

NetAnalysis v2.11



- [Introduction](#)
- [New Browser Support](#)
 - [Avast Secure Browser](#)
 - [CCleaner Browser](#)
- [New Features](#)
 - [Apple Safari](#)
- [Improvements](#)
 - [Property Set Information](#)
 - [Filter Functions](#)
- [Change Log](#)

Introduction

This release of NetAnalysis® adds support for two browsers which have been designed for the security/privacy market, Avast Secure Browser and CCleaner Browser. We have also added support for seventy-four new versions of other browsers.

New Browser Support

We have added support for the following browsers:

Avast Secure Browser



Avast Secure Browser (previously Avast Safe-Zone) is a Chromium based web browser developed by Avast. Initially, the browser was available alongside Avast's paid versions of their Avast Antivirus software. However, as of March 2016, the company included the web browser as part of its free antivirus software.

CCleaner Browser



CCleaner Browser is a Chromium based web browser developed by Piriform, the same company responsible for the data erasing, security software, CCleaner. The company describes the software as *"a web browser with built-in security and privacy features to keep you safe online. It comes packed with all the tools you need to manage your online privacy, identity, and personal data."*

New Features

Apple Safari

We have added support for auto-fill corrections, touch icon cache settings, per-site preferences and favicons.

Improvements

Property Set Information

Microsoft Internet Explorer and Edge (non-Chromium) browsers maintain files for recovering sessions and tracking browser navigation between tabs. NetAnalysis® shows this data when viewing Recovery Store, Tab Session, Roaming Tab Session and Travel Log entries. Some of the data for these types is stored in a data structure called a Property Set. This is simply a collection of properties, along with a FMTID (Format Identifier) to identify the property set format.

In previous version of NetAnalysis®, we only displayed a summary of the known properties in the Information panel. This has now been updated so we show all property IDs along with the raw values, as well as the CLSID for the Format Identifier. Some examples are shown below.

The following images show the Information panels from Recovery Store entries. The raw Property Set values are below the FMTID.

```
Information
1 Recovery Store ID: b15f4845-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
2 Created [UTC]: 2017-04-27 08:51:24.265
3 Modified [UTC]: 2017-04-27 08:54:30.008
4
5 Tab Sessions: (Count = 8)
6 Stream Name: O_TSRkHfSyr5xGhJwAwG0hXiW== ID: b15f4847-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
7 Stream Name: O_TSRkHfSyr5xGhJwAwG0hXiW== ID: df96d884-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:52:41.804]
8 Stream Name: O_TSRkHfSyr5xGhJwAwG0hXiW== ID: f0616cee-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:53:09.975]
9 Stream Name: O_TSRkHfSyr5xGhJwAwG0hXiW== ID: fd5fbf27-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:53:31.775]
10 Stream Name: ClosedTabList ID: b15f4849-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
11 Stream Name: ClosedTabList ID: b15f4848-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
12 Stream Name: ClosedTabList ID: c06400ba-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:49.462]
13 Stream Name: ClosedTabList ID: f0616cef-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:53:09.975]
14
15 Properties
16 Operating System: 10.0 [Microsoft Windows 10]
17 Locale ID: 2057 [en-GB English (United Kingdom)]
18 Version: 9
19
20 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
21 ID: 2 [0x02] VT_UI4 Value: 9
22 ID: 3 [0x03] VT_CLSID Value: b15f4845-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
23 ID: 7 [0x07] VT_CLSID Value: b15f4844-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
```

```
Information
1 Recovery Store ID : 21e7dddc-33b4-4f97-98ba-c98d3dfc1064
2 Created [UTC]: 2020-01-16 08:09:57.148
3 Modified [UTC]: 2020-01-16 08:12:06.516
4
5 Tab Sessions: (Count = 1)
6 Stream Name: O_TSegGnGtLLlUiXID0ezFitFyg== ID: 0eabebad-a354-447b-a0c9-f531d9bbfc3c
7
8 Properties
9 Operating System: 10.0 [Microsoft Windows 10]
10 Locale ID: 2057 [en-GB English (United Kingdom)]
11 Version: 19
12
13 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
14 ID: 2 [0x02] VT_UI4 Value: 19
15 ID: 3 [0x03] VT_CLSID Value: 21e7dddc-33b4-4f97-98ba-c98d3dfc1064
16 ID: 7 [0x07] VT_CLSID Value: 958ae36b-3837-11ea-b397-fcaa14290f80 [Date [UTC]: 2020-01-16 08:09:57.148]
17 ID: 11 [0x0B] VT_BOOL Value: True
18 ID: 12 [0x0C] VT_BOOL Value: True
```

```

Information
1 Recovery Store ID: 16cf0cbe-98d9-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 09:43:06.266]
2 Created [UTC]: 2015-12-02 09:39:02.172
3 Modified [UTC]: 2015-12-04 17:31:27.787
4
5 Tab Sessions: (Count = 28)
6 Stream Name: O_TsiktRhdIY5RGcd#tyqFAY+cw== ID: 81498986-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
7 Stream Name: O_TsiktRhdIY5RGcd#tyqFAY+cw== ID: 81498987-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
8 Stream Name: O_TsiktRhdIY5RGcd#tyqFAY+cw== ID: 81498988-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
9 Stream Name: O_TsiktRhdIY5RGcd#tyqFAY+cw== ID: 81498989-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
10 Stream Name: O_TsiktRhdIY5RGcd#tyqFAY+cw== ID: 8149898a-98db-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:00:23.900]
11 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad11c-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
12 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad11d-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
13 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad11e-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
14 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad11f-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
15 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad120-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
16 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad121-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
17 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad122-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
18 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad123-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
19 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad124-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
20 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad125-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
21 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad126-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
22 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad127-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
23 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad128-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
24 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad129-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
25 Stream Name: O_TStdUsr9uY5RGcd#tyqFAY+cw== ID: d0aad12a-98dd-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:16:56.071]
26 Stream Name: O_TSu3+k+t2Y5RGcd#tyqFAY+cw== ID: 8149cc81-98de-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:21:52.392]
27 Stream Name: O_TSVUp2k96Y5RGcd#tyqFAY+cw== ID: 4e7a9bcd-98e0-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:34:46.142]
28 Stream Name: O_TSVUp2k96Y5RGcd#tyqFAY+cw== ID: 4e7a9bce-98e0-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:34:46.142]
29 Stream Name: O_TSNej2Vm6a5RGcd#tyqFAY+cw== ID: 78d1fa96-9aa6-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 10:04:56.877]
30 Stream Name: O_TSVHzByqKa5RGcd#tyqFAY+cw== ID: 577538eb-9aa4-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 16:30:33.728]
31 Stream Name: O_TSVHzByqKa5RGcd#tyqFAY+cw== ID: 577538ec-9aa4-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 16:30:33.728]
32 Stream Name: O_TSVHzByqKa5RGcd#tyqFAY+cw== ID: 577538ed-9aa4-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 16:30:33.728]
33 Stream Name: O_TStqQE2aqa5RGcd#tyqFAY+cw== ID: ea44a478-9aaa-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 17:17:37.015]
34
35 Properties
36 Operating System: 6.3 [Microsoft Windows 8.1]
37 Locale ID: 2057 [en-GB English (United Kingdom)]
38 Version: 9
39
40 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
41 ID: 2 [0x02] VT_UI4 Value: 9
42 ID: 3 [0x03] VT_CLSID Value: 16cf0cbe-98d9-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 09:43:06.266]
43 ID: 7 [0x07] VT_CLSID Value: 85514b88-98d8-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 09:39:02.172]

