İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[TEMEL PARSING YAPISI 4](#_Toc330026389)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 17.12.2013 | 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 | TMG2010WEBV1\_0\_0Recorder |
| İstek yapan Adı Soyadı | Kaan Emre KOŞAR |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 17.12.2013 |
| İstek yapılan kurum adı | TUBITAK BILGEM |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | [\\95.183.206.2\bs\LOGS\INTRA-TMG\\*](file:///\\95.183.206.2\bs\LOGS\INTRA-TMG\*) (örn INTRA-TMG1\_ISALOG\_20131217\_WEB\_000.w3c) , (örn INTRA-TMG2\_ISALOG\_20131217\_WEB\_000.w3c)  Dosya adlarındaki “INTRA-TMG1” kısmı logun script ile hangi makinadan geldiği anlaşılması için kurum tarafından eklenmektedir. Orginal loglar “ISALOG\_...” formatında oluşmaktadır. Yazılacak Recorder Generic olması amacıyla sıralamalarda bu isimlendirmeye takılmadan çalışabilmesi ve ISALOG dan sonraki kısma dikkat edilmesi gerekmektedir. |
| İlişkili form adı |  |
| Servis Yetkilisi Notları | ----------------- |
| Geliştirici Notları |  |

# TEMEL PARSING

|  |  |
| --- | --- |
| **10.222.90.23 INTRA\burak.costu Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 Y 2013-12-17 12:42:41 INTRA-TMG-1 http://forum.antu.com/konular.aspx?gID=4&fID=9 app.medyanetads.com 83.66.160.22 80 32 3298 482 http GET http://app.medyanetads.com/impression.a2?tid=6554&ciid=337182&lid=0&led=0&ltype=0&cachebuster=109261689708 image/gif Inet 200 Internet Access Req ID: 0ab43fdd; Compression: client=No, server=No, compress rate=0% decompress rate=0% Internal External 0x480 Allowed - - 10.223.120.50 None app.medyanetads.com 60683 -** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2013-12-17 12:42:41** |
| SOURCENAME | **10.222.90.23** |
| EVENTCATEGORY | **Allowed** |
| EVENTTYPE | **GET** |
| USERSID | **INTRA\burak.costu** |
| LOGNAME | **RecorderName** |
| COMPUTERNAME | **INTRA-TMG-1** |
| CUSTOMSTR1 | **app.medyanetads.com** |
| CUSTOMSTR2 | **http** |
| CUSTOMSTR3 | **10.223.120.50** |
| CUSTOMSTR4 | **83.66.160.22** |
| CUSTOMSTR5 | **http://forum.antu.com/konular.aspx?gID=4&fID=9** |
| CUSTOMSTR6 | **http://app.medyanetads.com/impression.a2?tid=6554&ciid=337182&lid=0&led=0&ltype=0&cachebuster=109261689708** |
| CUSTOMSTR7 | **Internet Access** |
| CUSTOMSTR8 | **Internal** |
| CUSTOMSTR9 | **External** |
| CUSTOMSTR10 | **Req ID: 0ab43fdd; Compression: client=No, server=No, compress rate=0% decompress rate=0%** |
| CUSTOMINT1 | **3298** |
| CUSTOMINT2 | **482** |
| CUSTOMINT3 | **60683** |
| CUSTOMINT4 | **80** |
| CUSTOMINT5 | **200** |
| CUSTOMINT6 | **32** |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam log |

|  |  |
| --- | --- |
| **Fields** | **Example Log** |
| c-ip | 10.222.90.23 |
| cs-username | INTRA\burak.costu |
| c-agent sc-authenticated | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 Y |
| date time | 17.12.2013 12:42 |
| s-computername | INTRA-TMG-1 |
| cs-referred | <http://forum.antu.com/konular.aspx?gID=4&fID=9> |
| r-host | app.medyanetads.com |
| r-ip | 83.66.160.22 |
| r-port | 80 |
| time-taken | 32 |
| sc-bytes | 3298 |
| cs-bytes | 482 |
| cs-protocol | http |
| s-operation | GET |
| cs-uri | <http://app.medyanetads.com/impression.a2?tid=6554&ciid=337182&lid=0&led=0&ltype=0&cachebuster=109261689708> |
| cs-mime-type | image/gif |
| s-object-source | Inet |
| sc-status | 200 |
| rule | Internet Access |
| FilterInfo | Req ID: 0ab43fdd; Compression: client=No, server=No, compress rate=0% decompress rate=0% |
| cs-network | Internal |
| sc-network | External |
| error-info | 0x480 |
| action | Allowed |
| AuthenticationServer | - |
| MalwareInspectionThreatLevel | - |
| NAT address | 10.223.120.50 |
| SessionType | None |
| UrlDestHost | app.medyanetads.com |
| s-port | 60683 |
| SoftBlockAction | - |
|  |  |
|  |  |
|  |  |