**Log Source Type**: Forcepoint Websense Web Security

**Log Source Format**: Syslog

**Version**: 8.5.4

**Vendor Doc Reference(s)**:

* <https://www.websense.com/content/support/library/web/v85/siem/siem.pdf>
* <https://documentation.cysiv.com/articles/#!data-source-onboarding-device-configuration-reference/forcepoint-reference-information-and-cim-field-mapping>

**Sample Log Messages for Testing:**

<159>Dec 15 08:09:47 10.1.100.1 CEF:0|Forcepoint|Security|8.5.4|1525|Transaction permitted|1| act=permitted app=https dvc=10.1.100.184 dst=1.1.1.4.1 dhost=www.youtube.com dpt=443 src=173.188.106.122 spt=0 suser=LDAP:// OU\=Users,OU\=XYZ,OU\=Company,DC\=DC1,DC\=Company1,DC\=com/First Last loginID=- destinationTranslatedPort=0 rt=1702649387000 in=2172 out=596 requestMethod=GET requestClientApplication=- reason=- cs1Label=Policy cs1=- cs2Label=DynCat cs2=0 cs3Label=ContentType cs3=text/javascript; charset\=utf-8 cn1Label=DispositionCode cn1=1026 cn2Label=ScanDuration cn2=12 request=https://www.youtube.com/iframe\_api logRecordSource=Hybrid