# Your Question

**Article:** 00081
**Updated:** January 5, 2006
**Question:**
How to Manage and Modify Dates in Net Report Management Console Filters?

# Net Report Answer

## Introduction

This article explains how to manage and modify dates in Net Report Management Console Filters. This article includes the following sections:

- **Section 1:** Introducing the _time Field in NELRF.
- **Section 2:** Managing Dates Provided by Devices.
- **Section 3:** Modifying Dates.
- **Section 4:** Introducing the Locale Default Program Language.

## Terminology and Abbreviations

**Agent:** Agents are search tools that automatically seek out relevant on-line information based on your specifications. Agents are also called intelligent agents, personal agents, droids and so on.

**Event:** An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory. Most modern applications, particularly those that run in Macintosh and Windows environments, are said to be event-driven, because they are designed to respond to events.

**Field:** A space allocated for a particular item of information. A tax form, for example, contains a number of fields: one for your name, one for your Social Security number, one for your income, and so on. In database systems, fields are the smallest units of information you can access. In spreadsheets, fields are called cells. Most fields have certain attributes associated with them. For example, some fields are numeric whereas others are textual, some are long, while others are short. In addition, every field has a name, called the field name. In database management systems, a field can be required, optional, or calculated. A required field is one in which you must enter data, while an optional field is one you may leave blank. A calculated field is one whose value is derived from some formula involving other fields. You do not enter data into a calculated field; the system automatically determines the correct value. A collection of fields is called a record.

**Filter:** A program that accepts a certain type of data as input, transforms it in some manner, and then outputs the transformed data. For example, a program that sorts names is a filter because it accepts the names in unsorted order, sorts them, and then outputs the sorted names. Utilities that allow you to import or export data are also sometimes called filters.

**Locale:** the set of information that corresponds to a given language and country. The code locale setting affects the language of terms such as keywords and defines locale-specific settings such as the decimal and list separators, date formats, and character sorting order.

**NELRF:** Net Report Extensible Log Record Format.

**Object:** Generally, any item that can be individually selected and manipulated. This can include shapes and pictures that appear on a display screen as well as less tangible software entities. In

object-oriented programming, for example, an object is a self-contained entity that consists of both data and procedures to manipulate the data.

**OLE**: (Object Linking and Embedding) is Microsoft's framework for a compound document technology. Briefly, a compound document is something like a display desktop that can contain visual and information objects of all kinds: text, calendars, animations, sound, motion video, 3-D, continually updated news, controls, and so forth. Each desktop object is an independent program entity that can interact with a user and also communicate with other objects on the desktop. Part of Microsoft's ActiveX technologies, OLE takes advantage and is part of a larger, more general concept, the Component Object Model (COM) and its distributed version, DCOM. An OLE object is necessarily also a component (or COM object).

**Parameter:** (1) Characteristic. For example, specifying parameters means defining the characteristics of something. In general, parameters are used to customize a program. For example, filenames, page lengths, and font specifications could all be considered parameters.(2) In programming, the term parameter is synonymous with argument, a value that is passed to a routine.
Local

**UTC:** Coordinated Universal Time is a time scale that couples Greenwich Mean Time, which is based solely on the Earth's inconsistent rotation rate, with highly accurate atomic time. When atomic time and Earth time approach a one second difference, a leap second is calculated into UTC. UTC was devised on January 1, 1972 and is coordinated in Paris by the International Bureau of Weights and Measures. UTC, like Greenwich Mean Time, is set at 0 degrees longitude on the prime meridian.

**VBScript:** Short for Visual Basic Scripting Edition, a scripting language developed by Microsoft and supported by Microsoft's Internet Explorer Web browser. VBScript is based on the Visual Basic programming language, but is much simpler. In many ways, it is similar to JavaScript. It enables Web authors to include interactive controls, such as buttons and scrollbars, on their Web pages.

# Table of Contents

# Section 1: Introducing the _time Field in NELRF

This section covers the following sub-sections:

- 1.1 Introduction.
- 1.2 Date Format.
- 1.3 Entry Points.
- 1.4 Properties

## 1.1 Introducing the _time Field

The _time field is mandatory and contains the UTC date when an event was taken into account by a Net Report Agent. Agents are responsible for providing this information.

