



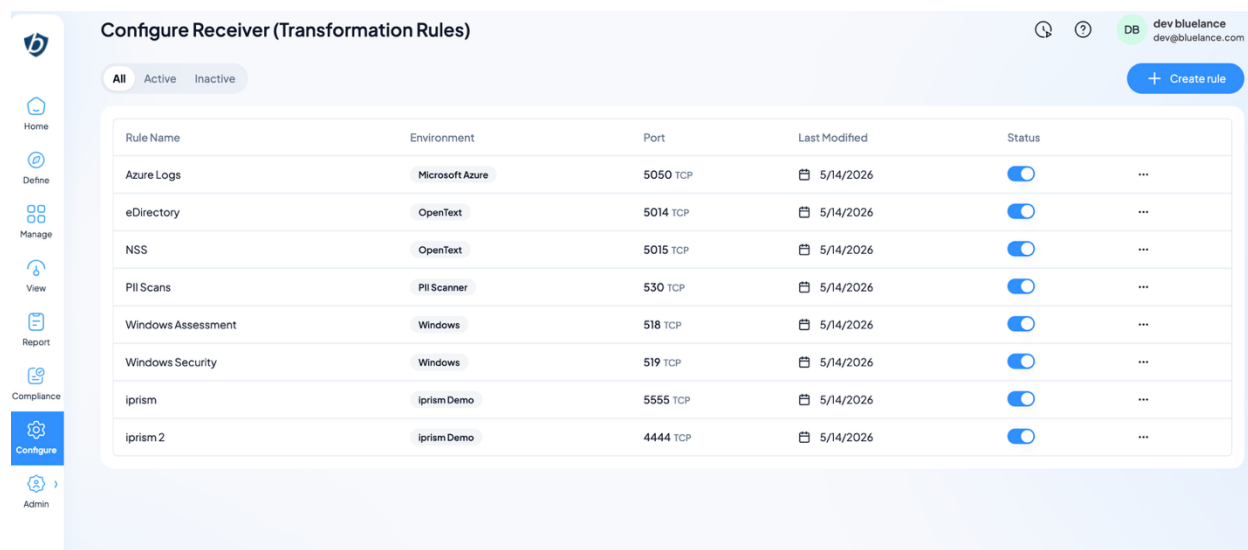
LT Auditor ^{MP} eDirectory and NSS Auditing

This document provides instructions for configuring and forwarding OpenText eDirectory and OES NSS audit activity to LT Auditor ^{MP}.

Audit data is collected by streaming syslog events directly to the LT Auditor ^{MP} application. By default, LT Auditor ^{MP} is configured to receive the following audit streams:

- OpenText eDirectory audit activity on port **5014**
- OpenText OES NSS file activity on port **5015**

These default port assignments can be modified within the LT Auditor ^{MP} console by navigating to the **Configure** section and updating the corresponding **Transformation Rules** for each audit source.



Rule Name	Environment	Port	Last Modified	Status
Azure Logs	Microsoft Azure	5050 TCP	5/14/2026	On
eDirectory	OpenText	5014 TCP	5/14/2026	On
NSS	OpenText	5015 TCP	5/14/2026	On
PII Scans	PII Scanner	530 TCP	5/14/2026	On
Windows Assessment	Windows	518 TCP	5/14/2026	On
Windows Security	Windows	519 TCP	5/14/2026	On
iprism	iprism Demo	5555 TCP	5/14/2026	On
iprism2	iprism Demo	4444 TCP	5/14/2026	On

To modify how LT Auditor ^{MP} receives audit data, click the three vertical action buttons located to the right of the configured receiver and select **Edit**. This will open the **Transformation Rules** configuration window.

Within the **Settings** tab, you can configure the listener parameters used to receive incoming audit data, including:

- IP Address
- Port Number
- Communication Protocol UDP, TCP, or TLS (Secure TCP)

An example of the receiver configuration is shown below.

Edit transformation rule

General

Settings

Rules

Notes

Connection

Type

TCP

Port

5014

Certificate file

Select file

Password

Processor settings

Days to keep logs

7

Threads

3

Max events per thread

1000

Messages

Message offset

Target log

Exclude logging from messages containing specific texts

Partition Status|Purge Vector|Local Received Up To|Transitive Vector|modifiersName|GUID|creatorsName|Revision|Object Class|Obituary|Private K

Use as delimiter to exclude multiple texts

Cancel

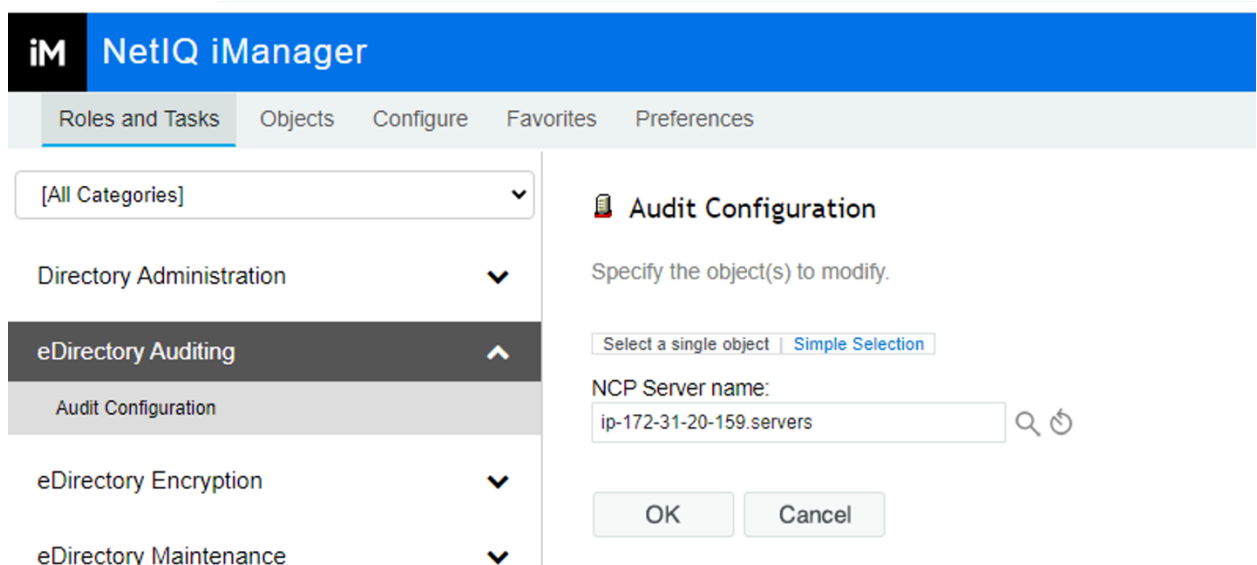
Save

Forwarding eDirectory CEF Audit Log Streams to LT Auditor^{MP}

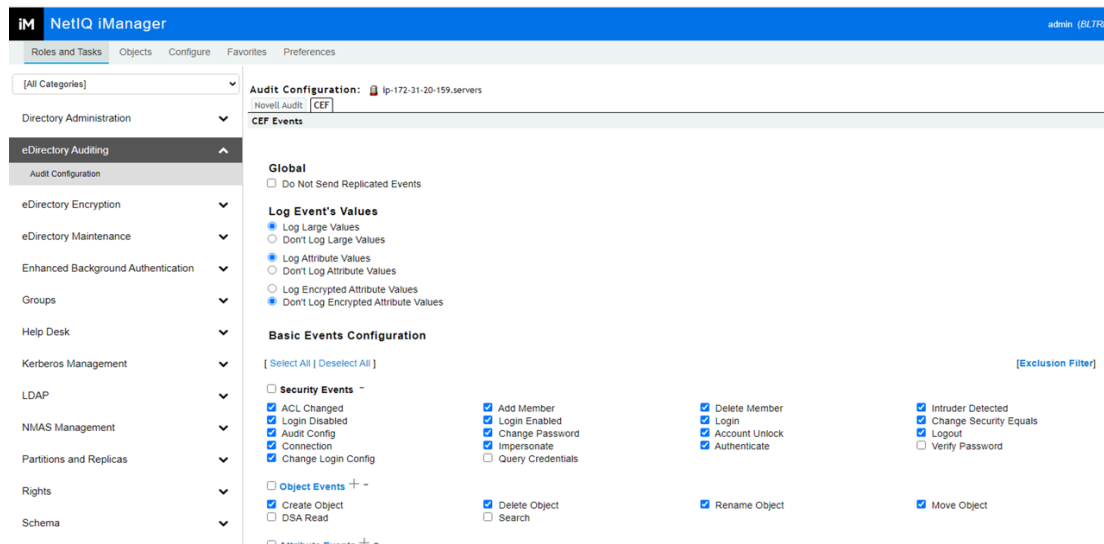
OpenText eDirectory LDAP servers can be configured to forward eDirectory activity logs to LT Auditor^{MP} by updating the following sections for each LDAP server in the environment. It is important to update **all LDAP servers** to avoid missing audit data.

Configure CEF Audit Settings Using iManager

- Login to iManager and select eDirectory Auditing as shown below and select a LDAP NCP server.



- Select CEF as shown below:



- Please configure CEF setting as shown below and save.

Global

☐ Do Not Send Replicated Events

Log Event's Values

- ☒ Log Large Values
☐ Don't Log Large Values
- ☒ Log Attribute Values
☐ Don't Log Attribute Values
- ☐ Log Encrypted Attribute Values
☒ Don't Log Encrypted Attribute Values

Security Events:

[[Select All](#) | [Deselect All](#)]

[[Exclusion Filter](#)]

☐ Security Events + -

- ☒ ACL Changed
- ☒ Login Disabled
- ☒ Audit Config
- ☒ Connection
- ☒ Change Login Config

- ☒ Add Member
- ☒ Login Enabled
- ☒ Change Password
- ☒ Impersonate
- ☐ Query Credentials

