



DHCP Auditing and Event Logging Guide

How to audit DHCP server on Windows Server 2008 and above

Enable DHCP Server Auditing

- Open DHCP Microsoft Management Console (MMC) snap-in > In the console tree click the DHCP server you want to configure > choose **IPv4** or **IPv6** > call menu by right clicking DHCP instance and go to **Properties** > On the **General** tab, select **Enable DHCP audit logging** > OK

Analyzing DHCP Server Log Files

- DHCP server log files are configured to manage growth and conserve disk resources. DHCP audit logs are located by default at the following path **%windir%\System32\dhcp**

DHCP Server Log File Format (IPv4)

- DHCP server logs are comma-delimited text files with each log entry representing a single line of text. Following are common fields in a log file entry:
 - **ID** - A DHCP Server Event ID code
 - **Date** - Date on which entry was logged
 - **Time** - Time at which entry was logged
 - **Description** - A description of DHCP Server event
 - **IP Address** - The IP Address of DHCP client
 - **Host Name** - The host name of the DHCP client
 - **Mac Address** - MAC address used by network adapter hardware

Prevent Rogue DHCP Servers

- Starting from Windows Server 2008 DHCP Server service is integrated with Active Directory to provide authorization and protect your network from rogue Windows-based DHCP servers
- Following commands used to control authorization for DHCP Servers :
 - **netsh dhcp show server** lists all authorized DHCP servers
 - **netsh dhcp add server <ServerDNS> [ServerIP]** authorizes DHCP
 - **netsh dhcp delete server <ServerDNS> [ServerIP]** revokes authorization

For Detailed Windows Server Auditing, Try Netwrix Auditor - netwrix.com/go/trial-ws

- **Change auditing:** detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™:** scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years or more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

List of Events logged

- 10 - new IP address leased
- 13 - IP address was found in use
- 14 - address pool was exhausted
- 50 - unreachable domain
- 54 - DHCP server was not authorized
- 55 - DHCP server was authorized
- 62 - another DHCP server was found
- 64 - no DHCP enabled interfaces

Complete list of events is available at <http://url2open.com/dhcpevents>

Enable IP Address Conflict Detection

Feature allows to control how many times DHCP server tests an IP address before leasing it to a client

- **netsh dhcp server set detectconflictretry 1**

When conflict detection is enabled DHCP server uses the ping process to test available scope of IP addresses before including it in DHCP lease offered to clients.

Note: A value of no greater than **2** for conflict detection is recommended to prevent increased load at server



 #1 for change auditing

Try Windows Server
Auditing For Free:

netwrix.com/go/trial-ws