İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329936537)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329936538)

[ÖRNEK PARSING 4](#_Toc329936539)

[TEMEL PARSING YAPISI 5](#_Toc329936540)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 27.07.2012 | V1 | Fortigate Syslog Recorder Güncellemesi, DHCP logları eklenildi.)  (CUSTOMSTR8=dir, CUSTOMSTR6=dhcp\_msg, CUSTOMSTR3=hostname, CUSTOMSTR4=mac, CUSTOMSTR5=ip, CUSTOMINT10=lease olarak güncellendi.) | Onur Sarıkaya |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | Fortigate |
| Versiyonu | Fortigate 1240B V.4.0.build0521,120313 MR3 Patch 6 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | FortigateSyslog\_1240B\_V40\_V1Recorder |
| İstek yapan Adı Soyadı | Hüseyin Sevin |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 27.07.2012 |
| İstek yapılan kurum adı | TİGEM |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no | - |
| İlgili ham log yolu/dosya ismi | FortigateSyslog\_1240B\_V40\_V1Recorder\_hamlog.rar |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# 

# ÖRNEK PARSING

|  |  |
| --- | --- |
| 396992 102026001 0 event 2012-07-27 10:17:35.000 | dhcp\_msg = Request | dir = Received | mac = 48:60:BC:05:22:E0 | ip = 172.17.212.17 | lease = 0 | hostname = fguler local7.info TIGEM\_MERKEZ Fortigate Syslog Recorder 0 0 0 0 0 0 0 0 0 0 FGT1KB3910600672 dhcp Client requests IP address/configuration parameters information root 6SEJy+d7S4kA0VSkUsezvxY3ITVK6YkS 2012-07-27 10:12:01.000 0 FIREWALL.FORTIGATE.SYSLOG.LOG.GENERAL.OTHER.S.0 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2012-07-27 10:17:35.000 |
| SOURCENAME | local7.info(Source) |
| EVENTCATEGORY |  |
| EVENTTYPE | event(type) |
| USERSID | - |
| LOGNAME | Fortigate Syslog Recorder |
| COMPUTERNAME | TIGEM\_MERKEZ(devname) |
| CUSTOMSTR1 | FGT1KB3910600672(device\_id) |
| CUSTOMSTR2 | dhcp(subtype) |
| CUSTOMSTR3 | fguler (hostname) |
| CUSTOMSTR4 | 48:60:BC:05:22:E0 (mac) |
| CUSTOMSTR5 | 172.17.212.17 (İp) |
| CUSTOMSTR6 | Request (dhcp\_msg) |
| CUSTOMSTR7 | Client requests IP address/configuration parameters (msg) |
| CUSTOMSTR8 | Received (dir) |
| CUSTOMSTR9 | İnformation (pri) |
| CUSTOMSTR10 | root |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 | 0 (lease) |
| DESCRIPTION |  |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |