



ArcSight SmartConnectors

Software Version: 24.1

Configuration Guide for Microsoft DHCP File SmartConnector

Document Release Date: January 2024

Software Release Date: January 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft DHCP File SmartConnector	4
Product Overview	5
Configuring DHCP	6
Rotating Log Format	6
Auditing Logging	7
Naming of Audit Log Files	7
Enabling Audit Logging for Windows 2012 R2	8
Enabling Audit Logging for Windows 2016	9
Installing the SmartConnector	12
Preparing to Install the SmartConnector	12
Installing the SmartConnector	12
Device Event Mapping to ArcSight Fields	14
Microsoft DHCP IPv4 Event Mappings to ArcSight ESM Fields	14
Microsoft DHCP IPv6 Event Mappings to ArcSight ESM Fields	15
Event IDs for IPv4	15
Event IDs for IPv6	17
Troubleshooting	19
Send Documentation Feedback	20

Configuration Guide for Microsoft DHCP File SmartConnector

This guide provides information for installing and configuring the SmartConnector for Microsoft DHCP File for log file event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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

You must have read/write access to the DHCP folder to read the DHCP files. If the connector is running as a service, then the SYSTEM user must have read/write access to the DHCP folder.



Note: You must restart the connector after you have completed the configuration, so that the connector can start processing events.

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

Log Format	Rotating Logs
	/var/log/access.03.log

Auditing Logging

The following can be specified for DHCP servers running Windows Server 2012 R2, 2016 and 2019:

- 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 2012 R2, 2016 and 2019 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.

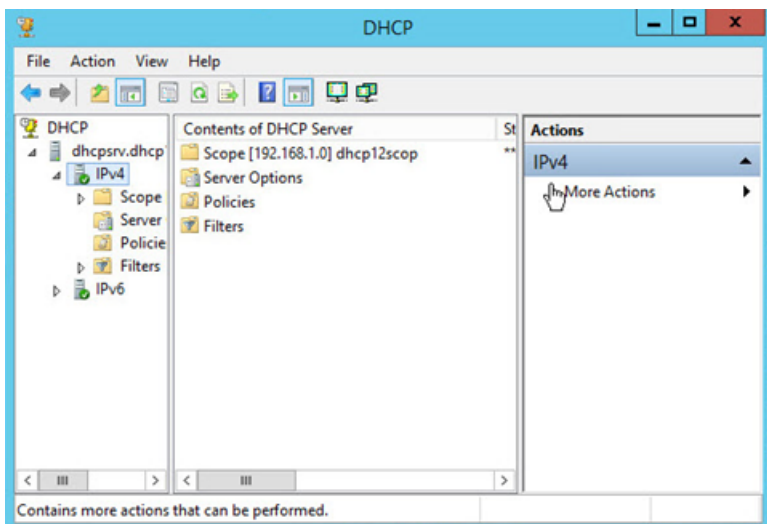
After audit logging starts, the DHCP server performs disk checks at regular intervals, to ensure both the ongoing availability of server disk space and that the current audit log file does not become too large or grow too quickly.

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.

Enabling Audit Logging for Windows 2012 R2

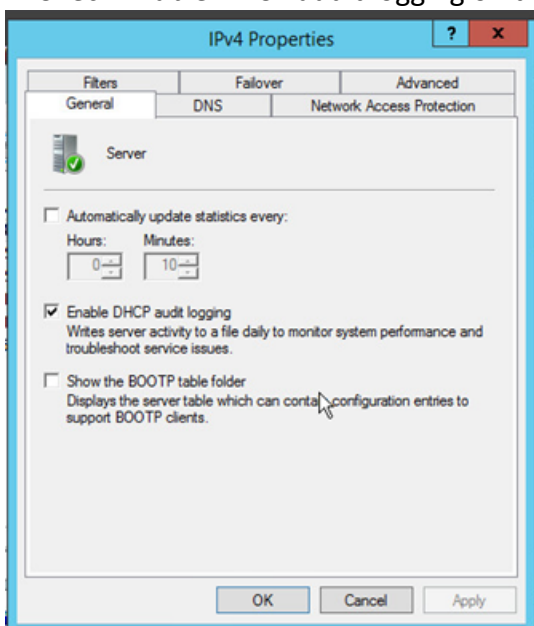
To configure DHCP for event collection:

- 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.

