

User's Manual

FOR VAMSOFT ORF LOG TO XML CONVERSION TOOL 1.1

Revision: 1.1
Date: June 17, 2008

Preface

WHAT IS THIS MANUAL ABOUT?

This documentation describes the usage of the ORF Log To XML command line conversion tool.

WHO SHOULD READ THIS MANUAL?

This guide is intended to be read by software developers and system administrators who need the ORF log data represented as an XML document.

HOW DOES THIS SOFTWARE HELP?

This tool converts the ORF text log files to **XML**. XML is an evolving, platform independent standard for representing data, supported by most of today's development environments. By using **XSLT** (*Extensible Stylesheet Language Transformations*), the XML data can be presented in a human-readable form (typically HTML) with a very little effort. Due to its low memory footprint, this tool can handle even large ORF log files well.

Requirements

SYSTEM REQUIREMENTS

The software supports the following operating system platforms:

- Microsoft® Windows® 2000
- Microsoft® Windows® 2003
- Microsoft® Windows® XP
- Microsoft® Windows® Vista

SOFTWARE REQUIREMENTS

The tool requires the Vamsoft OLE DB Log Provider 1.5 or above to be installed locally. You can download this software from <http://www.vamsoft.com/logprovider>.

(Administrator privileges are required to install and uninstall the provider.)

Note that **ORF** is not required to be installed locally.

Package Contents

The package is organized into the following structure:

/tool

Contains the conversion tool.

/sample

/sample.log

A sample log file, also contained in the log provider package.

/readme.pdf

This document.

■ Installation and Uninstallation

To install this tool, extract the contents of the package into an arbitrary folder - a folder in the system path might be a practical idea. You can safely delete this folder if you do not need the tool anymore, no uninstallation is needed.

■ Using the Tool

DISPLAYING HELP

A brief help can be displayed from the command line using the *-h* (or *-help*) switch or by using no parameters at all.

PERFORMING CONVERSION

The conversion can be started running `orflogtoxml.exe` with the *-c* (or *-convert*) switch:

`orflogtoxml -c source_filename target_filename`

Where *source_filename* is the file name of the ORF log to be converted, and *target_filename* refers to the resulting XML file. File names containing spaces should be enclosed in double quotes. If the target file already exists, it will be overwritten.

SAMPLE LOG

You can test the utility using the sample log file from the package */samples/sample.log*. This file demonstrates some possible log column values for testing purposes. Executed in the package */sample* folder, the following command should produce `sample.xml`:

`orflogtoxml -c sample.log sample.xml`

Viewing the generated `sample.xml` is the easiest way to understand the concept of the output format.

DATE LOCALIZATION

When no additional parameter is added, timestamps are written to the file according to the ISO 8601:1988(E) format also used in ORF log files. To specify a different format, you should submit the Locale ID (LCID) to be used when converting the Time field of the log records. For example,

```
orflogtoxml -c source_filename target_filename 1033
```

would convert dates according to the U.S. English format. A list of locale identifiers can be found at <http://www.microsoft.com/globaldev/reference/winxp/xp-lcid.mspx>.

ERRORS DURING THE CONVERSION

Errors occurring during the conversion are written to the console output and result in immediate abortion. Also, the exit code is set to 255.

XML Format

The resulting XML file contains all information found in the source log file except for the comment fields.

The root node is an `<ORFLog>` element. It has only one attribute, the *source_filename* (provided when [performing the conversion](#)) as *name*.

The root node has `<Entry>` child elements matching the records (lines) in the log file.

The `<Entry>` element holds values extracted from the log record, associated with columns of log file. For instance, recipient(s) can be found in one or more `<Recipient>` elements, if any. The following is a snippet from *sample.xml*:

```
<Entry>
  <Version>4.0 REGISTERED</Version>
  <Verbose>True</Verbose>
  <Class>System Message</Class>
  <Server>mail.example.net</Server>
  <Time>2007-05-04T09:49:01</Time>
  <Severity>Information</Severity>
  <FilteringPoint>Non-filtering</FilteringPoint>
  <Message>System event with Info severity.</Message>
  <LineNr>0</LineNr>
</Entry>
```

The table below lists the possible child elements, and their possible values (where appropriate).

