# CFL - Active Directory

Active Directory logs a few different Event Codes for authentication failures.

- 4771 "Kerberos pre-authentication failed"
- 4776 "The domain controller attempted to validate the credentials for an account"

When searching for 4776, you must also search for the word "Failure" because this code is also used for successful AuthN attempts.

Sample search for Splunk:

```
sourcetype="WinEventLog:Security" (EventCode="4771" AND Account_Name !=*$ AND Account_Name != - ) OR
(EventCode="4776" AND Failure AND Logon_Account != *$) | eval uid=coalesce(Logon_Account,Account_Name) | eval
client = coalesce(Client_Address,Source_Workstation) | fields + uid + client + ComputerName
```

This search explicitly removes local system accounts.

Note: 4776 events are logged with "Source Workstation" which is the computer machine name, not a remote IP address. To determine the remote IP address, you may need to examine the IIS logs for the respective request.