```

The following images show the Information panels from Tab Session entries. The raw Property Set values are below the FMTID.

```

Information
1 Tab Session ID: b15f4847-2b26-11e7-bf8f-00301b48578b [Date [UTC]: 2017-04-27 08:51:24.265]
2 Session State: Ordered
3 Modified [UTC]: 2017-04-27 08:53:44.751
4
5 Parent Name: RecoveryStore.{B15F4845-2B26-11E7-BF8F-00301B48578B}
6 Stream Name: O_TSRkhsfSYr5xG#jwAwG0hXiW==
7
8 Travel Logs: (Count = 6)
9 Stream Name: TL1
10 Stream Name: TL2
11 Stream Name: TL3
12 Stream Name: TL4
13 Stream Name: TL5
14 Stream Name: TL6
15
16 Travel Log: 0, 1, 2, 3, 4, 5, 6 (Last Displayed: 6)
17
18 Properties
19 Operating System: 10.0 [Microsoft Windows 10]
20 Locale ID: 2057 [en-GB English (United Kingdom)]
21 Version: 9
22
23 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
24 ID: 2 [0x02] VT_UI4 Value: 9
25 ID: 4 [0x04] VT_UI4 Value: 6
26 ID: 6 [0x06] VT_FILETIME Value: 2017-04-27 08:52:47.833 [UTC]
27 ID: 7 [0x07] VT_I4 Value: 0
28 ID: 9 [0x09] VT_UI4 Value: 1
29 ID: 10 [0x0A] VT_FILETIME Value: 2017-04-27 08:53:11.955 [UTC]
30 ID: 13 [0x0D] VT_UI4 Value: 1
31 ID: 14 [0x0E] VT_UI4 Value: 0
32 ID: 17 [0x11] VT_UI4 Value: 0

```

```
Information
1 Tab Session ID: 22a7ff1e-cc86-11e2-bee6-00301b46bd20 [Date [UTC]: 2013-06-03 19:45:25.365]
2 Session State: Ordered
3 Modified [UTC]: 2013-06-03 19:45:26.381
4
5 Parent Name: RecoveryStore.{22a7ff1d-cc86-11e2-bee6-00301b46bd20}
6 Stream Name: ORDERED_TS0
7
8 Travel Logs: (Count = 1)
9 Stream Name: TL2
10
11 Travel Log: 0, 1, 2 (Last Displayed: 2)
12
13 Properties
14 Operating System: 6.2 [Microsoft Windows 8]
15 Locale ID: 2057 [en-GB English (United Kingdom)]
16 Version: 6
17
18 FMTID: 0b00252a-8d48-4d0b-b3a9-7b79887f2b96
19 ID: 2 [0x02] VT_UI4 Value: 6
20 ID: 4 [0x04] VT_UI4 Value: 2
21 ID: 6 [0x06] VT_FILETIME Value: 2013-06-03 18:44:54.749 [UTC]
22 ID: 7 [0x07] VT_I4 Value: 0
23 ID: 9 [0x09] VT_UI4 Value: 4
24 ID: 10 [0x0A] VT_FILETIME Value: 2013-06-03 18:44:57.452 [UTC]
25 ID: 13 [0x0D] VT_UI4 Value: 1
```

The following images show the Information panels from Tab Roaming entries. The raw Property Set values are below the FMTID.

```
Information
1 Tab Session ID: 79a678b2-98dc-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-02 10:07:20.584]
2 Session State: Roaming
3 Modified [UTC]: 2015-12-04 17:21:17.348
4
5 Parent Name: <none>
6
7 Travel Logs: (Count = 1)
8 Stream Name: TL3
9
10 Travel Log: 3 (Last Displayed: 3)
11
12 Properties
13 Operating System: 6.3 [Microsoft Windows 8.1]
14 Locale ID: 2057 [en-GB English (United Kingdom)]
15 Version: 9
16
17 Tab Roaming Machine Information v2
18 Source: \\digital02\IE TravelLog\Travel Logs\Internet Explorer v11 (9600) TravelLog\2016_01_08_15_03_32_272\Local\Microsoft\Internet
Explorer\TabRoaming\{D8501CB7-A638-43FC-8384-869E5E2CD0A8}\MachineInfo.dat
19 Machine Name: RECOVERY1
20 Operating System: 6.3 [Microsoft Windows 8.1]
21 Locale ID: 2057 [en-GB English (United Kingdom)]
22
23 Modified [UTC]: 2015-12-04 17:21:17.348
24 Timestamp [UTC]: 2015-12-04 10:04:00.965
25
26 FMTID: 8d06be37-1a1a-4762-9d01-33fdf4881f84
27 ID: 2 [0x02] VT_UI4 Value: 9
28 ID: 4 [0x04] VT_UI4 Value: 3
29 ID: 9 [0x09] VT_UI4 Value: 0
30 ID: 10 [0x0A] VT_FILETIME Value: 2015-12-04 17:20:57.785 [UTC]
31 ID: 14 [0x0E] VT_UI4 Value: 0
32 ID: 1000 [0x3E8] VT_UI4 Value: 2
33 ID: 1001 [0x3E9] VT_LPWSTR Value: {79A678B2-98DC-11E5-8277-FCAA14063E73}
34 ID: 1002 [0x3EA] VT_LPWSTR Value: http://www.neowin.net/images/orion/icons/favicon-196x196.png
```