Element	Description	Values / Example
<i>Version</i>	Version of the ORF instance that generated the event.	<i>4.0 REGISTERED</i>
<i>Verbose</i>	Tells if the event has <i>Verbose</i> or <i>Short</i> log message.	True, False
<i>Class</i>	Event class.	System Message, Blacklist, Whitelist, Pass, Intermediate
<i>Server</i>	Local server name.	<i>smtp.example.net</i>
<i>Source</i>	SMTP Virtual Server related to the event.	<i>SMTPSVC-1</i>
<i>Time</i>	Event timestamp in the format specified, see Date Locale for more information.	<i>January 1, 2007</i>
<i>Action</i>	Specifies an action performed.	See Action Values for possible values and explanation.
<i>Severity</i>	Event severity.	Information, Warning, Error, Critical Error
<i>FilteringPoint</i>	Tells at what stage the event occurred.	On Arrival, Before Arrival, Non-filtering
<i>RelatedIP</i>	IPv4 address related to the event.	<i>192.168.251.1</i>
<i>MessageID</i>	MIME Message-ID of the email.	<i><d0e601c63af5\$64688a55\$7df82f1@example.com></i>
<i>Sender</i>	SMTP envelope sender email address.	<i>sender@example.com</i>
<i>Recipient</i>	Contains an SMTP envelope recipient of the email.	<i>john@example.com</i>
<i>HeloDomain</i>	Contains the SMTP HELO/EHLO domain.	<i>example.com</i>
<i>Subject</i>	Subject of the email, decoded, as an Unicode string. Might contain trailing whitespace.	<i>Congratulations!</i>
<i>Message</i>	Log message text.	<i>Email passed checks.</i>
<i>LineNr</i>	The number of the line containing the log record inside the log file.	Non-negative integer values.

ACTION VALUES

The following table lists the possible values of *<Action>* elements and their meaning.

Value	Action Performed
<i>Reject</i>	Email was rejected.
<i>Tag Subject</i>	Email subject was tagged.
<i>Tag Header</i>	Email header was tagged.
<i>Redirect Email</i>	Email was redirected.
<i>Replace Attachment</i>	Attachment(s) were replaced.
<i>Remove Recipient</i>	Recipient(s) were removed.
<i>Whitelist Recipient</i>	Recipient(s) were whitelisted.

COMPATIBILITY AND COLUMN TRANSLATIONS

The tool is compatible with logs generated by ORF version 1.0 and above, though (due to format changes between ORF versions) some columns may have data in ORF 4.0 and later logs only.

Also, some columns may be translated into the new format. For instance, ORF 3.0 logs did not have an *Action* column, but expressed the action performed in the *Event Class* column. In the case of the **RejectMail** ORF 3.0 event class, the event class is converted into an ORF 4.0 **Blacklist event** class and a **Reject** action (*<Action>Reject</Action>*).

Notes

INTERNATIONALIZATION ISSUES

The *Subject* element contains the decoded email subject. Due to the nature of emails, it is expected that this column contains international characters, e.g. Cyrillic, Hebrew or Far Eastern text. Make sure that transformations made on the Subject column data preserves the original Unicode UTF-16 encoding of the text.

PARSING THE LOG MESSAGE

When writing your application, please consider that we do not recommend parsing the log message column contents because:

- Messages are likely to change between ORF versions
- Messages are different for the default Verbose mode and the Short logging mode
- Messages are not documented (for the above two reasons)

LOG EVENT TIME

ORF generates log event timestamps in the local time zone or in UTC, depending on the configuration. In either case, the event times are adjusted to the local time zone when the provider returns them. For example, if the log was generated in time zone DST (UTC-7 hours, Los Angeles) but the logs were processed on a computer in EDT (UTC-5 hours, New York), 1:00AM DST is returned as 3:00AM, due to the +2 hours difference between DST and EDT.

Note that the conversion tool does not perform the above adjustment on the log file names, because the file name format is configurable and might contain a timestamp.

■ Technical Support

If you have any questions regarding the above, please contact us.

Email: orf-support@vamsoft.com
News server: news.vamsoft.com
Phone: (+36) 1 279 2090
Fax: (+36) 1 279 1260
World Wide Web: <http://www.vamsoft.com/>
Postal Address: Vamsoft Ltd.
Budapest
Györök utca 11.
H-1113
HUNGARY