The table contained herein provides guidance on where some of the lookup files are stored within the Splunk drive structure on the Splunk Enterprise Server (ES) system. The $SPLUNK\_HOME environment variable below is set to /opt/splunk on the ES system.

Splunk Directories

| **File** | **Path** |
| --- | --- |
| Asset list | $SPLUNK\_HOME/etc/apps/SA-IdentityManagement/lookups |
| Identities | $SPLUNK\_HOME/etc/apps/SA-IdentityManagement/lookups |
| da\_ess\_threat\_local | $SPLUNK\_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat\_intel |
| TAXII feed | $SPLUNK\_HOME/etc/apps/SplunkEnterpriseSecuritySuite/auth |
| whois\_tracker.csv | $SPLUNK\_HOME/var/lib/splunk/modinputs/whois |
| Exported Content | $SPLUNK\_HOME/etc/apps/SA-Utils/local/data/appmaker/\* |
| expected\_views.csv | $SPLUNK\_HOME/etc/apps/SA-AuditAndDataProtection/metadata/local.meta/  --AND--  $SPLUNK\_HOME/etc/apps/SA-AuditAndDataProtection/lookups/expected\_views.csv |
| Application Protocols | $SPLUNK\_HOME/etc/apps/SA-NetworkProtection/lookups/application\_protocols.csv |
| Categories List | $SPLUNK\_HOME/etc/apps/SA-IdentityManagement/lookups |
| Interesting Processes | $SPLUNK\_HOME/etc/apps/SA-EndpointProtection/lookups/interesting\_processes.csv |
| Interesting Services | $SPLUNK\_HOME/etc/apps/SA-EndpointProtection/lookups/interesting\_services.csv |
| Primary Functions | $SPLUNK\_HOME/etc/apps/SA-EndpointProtection/lookups/primary\_functions.csv |
| Prohibited Traffic | $SPLUNK\_HOME/etc/apps/SA-NetworkProtection/lookups/prohibited\_traffic.csv |