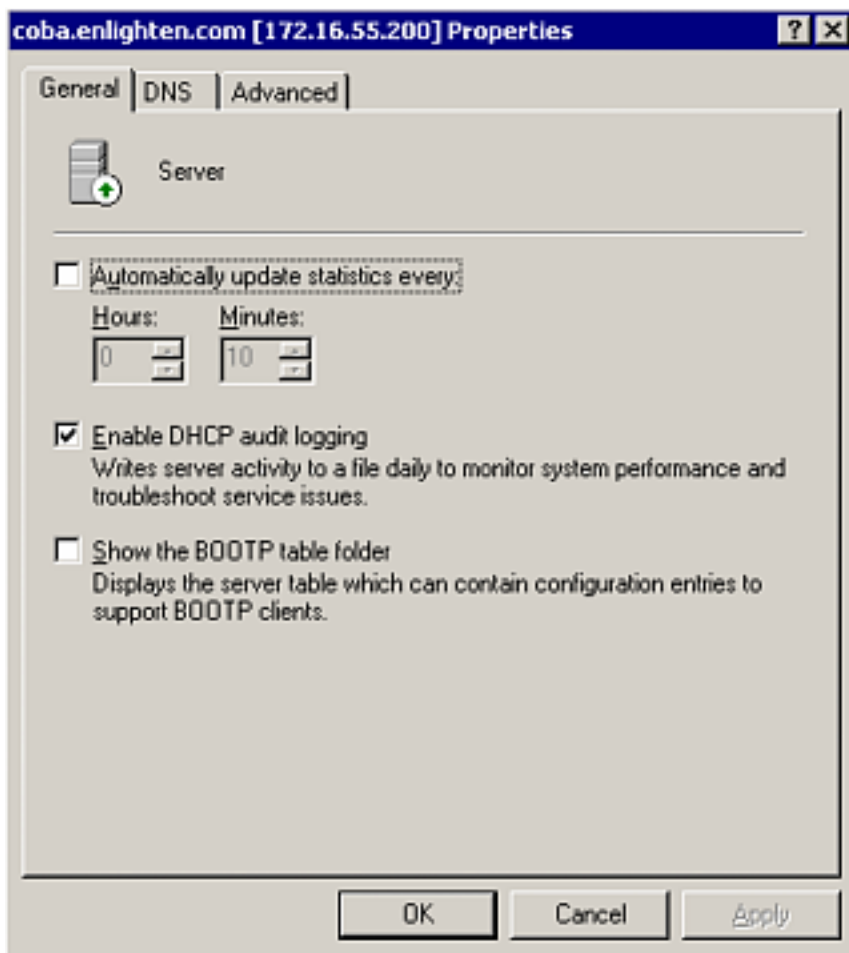


5 Click **OK**.

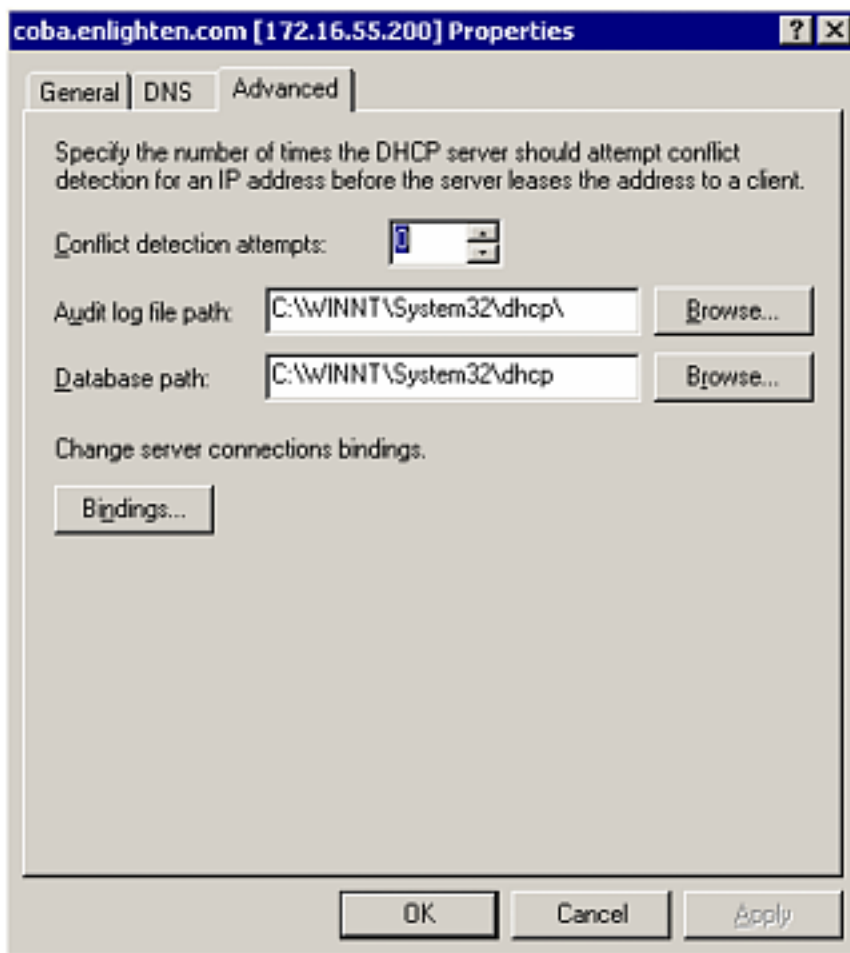
Enabling Audit Logging for Windows 2016

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

Installing the SmartConnector

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



Note: 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.

Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:


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

Installing the SmartConnector


The installation steps described in this section are specific to the Microsoft DHCP File SmartConnector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Microsoft DHCP File SmartConnector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down list, select **Microsoft DHCP File** as the type of connector, then click Next.
5. Enter the following parameters to configure the SmartConnector and then click **Next**.

Parameter	Description
Log File	<p>Enter the parameters for each DHCP server log file to be read by the connector.</p> <p>When you click Add, the default value populated for each of the DHCP server log files is 'C:\WINNT\System32\DHCP\DhcpSrvLog- 'EEE' .log'.</p> <p>Edit the default value for each of the log files.</p> <div> Note: When you edit the default value, ensure that 'EEE' is present in the file name because it is a variable and configures connector to read newly generated files.</div> <p>If IPv6 is used, add v6 to the log file name. For example, 'C:\WINDOWS\System32\DHCP\DhcpV6SrvLog- 'EEE' .log'. V6 is case-insensitive.</p>

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.

 **Note:** If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

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	2012/2016 depend on format of log
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 1	Subnet_Prefix
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	2012/2016 depend on format of log
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.

ArcSight ESM Field	Device-Specific Field
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.
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.

ArcSight ESM Field	Device-Specific Field
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.
11011	Stopped.
11012	Audit Log Paused.

ArcSight ESM Field	Device-Specific Field
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, redirection must occur on the connector side by configuring the log folder on the DHCP connector as:

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

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Microsoft DHCP File SmartConnector (SmartConnectors 24.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!