Developer's Manual

FOR **VAMSOFT OLE DB PROVIDER FOR ORF LOG FILES 1.5**

Revision: 1.5
Date: June 18, 2008

Preface

WHAT IS THIS MANUAL ABOUT?

This documentation intends to supply the reader with information about using the Vamsoft OLE DB Provider for ORF Log Files.

WHO SHOULD READ THIS MANUAL?

This guide is intended to be read by software developers who want to process ORF log files programatically, e.g. for generating reports or importing them into an SQL database. The manual assumes that the reader is familiar with ORF, the selected development environment and the Microsoft® ActiveX® Data Objects (ADO) or ADO.NET technologies.

HOW DOES THIS SOFTWARE HELP?

The provider allows the developer to access processed ORF log data as database tables using the OLE DB Provider written specifically for this purpose. The OLE DB Provider can be used easily from any languages/technologies that support COM and ActiveX Data Objects (ADO) or ADO.NET, including, but not limited to:

- Microsoft® Visual C++®
- Microsoft® Visual Basic®
- Microsoft® Visual C#®
- Microsoft® Visual Basic.NET®
- Borland® Delphi™
- VBScript (Windows® Scripting Host)
- JScript (Windows® Scripting Host)
- Classic ASP (VBScript/JScript)
- Sun® Java
- ASP.NET
- PHP (Win32 only)
- Perl (Win32 only)
- Python (Win32 only)
- Ruby (Win32 only)

This package offers examples in all languages above, except Microsoft® Visual Basic® and Sun® Java.

System Requirements

The software supports the following operating system platforms:

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

- Microsoft® Windows® Vista

Note that **ORF is not required** to be installed locally, the provider runs independently.

Administrator privileges are required to install and uninstall the provider.

The development tool must support manipulating COM/OLE objects (ActiveX Data Object or ADO, specifically).

Package Contents

The package is organized into the following structure:

/provider
Contains the OLE DB provider DLL file.

/samples
Contains a sample log file and code examples for using the provider in various programming languages.

/sample.log
A sample log file that demonstrates the various possible combinations of log column values, for testing purposes.

/asp
Classic ASP examples, written in VBScript and JavaScript/JScript.

/asp.net
ASP.NET examples, written in C# and Visual Basic.NET (Microsoft® Visual Studio 2005, Visual Studio 2005 Express or newer, .NET 2.0).

/delphi
Borland® Delphi™ 7.0 example.

/jscript
Windows® Scripting Host (WSH) example, with JavaScript/JScript

/perl
Perl 5 example (ActiveState ActivePerl, Win32).

/php
PHP 4/5 example (Win32).

/vbscript
Windows® Scripting Host (WSH) example, with VBScript.

/readme.pdf
This document.

Installing and Uninstallation

Both the installation and uninstallation of the provider require administrator privileges.

INSTALLATION

Follow the steps below to install the provider.

1. Copy the ***orflogdb.dll*** file from the ***/provider*** folder to an arbitrary folder on the computer. Note that the file must not be moved or deleted once installed.

2. Open a command prompt, enter to the above folder and run:

   regsvr32 orflogdb.dll

   On a successful installation, you should get "*DllRegisterServer in orflogdb.dll succeeded*".

Your development environment might have to be restarted to take advantage of the newly installed provider.

If you need to move the provider DLL to another location after it has been installed, uninstall the provider first, move the file, and reinstall it.

UNINSTALLATION

1. Open a command prompt, enter to the installation folder and run:

   regsvr32 -u orflogdb.dll

   On a successful installation, you should get "*DllUnregisterServer in orflogdb.dll succeeded*".

NOTES

Before installing a new version of the provider, the previous version **MUST** be uninstalled first.

Using the Provider

PREREQUISITES

To use the provider, you need a development tool that supports manipulating COM/OLE objects and ActiveX Data Objects (ADO) or ADO.NET. The provider also has to be installed, as described in the Installation section.

CONNECTION STRING

An ADO *connection string* is list of property-value pairs that describe the ADO connection parameters. Connection strings are used to connect to ADO data sources. In the case of this provider, two properties must be specified in the connection string: the *provider name* and the *log folder*.

Provider property: Provider name
The provider can be specified in the *connection string* or the value of the *Provider* property of an ADODB.Connection object. The following two provider names are accepted:

orflogdb.provider
-or-
Vamsoft OLE DB Provider for ORF Log Files

Data Source property: Log folder
The connection string must specify the location of the ORF log files to be opened in the *Data Source* property.

Examples:

Provider=orflogdb.provider;Data Source=C:\Logs\ORF
Provider=Vamsoft OLE DB Provider for ORF Log Files;Data Source=C:\Logs\ORF

TABLE NAMES

The provider searches the log folder for ORF log files and turns them into database tables. The tables are named the same as the log file, e.g. ***orfee-2008-01-01.log*** can be a table name for a log file generated on January 1, 2008.

For querying the list of tables (log files), use the OpenSchema() method of the ADODB.Connection object with the *adSchemaTables* parameter.

TABLE COLUMNS

Log columns are translated into table columns for each log file. For more information, see the Compatibility and Column Translation section below.

The table schema is fixed, so the table columns below are always present, even if their corresponding log column is missing. For example, the *x-msg-subject* log column may not be present

in the log file, but the *Subject* table column is guaranteed to be available (containing empty strings).

The table below lists the columns, their types, and their possible values (where appropriate).