## 1.2 Date Format

The format of the date is as follows:

YYYY-MM-DD hh:mm:ss.nnnnnn

where

- YYYY: year.
- MM: month.
- DD: day.
- hh: hour.
- mm: minute.
- ss: second.
- nnnnnn: microsecond.

## 1.3 Entry Points

The _time field can be accessed from different places in the Net Report Filter Engine as properties of the **Record** object.

The _time field can be accessed from the following places:

- Fields.
- Rules.
- Actions.

## 1.4 Properties

a) **Record.time**: gives the date when the event was taken into account by an agent.

**Note:** This property is an OLE date.

b) **Record.milliSeconds**: OLE dates do not include micro/milliseconds. However the following additional property enables Net Report to obtain the milliseconds:
`Record.milliSeconds`.

# Section 2: Managing Dates Provided by Devices

This section covers the following types of formats:

- 2.1 The Format Provided by the Device is Close to the Standard NELRF Format.
- 2.2 The Format Provided by the Device Corresponds to the Literal Expression of the Date in a Particular Language.
- 2.3 The Format Provided by the Device Does Not Correspond to a Date in the NELRF Format nor to a Date expressed in Any Other Language.
- 2.4 The Format Provided by the Device Does Not Include Certain Elements of the Date.
- 2.5 The Agent Only Provides the Date when the Event was Taken into Account.

## 2.1 The Format Provided by the Device is Close to the Standard NELRF Format

This is the case for logs in W3C format, which are obtained from Internet Information Server (IIS) devices. In this case, a function which is specialized in the conversion from the literal form of a date in NELRF format to an OLE date is available: NelrfValueToVariantDate().

In the fields in an IIS Filter, it is used for the "TimeRecord" field:

```
NelrfValueToVariantDate(Record("date")&" "&Record("time"))
```

- An example of a date in a W3C log:

```
2004-01-01 02:09:43
```

With this example, you should get

```
Record("date") = "2004-01-01"
Record("time") = "02:09:43"
```

So

```
NelrfValueToVariantDate(Record("date")&" "&Record("time"))
```

Is

```
NelrfValueToVariantDate("2004-01-01"&" "& "02:09:43")
```

## 2.2 The Format Provided by the Device Coresponds to the Literal Expression of the Date in a Particular Language

This is the case for Flat Files such as Apache Flat Files. The format for the date is in the English written form. In this case, a function exists which enables Net Report to convert the literal form of the date to a date type value according to the country in question:

```
g_NRScriptHlp.DateConv()
```

Which would give the following for the "TimeRecord" field:

```
g_NRScriptHlp.DateConv(Record("date") & " " & Record("time"),"en-gb")
```

For the second parameter ("en-gb" in this example), please see Net Report's documentation concerning the different values possible:
http://www.netreport.fr/knowledgebase/UserHelp/11_Reference_Material/04_Net_Report_Local_IDs/00_Introducing_Locale_IDs.htm

- An example of a date in an Apache log:

```
13/Jun/2003:23:24:41
```

With this example, you should get

```
Record("date") = "13/Jun/2003"
Record("time") = "23:24:41"
```

So

```
g_NRScriptHlp.DateConv(Record("date") & " " & Record("time"),"en-gb")
```

is

```
g_NRScriptHlp.DateConv("13/Jun/2003"& " " & "23:24:41","en-gb")
```

## 2.3 The Format Provided by the Device Does Not Correspond to a Date in the NELRF Format nor to a Date expressed in Any Other Language.

In this case, there are two possibilities:

- Produce a string that is similar to a date in the NELRF format.
- Produce a string that is similar to a format corresponding to an other language, and use the appropriate function (`NelrfValueToVariantDate or g_NRScriptHlp.DateConv`).

In the Check Point (Flat File) Filter, for example, the literal form of the date in the English/US format is rebuilt from the elements available, and used as the first parameter in the `DateConv` function:

```
g_NRScriptHlp.DateConv(Record("day")&" "&Record("month")&" "&Record("year")&"
"&record("time"),"en-us")
```

- An example of a date in a CheckPoint log:

```
"30Apr2004"  "21:17:56"
```

With this example, you should get

```
Record("day") = "30"
Record("month") = "Apr"
Record("year") = "2004"

Record("time") = "21:17:56"
```

So

```
g_NRScriptHlp.DateConv(Record("day")&" "&Record("month")&" "&Record("year")&"
"&record("time"),"en-us")
```

