

At 12:00 A.M. local time on the server computer, the DHCP server closes the existing log and moves to the log file for the next day of the week. For example, if the day of the week changes at 12:00 A.M. from Wednesday to Thursday, the log file named `DhcpSrvLog-Wed.Log` is closed and the file named `DhcpSrvLog-Thu.Log` is opened and used for logging events.

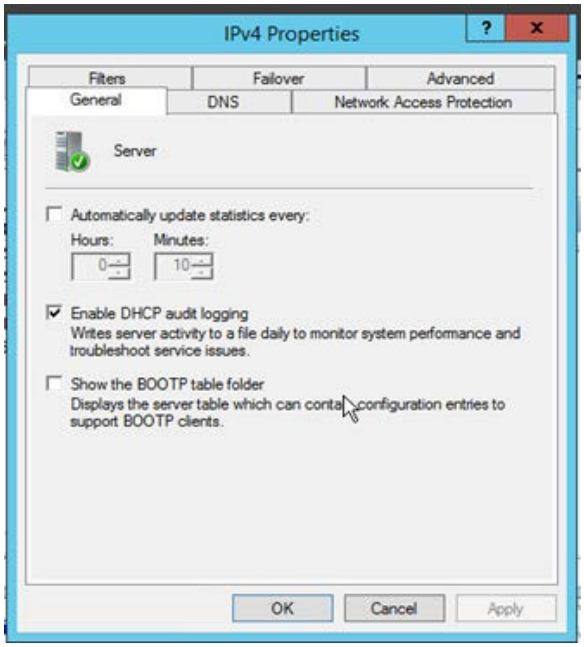
Enable Audit Logging for Windows 2012 R2

To configure DHCP for event collection:

1. Go to **Start > Administrative Tools > DHCP**.
2. Expand the applicable DHCP server tree, and then expand **IPv4** or **IPv6**.



3. Right-click on **IPv4** or **IPv6** and select **Properties**.
4. Check Enable DHCP audit logging on the **General** tab.



5 Click **OK**.

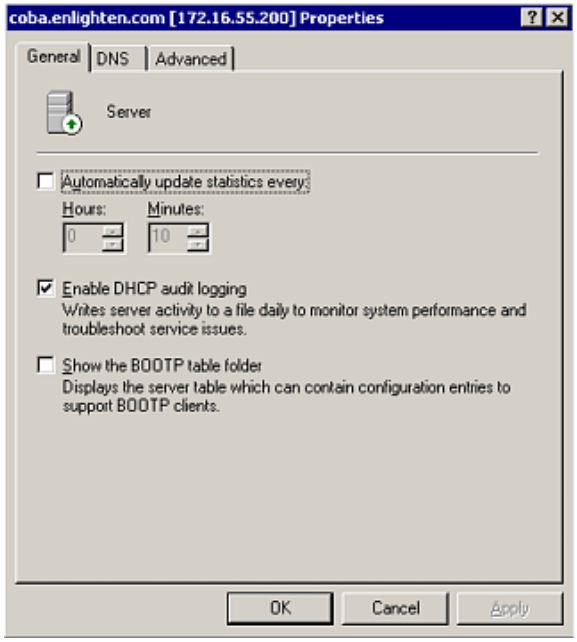
Enable Audit Logging for Windows 2008

To configure DHCP for event collection:

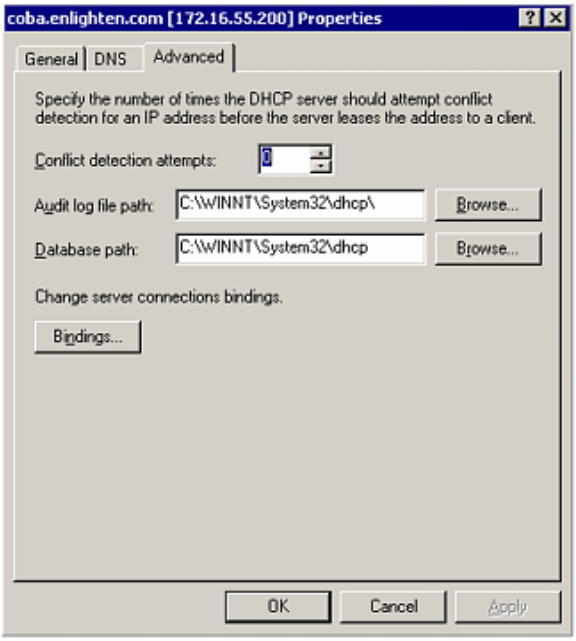
1 Launch DHCP configuration.