Column name	Description	Values / *Example*	Type
Version	Version of the ORF instance that generated the event.	*4.0 REGISTERED*	Text
Verbose	Tells if the event has *Verbose* or *Short* log message.	True, False	Boolean
Class	Event class.	System Message, Blacklist, Whitelist, Pass, Intermediate	Text
Server	Local server name.	*smtp.example.net*	Text
Source	SMTP Virtual Server related to the event.	*SMTPSVC-1*	Text
Time	Event timestamp, always in the local time zone.	*January 1, 2007*	DateTime
Action_Reject	True, if the email was rejected.	True, False	Boolean
Action_TagSubject	True, if the email subject was tagged.	True, False	Boolean
Action_TagHeader	True, if the email header was tagged.	True, False	Boolean
Action_Redirect	True, if the email was redirected.	True, False	Boolean
Action_ReplaceAtt	True, if attachment(s) were replaced.	True, False	Boolean
Action_RemoveRcpt	True, if recipient(s) were removed.	True, False	Boolean
Action_WhitelistRcpt	True, if recipient(s) were whitelisted.	True, False	Boolean
Severity	Event severity.	Information, Warning, Error, Critical Error	Text
FilteringPoint	Tells at what stage the event occurred.	On Arrival, Before Arrival, Non-filtering	Text
RelatedIP	IPv4 address related to the event.	*192.168.251.1*	Text
MessageID	MIME Message-ID of the email.	*<d0e601c63af5$64688a55$7df782f1@example.com>*	Text

Sender	SMTP envelope sender email address.	*sender@example.com*	Text
Recipients	A semicolon-separated list of the SMTP envelope recipient(s) of the email.	*john@example.com;jane@example.com*	Text
HeloDomain	Contains the SMTP HELO/EHLO domain.	*example.com*	Text
Subject	Subject of the email, decoded, as an Unicode string.	*Your reduced salary.*	Text
Message	Log message text.	*Email passed checks.*	Text
LineNr	The number of the line containing the log record inside the log file.	Non-negative integer values.	Integer

COMPATIBILITY AND COLUMN TRANSLATIONS

The table schema outlined above conforms with the ORF 4.2 log format, but backward compatibility is guaranteed with ORF logs (from version 1.0). However, due to log format changes in the various ORF versions, some columns may have data in ORF 4.2 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 the **RejectMail** ORF 3.0 event class, the event class is decomposed into an ORF 4.0 ***Blacklist*** *event class* and a ***Reject*** *action* (*Action_Reject = True)*.

SQL SUPPORT

The provider *does not* support SQL statements.

Examples

SAMPLE LOG

You can test the provider using the sample log file from the package */samples/sample.log*. This file demonstrates the various possible combinations of log column values, for testing purposes.

Note that the sample log file contains Unicode characters: an email subject. These are visualized improperly in the Delphi™ 7.0 data controls (see the source code for more information), and on the console in case of the WSH examples, but the content received from the provider is the same as the data found in the log file.

NOTES: C# EXAMPLE

The C# example can be compiled and run using Microsoft® Visual C# Express or Microsoft® Visual Studio ® 2005. The project requires .NET 2.0.

NOTES: DELPHI™ EXAMPLE

Compiling the Delphi™ example requires Borland® Delphi™ 7.0 installed with ADO Express components. Before the application could be run within the debugger, it is recommended to add **"EOleDbException"** to the list of ignored exceptions (go to *Tools>Debugger Options>Language Exceptions* from the main menu), as it is used internally by the provider.

NOTES: WINDOWS® SCRIPTING HOST EXAMPLES

Both the JavaScript/JScript and the VBScript example can be run using **cscript.exe** as demonstrated below:

```
cscript dump.js
cscript dump.vb
```

In case of a successful run, you should be able to see the contents of the *sample.log* file dumped to the console.

Notes

INTERNATIONALIZATION ISSUES

The *Subject* column of the log tables contain 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. For instance, if you plan to import the log data into an SQL database, use database field types that support storing Unicode text (e.g. NTEXT/NVARCHAR for Microsoft® SQL Server) and/or choose the database/table/field encoding with Unicode-compliance in mind.

PARSING THE LOG MESSAGE

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

- 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, e.g. Los Angeles) and the logs are being processed on a computer in EDT (UTC-5 hours, e.g. New York), 1:00AM DST is returned as 3:00AM, due to the +2 hours difference between DST and EDT.

Note that the provider does not perform the above adjustment on the log file names. Actually, the provider does not have the concept of the timestamp in the log file name, because the file name format is configurable. By default, ORF generates logs with *orfee-{YEAR}-{MONTH}-{DATE}.log* format, but this can be changed by the user. When ORF needs to log an event, it takes the timestamp for the event and generates a log file name from that. According to the new filename, the event is logged either to an existing log file is used or a new log file one is generated. Thus, the log files might have a timestamp in their name and if they do, they are in the configured time zone (local time zone by default, or UTC).

SQL SERVER 2005 SUPPORT

Importing log data into Microsoft® SQL Server 2005 using the *Linked Server* feature is not supported from SQL Server 2005 Service Pack 2. In previous versions, make sure to set the *Allow inprocess* option (right-click on *Server Objects/Linked Servers/Providers/orflogdb.provider*), otherwise the provider will fail to load.

Technical Support

Please contact our technical support using contact options below. Using the Community Forums is recommended (we are active there as well).

Before contacting us, please check the product documentation and the ORF FAQ, you may find a quick answer for your question there.

Email:	orf-support@vamsoft.com
Community Forums	http://www.vamsoft.com/forum
Phone:	(+36) 1 279 2299
Fax:	(+36) 1 279 1260
World Wide Web:	http://www.vamsoft.com
Postal Address:	Vamsoft Ltd. Budapest Györök utca 11. H-1113 HUNGARY