Is

```
g_NRScriptHlp.DateConv("30"&" "&"Apr"&" "&"2004"&" "21:17:56","en-us")
```

## 2.4 The Format Provided by the Device Does Not Include Certain Elements of the Date.

For devices such as Snort, certain elements are not provided by the log (for example, the year). In this case, Net Report uses either the current year or the previous year in the filters to form the literal form of a date, which gives the following for the Snort filter's Time field:

```
iff(g_NRScriptHlp.DateConv(Record("month")&"/"&Record("day")&"/"&year(now)&"
"&Record("time"),"en-
us")>now,g_NRScriptHlp.DateConv(Record("month")&"/"&Record("day")&"/"&year(now)-
1&" "&Record("time"),"en-
us"),g_NRScriptHlp.DateConv(Record("month")&"/"&Record("day")&"/"&year(now)&"
"&Record("time"),"en-us"))
```

- An example of a date in a Snort log:

```
May 13 02:49:27
```

In this case, Net Report performs the following activities:
Net Report obtains the Record `("month")` Field = May
Net Report obtains the Record (`"day"`) Field = 13
Net Report adds the current year (for example 2005), then if the date obtained is after the current date then Net Report replaces the current year by [current year -1] (for example 2005 – 1 = 2004).

For example, using the Snort log example above:

- If the current date is May 1, 2005, then Net Report will generate the following date for the log (2005 -1):
13 May 2004

- If the current date is June 1, then Net Report will generate the following date for the log (2005):
13 May 2005

### 2.5 The Agent Only Provides the Date when the Event was Taken into Account.

In this case, the date taken into account by the agent for each event (Record.time) is used as the time reference.

# Section 3 : Modifying Dates

## 3.1 Adding years,months,days, hours….

It is possible to rework a date's value by using a VBScript function (for example, add/remove hours).

For example: to add nine hours to a date:

```
DateAdd("h",9,CDate("01 01 1970 05:00:00")
```

For more information, please see:
**http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/f0ff19c4-0a74-44ca-867f-4739a814a88d.asp**

## 3.2 Convert Unix Time format to normal time format

Unix time is used by a small amount of devices ( like Squid) and can be converted to the standard time format. The value provided by Unix time format returns the number of seconds that have passed since midnight, 1st January 1970 GMT (or 7pm, 31st December 1969 EST).To get our time format, add this value of seconds to the January 1st 1970.
To create the date, use the previous command:

DateAdd("s",Record("time"),CDate("01 01 1970"))

- An example of a date in a Squid log:

```
Ex : 1110801174.183
Record(“time”) = “1110801174.183”
```

So

```
DateAdd("s",Record("time"),CDate("01 01 1970"))
```

Is

```
DateAdd("s",Record("1110801174.183"),CDate("01 01 1970"))
```

# Section 4: Introducing the Locale Default Program Language

## 4.1 Introducing Locale

**Locale** defines the set of information that corresponds to a given language and country. The code locale setting affects the language of terms such as keywords and defines locale-specific settings such as the decimal and list separators, date formats, and character sorting order.

The system locale setting affects the way locale-aware functionality behaves, for example, when you display numbers or convert strings to dates. You set the system locale using the Control Panel utilities provided by the operating system.

Although the code locale and system locale are generally set to the same setting, they may differ in some situations. For example, in Visual Basic, Standard Edition and Visual Basic, Professional Edition, the code is not translated from English-U.S. The system locale can be set to the user's language and country, but the code locale is always set to English-U.S. and can't be changed. In this case, the English-U.S. separators, format placeholders, and sorting order are used.

## 4.1 Net Report's Definition of Locale

Locale, here defines the default language of a program, which has an effect on the literal representation of the dates and numbers. Please note the following examples.

**Implicit conversions:** from a number or a date to a string and vice-versa.
**Explicit conversions:** using functions which use the default locale:

- some functions have no parameter to specify a locale
- some functions use the default locale if a value for the locale parameter has not been specified.

Net Report defines the locale by "en-us" (English US) and assumes that no other action or initialization modifies the latter.

**Note:** The VBScript `SetLocale()` function must never be used.

For an example of possible side effects, please test the following script:

```
SetLocale("en-us")
MsgBox Month(CDate("03 09 1970 05:00:00")) 'sends 3
SetLocale("fr-fr")
MsgBox Month(CDate("03 09 1970 05:00:00")) 'sends 9
WSCRIPT.QUIT
```