2 Right click on the domain name; select **Properties**.

3 From the Properties window, General tab, select **Enable DHCP audit logging**.



4 Click the **Advanced** tab.



5 Change or accept the default audit log path.

You will find a rotating scheme of files following each day of the week; for example:

```
DhcpSrvLog.Mon.Log
DhcpSrvLog.Tue.Log
DhcpSrvLog.Wed.Log
DhcpSrvLog.Thu.Log
DhcpSrvLog.Fri.Log
DhcpSrvLog.Sat.Log
DhcpSrvLog.Sun.Log
```

For IPv6, the file names contain V6; for example: `DhcpV6SrvLog.Mon.Log`

Install the SmartConnector

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

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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 HPE SSO and Protect 724 sites.

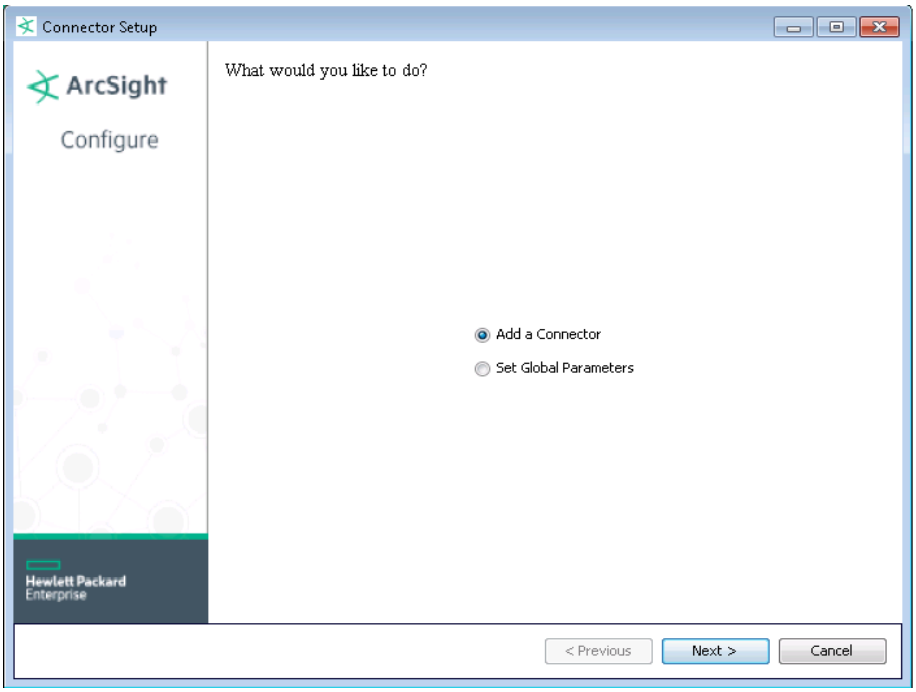
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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 HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

