İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[ÖRNEK PARSING 4](#_Toc330026388)

[TEMEL PARSING YAPISI 5](#_Toc330026389)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 21.07.2012 | V1 | Customvar1 alanının boş bırakılması durumunda recorder log dosyalarını okur.  block yazılması durumunda sadece block kayıtlarının okunması sağlanır.  delete yazılması durumunda dosya okunur ve sonrasında silinir.  block,delete yazılması durumunda ise block kayıtları okunduktan sonra okunan dosya delete edirlir. | Fatih Sakar |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | BelNum12072012-01 |
| Ürün Adı | IBekci |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | IBekciAccessV\_1\_0\_1Recorder |
| İstek yapan Adı Soyadı | Fatih Sakar |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 12.06.2012 |
| İstek yapılan kurum adı | Başbakanlık |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | 20120605121001.kyt |
| İlişkili form adı |  |
| Servis Yetkilisi Notları | ----------------- |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| Jun 05 12:05:02.149209 logid -17- rule 31/(match) block in on et1\_A: 178.33.236.150.4234 > 172.16.1.10.53: 17937 [1au][|domain] | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Jun 05 112:05:02 |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | block |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | in |
| CUSTOMSTR2 | et1\_A |
| CUSTOMSTR3 | 178.33.236.150 |
| CUSTOMSTR4 | 172.16.1.10.53 |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | 17 |
| CUSTOMINT2 | 31 |
| CUSTOMINT3 | 4234 |
| CUSTOMINT4 | 17937 |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam log |

# 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 |  |