# LDAP Authentication Broken in Elasticsearch 8.18.0: The Entitlements Bug

Jochen Kressin · 2026-08-18


## Introduction

Imagine you've just upgraded your Elasticsearch cluster to version 8.18.0, excited about the latest features and improvements. You fire up Kibana, enter your Active Directory credentials—and boom. Authentication fails. Your LDAP integration, which has been working flawlessly for months, suddenly stops working with a cryptic `NotEntitledException` error.

If this sounds familiar, you're not alone. A bug in Elasticsearch's entitlements security framework broke LDAP and Active Directory authentication for many users. Let's dive into what happened, why it happened, and how to fix it.

## Problem Description

After upgrading to Elasticsearch 8.18.0, LDAP authentication to Active Directory fails with the following error message:

```
[WARN ][o.e.x.s.a.l.s.LdapUtils  ] [elk] Failed to obtain LDAP connection from pool -
LDAPException(resultCode=91 (connect error), errorMessage='An error occurred while attempting to
connect to server EXAMPLE:389:  IOException(LDAPException(resultCode=91 (connect error),
errorMessage='An error occurred while attempting to establish a connection to server
EXAMPLE/1.1.1.1:389:  NotEntitledException(component [x-pack-core], module [unboundid.ldapsdk],
class [class com.unboundid.ldap.sdk.ConnectThread], entitlement [outbound_network]),
ldapSDKVersion=6.0.3, revision=405ee52a554f9867e81d4598a5b2f97beabeb29a)'))')
```

The key part of this error is: `NotEntitledException(component [x-pack-core], module [unboundid.ldapsdk], class [class com.unboundid.ldap.sdk.ConnectThread], entitlement [outbound_network])`.

This error appears when Elasticsearch tries to connect to your LDAP or Active Directory server—whether you're using standard LDAP on port 389 or LDAPS on port 636. The frustrating part? Tools like `ldapsearch` work perfectly fine from the same server, confirming that network connectivity and LDAP credentials are correct.

## Root Cause Analysis

The root cause is a missing permission in Elasticsearch's new entitlements security framework. The Active Directory and LDAP authenticators in X-Pack use the UnboundID LDAP SDK to establish connections to LDAP servers. This SDK needs to open network sockets, which requires the `outbound_network` entitlement. Unfortunately, the X-Pack Core module's policy file was missing this permission, causing the authentication to fail with a `NotEntitledException`.

The Entitlements framework itself was introduced progressively: it first appeared as an experimental feature in Elasticsearch 8.16.0, and was made permanent—fully replacing the Java SecurityManager—in 8.18.0. The Java SecurityManager had been deprecated since Java 17 and was completely removed in Java 24, which drove this change. The LDAP permission bug was present from the very first version that began enforcing entitlements.

Here's what happens under the hood:

1. A user attempts to log in using LDAP/AD credentials
2. X-Pack's authentication realm tries to connect to the LDAP server
3. The UnboundID SDK attempts to call `Socket.connect()`
4. Elasticsearch's entitlement checker intercepts this call
5. It finds that the `unboundid.ldapsdk` module doesn't have `outbound_network` permission
6. The connection is blocked with a `NotEntitledException`

The irony here is that this security feature designed to make Elasticsearch safer actually broke a critical authentication method.

## Solution

The good news is that Elastic identified and fixed this bug. The fix was included in the following versions (note: patch releases for older minor branches are often published chronologically after newer minor releases, which is why 8.17.9 contains the fix while 8.18.0 does not):

- **Elasticsearch 8.17.9**
- **Elasticsearch 8.18.7**
- **Elasticsearch 9.0.4**

To resolve the issue permanently, upgrade to one of these patched versions. Here's how:

### Step 1: Check Your Current Version

First, verify which version you're running:

```
curl -X GET "localhost:9200/"
```

Look for the `version.number` field in the response.

## Step 2: Upgrade Elasticsearch

Follow Elasticsearch's standard upgrade procedure for your deployment type:

**For a rolling upgrade** (recommended for production):

Repeat the following steps for each node in your cluster, one at a time:

1. Disable shard allocation to avoid unnecessary I/O when the node shuts down:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.routing.allocation.enable": "primaries"
  }
}
```

2. Stop the node, upgrade it to the patched version, and restart it
3. Wait for the node to rejoin the cluster, then re-enable shard allocation:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.routing.allocation.enable": "all"
  }
}
```

4. Wait for the cluster to return to a `green` status before moving to the next node:

```
curl -X GET "localhost:9200/_cluster/health"
```

**For a full cluster restart** (suitable for non-production environments):

1. Stop all Elasticsearch nodes
2. Upgrade all nodes to the patched version
3. Start all nodes

## Step 3: Verify LDAP Authentication

After upgrading, test LDAP authentication:

```
curl -u ldap_user:password -X GET "localhost:9200/_security/_authenticate"
```

You should see a successful response with the user's details and no `NotEntitledException` errors in the logs.

### Workaround Without Upgrading

If you cannot immediately upgrade, Elastic provides an official workaround: patch the entitlement policy directly via a JVM option, without touching Elasticsearch's code or binaries.

Create a file called `${ES_CONF_PATH}/jvm.options.d/workaround-127061.options` and add the following line:

```
-Des.entitlements.policy.x-pack-
core=dmVyc2lvbnM6CiAgLSA4LjE4LjAKICAtIDkuMC4wCnBvbGljeToKICB1bmJvdW5kaWQubGRhcHNkazoKICAgIC0gc2V0X
2h0dHBzX2Nvbm5lY3Rpb25fcHJvcGVydGllcwogICAgLSBvdXRib3VuZF9uZXR3b3Jr
```

This base64-encoded string patches the x-pack-core policy to grant the `unboundid.ldapsdk` module the `outbound_network` entitlement it needs. Restart Elasticsearch after adding the file. This workaround is explicitly documented by Elastic and is safe to apply while you prepare for the upgrade.

## Takeaways

1. **Test authentication after major upgrades**: Even minor version updates can introduce breaking changes. Always test critical functionality like authentication in a non-production environment before upgrading production systems.
2. **The entitlements framework is here to stay**: Elasticsearch's new security model provides better isolation between modules. While this bug was unfortunate, the framework itself is a positive security enhancement. Expect similar permission-related issues to potentially surface as this feature matures.
3. **Version-specific bugs can span multiple releases**: This bug was introduced in 8.16.0 and affected all 8.16.x, 8.17.x (before 8.17.9), 8.18.x (before 8.18.7), and 9.0.x (before 9.0.4) releases. If you encounter authentication issues after upgrading, check the Elasticsearch known issues page and release notes for the full affected version range.
4. **LDAP testing from the OS level isn't enough**: Tools like `ldapsearch` run outside Elasticsearch's JVM and aren't subject to the entitlements framework. Just because LDAP works from the command line doesn't mean it will work within Elasticsearch.
5. **Official workarounds exist for entitlement bugs**: Unlike many code-level bugs, entitlement policy issues can often be patched without upgrading, by injecting a corrected policy via JVM options. Check the Elasticsearch known issues page for the official workaround before rolling back.
6. **Monitor your logs closely**: The `NotEntitledException` error is clear once you know what to look for, but it can be buried in verbose logs. Set up proper log monitoring to catch authentication failures quickly.

**Looking for a robust authentication solution that works reliably across Elasticsearch versions?Search Guard offers enterprise-grade security with comprehensive LDAP, Active Directory, and multi-factor authentication support—battle-tested and actively maintained.**

---

This article was published on the Search Guard blog: https://search-guard.com/blog/ldap-authentication-broken-elasticsearch-8-18-entitlements-bug/