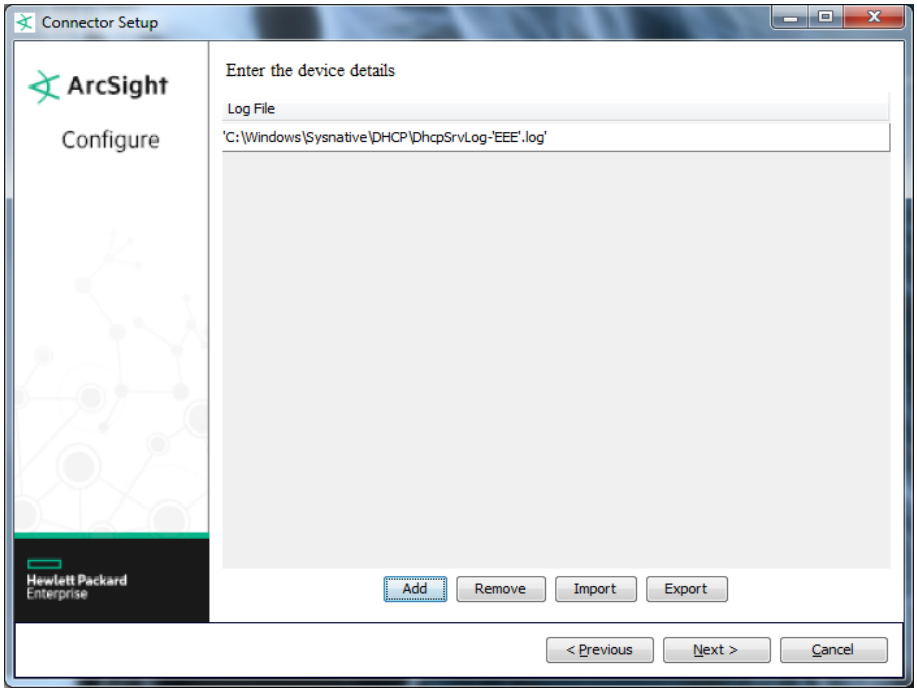
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE 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.

Parameter	Setting
Format Preserving Identity	The HPE 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 HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE 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 **Microsoft DHCP File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description

Parameter	Description
Log File	Enter the parameters for each DHCP server log file to be read by the connector. When you click Add, the default value is 'C:\WINNT\System32\DHCP\DhcpSrvLog-'EEE'.log'. Change the default value to match the DHCP server log file name and the folder in which it is located. For IPv6, you need to add v6 to the log file name; for example, 'C:\WINDOWS\System32\DHCP\DhcpV6SrvLog-'EEE'.log'. V6 is case-insensitive.

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.

Microsoft DHCP IPv4 Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high = 50..99; medium = 14, 18, 31, 33, 34, 35, 36; low = 00, 01, 02, 10, 11, 12, 13, 15, 16, 17, 20, 21, 22, 23, 24, 25, 30, 32
Device Custom Number 1	leases expired
Device Custom Number 2	leases deleted
Device Custom Number 3	QResult (Windows 2008)
Device Custom String 1	Probation Time (Windows 2008)
Device Custom String 2	Correlation ID (Windows 2008)
Device Custom String 3	DHCID (Windows 2008)
Device Custom String 4	MAC Vendor Prefix
Device Custom String 5	Ethernet Vendor
Device Custom String 6	Relay Agent Information
Device Event Class Id	ID
Device Product	'DHCP Server'
Device Receipt Time	Date, Time
Device Severity	ID
Device Vendor	'Microsoft'
Device Version	One of (_DEVICE_VERSION,"Unknown")
External ID	Transaction ID (Windows 2008)
Name	Description
Source Address	IP_Address
Source Host Name	Host_Name
Source Mac Address	MAC_Address
Source User Name	UserName (Windows 2008)

Microsoft DHCP IPv6 Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high = 11023, 11025, 11028, 11029; medium = 11005, 11006, 11007, 11014, 11016; low = 11000, 11001, 11002, 11003, 11004, 11008, 11009, 11010, 11011, 11012, 11013, 11015, 11017, 11018, 11019, 11020, 11021, 11024, 11022, 11030, 11031, 11032
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	leases expired
Device Custom Number 2	leases deleted
Device Custom Number 3	Duid Length
Device Custom String 1	Error Code
Device Custom String 2	Duid Bytes(Hex)
Device Custom String 3	Dhcid
Device Event Class ID	ID
Device Product	'DHCP Server'
Device Receipt Time	Create Time Stamp (Date, Time)
Device Severity	ID
Device Vendor	'Microsoft'
Device Version	One of(_DEVICE_VERSION,"Unknown")
Name	Description
Source Host Name	Host_Name
Source User Name	User_Name

