İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[TEMEL PARSING YAPISI 4](#_Toc330026389)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 12.12.2012 | V1 | -------------------------------- | Kaan Emre KOŞAR |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | TMG2010 |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | TMG2010V1\_0\_0Recorder |
| İstek yapan Adı Soyadı | Kaan Emre KOŞAR |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 27.12.2012 |
| İstek yapılan kurum adı | THK Universitesi |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | [\\95.183.206.2\TMG\_Log\\*](file:///\\95.183.206.2\TMG_Log\*) (örn ISALOG\_20121221\_FWS\_000.w3c) |
| İlişkili form adı |  |
| Servis Yetkilisi Notları | ----------------- |
| Geliştirici Notları |  |

# TEMEL PARSING

|  |  |
| --- | --- |
| **THKUS05 2012-12-23 00:00:02 ICMP 95.183.207.253:1280 95.183.207.254:256 95.183.207.253 External Local Host Denied 0xc004000d Default rule Unidentified IP Traffic 0 0 0 0 - - - - 0 0 - - :: - 0 -** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2012-12-23 00:00:02** |
| SOURCENAME | **THKUS05** |
| EVENTCATEGORY | **ICMP** |
| EVENTTYPE | **Denied** |
| USERSID |  |
| LOGNAME | **RecorderName** |
| COMPUTERNAME |  |
| CUSTOMSTR1 | **External** |
| CUSTOMSTR2 | **Local Host** |
| CUSTOMSTR3 | **95.183.207.253 Not: IPv6 olarak gelebilir.** |
| CUSTOMSTR4 | **95.183.207.254 Not: IPv6 olarak gelebilir.** |
| CUSTOMSTR5 | **95.183.207.253 Not: IPv6 olarak gelebilir.** |
| CUSTOMSTR6 | **Unidentified IP Traffic (tek kelimede olabilmekte.)** |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | **Default rule** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 | **1280** |
| CUSTOMINT4 | **256** |
| CUSTOMINT5 | **0 birincisi** |
| CUSTOMINT6 | **0 ikincisi** |
| CUSTOMINT7 | **0 üçüncüsü** |
| CUSTOMINT8 | **0 dördüncüsü** |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam log |