- ☒ Delete Member
- ☒ Login
- ☒ Account Unlock
- ☒ Authenticate

- ☒ Intruder Detected
- ☒ Change Security Equals
- ☒ Logout
- ☐ Verify Password

Object Events:

☐ Object Events + -

- ☒ Create Object
- ☐ DSA Read

- ☒ Delete Object
- ☐ Search

☒ Rename Object

☒ Move Object

Attribute Events:

☐ Attribute Events + -

☐ Read Attribute

☐ Compare Attribute Value

☐ Delete Attribute

☒ Add Value

☒ Delete Value

LDAP Events:

☐ LDAP Events + -

☒ LDAP Bind

☒ LDAP Search

☐ LDAP Add Response

☐ LDAP Modify Response

☐ LDAP Modify DN Response

☐ LDAP Bind Response

☐ LDAP Search Response

☐ LDAP Compare

☐ LDAP Delete

☐ LDAP Abandon

☒ LDAP Unbind

☐ LDAP Search Entry Response

☐ LDAP Compare Response

☐ LDAP Delete Response

☐ LDAP Extended Operation

☒ LDAP Connection

☐ LDAP Add

☐ LDAP Modify

☐ LDAP Modify DN

☐ LDAP System Extended Operation

Configure CEF Configuration File on a SLES LDAP Server

- Open the file `auditlogconfig.properties` (default location: `/etc/opt/novell/eDirectory/conf`).
- Uncomment and modify the following lines. This example assumes the use of the TCP protocol. However, you have the choice of UDP or TLS.

```
log4j.rootLogger=debug, S
log4j.appender.S=org.apache.log4j.net.SyslogAppender
log4j.appender.S.Host=<IP Address of LT Auditor MP>
log4j.appender.S.Port=5014
log4j.appender.S.Protocol=TCP
log4j.appender.S.Threshold=INFO
log4j.appender.S.CacheEnabled=no
log4j.appender.S.layout=org.apache.log4j.PatternLayout
log4j.appender.S.layout.ConversionPattern=%c: %m%n
```

- Open `/etc/opt/novell/eDirectory/conf/ndsmodules.conf` and add to ensure auto restart on reboot:

```
cefauditds    auto    #cefauditds
```

- Restart `cefauditds` to activate auditing and forwarding with commands:

```
ndstrace -c "unload cefauditds"
```

```
ndstrace -c "load cefauditds"
```

Forwarding OES-NSS File Activity Log Streams to LT Auditor^{MP}

Sending NSS audit data streams to **LT Auditor^{MP}** requires the installation of an agent on all **SLES OES servers** that host NSS volumes. Please follow the steps outlined below to install and configure this module.

1. Copy and Install the Module

- Copy the package `LTAuditorMP-OES-xx.x.x.x-x.x86_64.rpm` to an OES server that hosts NSS volumes.
- Open a terminal window and switch to root (`su`).
- Run the following command to install the package:

```
rpm -ivh LTAuditorMP-OES-25.0.0.0-0.x86_64.rpm
```
- The module will be installed into the `/opt/bluelance` directory.

2. Configure Audit Forwarding

- Navigate to `/opt/bluelance/bin`.
- Run the configuration script:

```
./update_syslog_config.sh
```
- The script will prompt you to enter the following details:
 1. **Host/IP** of the LT Auditor^{MP} server.
 2. **Port** (default is 5015).
 3. **Protocol** (default is TCP; options: UDP, TCP, or TLS).
 4. If TLS is selected, additional prompts will request:
 - **CA Certificate Path** (path to the certificate file).
 - **Enable Mutual TLS** (default is No).
 - **Verify Server Certificate** (default is Yes).
 - **Server Name** for SNI/hostname verification (default is `syslog.example.com`).
- Once completed, the script will start the required daemons.

3. Manage Services

- You can manage the audit services using systemctl commands:

```
systemctl start ltaudit.service
systemctl stop ltaudit.service
systemctl status ltaudit.service
systemctl restart ltaudit.service
```

- Alternatively, you can use the control script:

```
/opt/blue lance/bin/ltaudit.rc start
/opt/blue lance/bin/ltaudit.rc stop
/opt/blue lance/bin/ltaudit.rc status
```

4. Firewall Configuration

- Ensure that no firewalls are blocking communication between the OES servers and the LT Auditor^{MP} system.
- By default, NSS file audit logs are sent over port **5015**. If you configured a custom port, ensure that port is allowed through the firewall.
- To quickly validate connectivity, run the following command from the OES server:

```
nc -zv <LT_AuditorMP_Host> <Port>
```

- A successful response confirms that the connection is open.

5. Log Verification

- To confirm that auditing is active, review the log file:

```
cat /opt/blue lance/log/nssstatus.log
```

- Ensure that the file contains the message:

```
Successfully opened live vigil file
```

- Additionally, review the application logs located in:

```
/opt/blue lance/logs
```

- Failure to send streams will be recorded in

```
/opt/blue lance/log/syslog_send.log.
```

Note: If the target host is unavailable, audit streams are **cached locally and resent** once connectivity is restored, ensuring **no loss of audit data**.