Event IDs for IPv4

ArcSight ESM Field	Device-Specific Field
00	The log was started.
01	The log was stopped.
02	The log was temporarily paused due to low disk space.
10	A new IP address was leased to a client.
11	A lease was renewed by a client.
12	A lease was released by a client.
13	An IP address was found to be in use on the network.
14	A lease request could not be satisfied because the scope's address pool was exhausted.
15	A lease was denied.
16	A lease was deleted.
17	A lease was expired.
18	A lease was expired and DNS records were deleted (Windows 2008).
20	A BOOTP address was leased to a client.
21	A dynamic BOOTP address was leased to a client.
22	A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
23	A BOOTP IP address was deleted after checking to see it was not in use.
24	IP address cleanup operation has begun.

ArcSight ESM Field	Device-Specific Field
25	IP address cleanup statistics.
30	DNS update request to the named DNS server.
31	DNS update failed.
32	DNS update successful.
33	Packet dropped due to NAP policy (Windows 2008).
34	DNS update request failed as the DNS update request queue limit exceeded.(Windows 2012 R2)
35	DNS update request failed. (Windows 2012 R2)
36	Packet dropped because the server is in failover standby role or the hash of the client ID does not match. (Windows 2012 R2)
50	Unreachable domain.
51	Authorization succeeded.
52	Upgraded to a Windows Server 2008 operating system.
53	Cached authorization.
54	Authorization failed. When this event occurs it is likely followed by the server being stopped.
55	Authorization (servicing).
56	Authorization failure. Stopped servicing. You must first authorize the server in the directory before starting it again.
57	Server found in domain. Another DHCP server exists and is authorized for service in the same domain.
58	Server could not find domain.
59	Network failure. A network-related failure prevented the server from determining if it is authorized.
60	No DC is DS Enabled.
61	Another DHCP server was found on the network that belongs to the Active Directory domain.
62	Another DHCP server was found on the network.
63	Restarting rogue detection.
64	No DHCP enabled interfaces.
Event ID	Meaning

Event IDs for IPv6

ArcSight ESM Field	Device-Specific Field
11000	Solicit.
11001	Advertise.
11002	Request.
11003	Confirm.
11004	Renew.
11005	Rebind.
11006	Decline.
11007	Release.
11008	Information Request.
11009	Scope Full.
11010	Started.

ArcSight ESM Field	Device-Specific Field
11011	Stopped.
11012	Audit Log Paused.
11013	DHCP Log File.
11014	Bad address.
11015	Address is already in use.
11016	Client deleted.
11017	DNS record not deleted.
11018	Expired.
11019	Expired and deleted count.
11020	Database cleanup begin.
11021	Database cleanup end.
11022	DNS IPv6 Update Request.
11023	Service not authorized in AD.
11024	Service authorized in AD.
11025	Service has not determined if it authorized in AD.
11028	DNS IPv6 update request failed as the DNS update request queue limit exceeded. (Windows 2012 R2)
11029	DNS IPv6 update request failed. (Windows 2012 R2)
11030	DHCPv6 stateless client records purged. (Windows 2012 R2)
11031	DHCPv6 stateless client record is purged as the purge interval has expired for this client record. (Windows 2012 R2)
11032	DHCPv6 Information Request from IPv6 Stateless Client. (Windows 2012 R2)
Event ID	Meaning

Troubleshooting

What do I do if I receive a 'File Not Found' Exception?

When the connector is collecting events from a Microsoft Windows 2008, or 2012 R2 64-bit machine, an exception such as the following may occur:

```
java.io.FileNotFoundException: C:\Windows\System32\dhcp\DhcpSrvLog-XXX.log
```

Windows 64-bit systems redirect file access from `System32` to `SysWOW64` for 32-bit applications. DHCP Server is a 64-bit application that still writes the log to the `System32/dhcp` folder; therefore, the SmartConnector cannot locate the log file. To work around this problem, re-direction must occur on the connector side by configuring the log folder on the DHCP connector as:

```
C:\Windows\Sysnative\dhcp\DhcpServLog-XXX.log
```