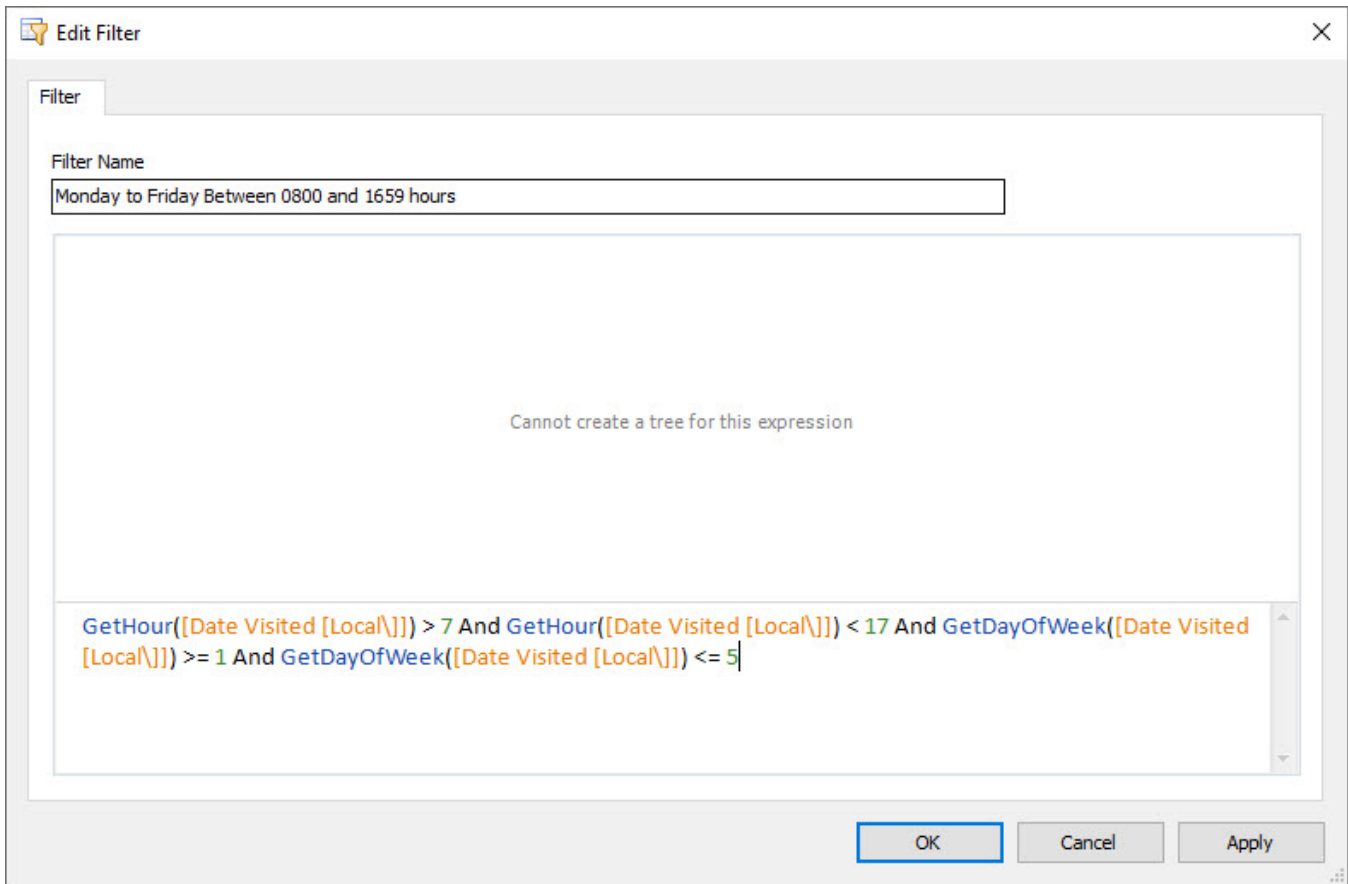
```
Information
1 Tab Session ID: 666504d7-9aab-11e5-8277-fcaa14063e73 [Date [UTC]: 2015-12-04 17:21:05.264]
2 Session State: Roaming
3 Modified [UTC]: 2015-12-04 17:21:58.210
4
5 Parent Name: <none>
6
7 Travel Logs: (Count = 5)
8 Stream Name: TL0
9 Stream Name: TL1
10 Stream Name: TL2
11 Stream Name: TL3
12 Stream Name: TL4
13
14 Travel Log: 0, 1, 2, 3, 4 (Last Displayed: 4)
15
16 Properties
17 Operating System: 6.3 [Microsoft Windows 8.1]
18 Locale ID: 2057 [en-GB English (United Kingdom)]
19 Version: 9
20
21 Tab Roaming Machine Information v2
22 Source: \\digital02\IE TravelLog\Travel Logs\Internet Explorer v11 (9600) TravelLog\2016_01_08_15_03_32_272\Local\Microsoft\Internet
Explorer\TabRoaming\{D8501CB7-A63B-43FC-83B4-869E5E2CD0A8}\MachineInfo.dat
23 Machine Name: RECOVERY1
24 Operating System: 6.3 [Microsoft Windows 8.1]
25 Locale ID: 2057 [en-GB English (United Kingdom)]
26
27 Modified [UTC]: 2015-12-04 17:21:58.210
28 Timestamp [UTC]: 2015-12-04 10:04:00.965
29
30 FMTID: 8d06be37-1a1a-4762-9d01-33fdf4881f84
31 ID: 2 [0x02] VT_UI4 Value: 9
32 ID: 4 [0x04] VT_UI4 Value: 4
33 ID: 9 [0x09] VT_UI4 Value: 0
34 ID: 10 [0x0A] VT_FILETIME Value: 2015-12-04 17:21:13.456 [UTC]
35 ID: 14 [0x0E] VT_UI4 Value: 0
36 ID: 1000 [0x3E8] VT_UI4 Value: 2
37 ID: 1001 [0x3E9] VT_LPWSTR Value: {666504D7-9AAB-11E5-8277-FCAA14063E73}
38 ID: 1002 [0x3EA] VT_LPWSTR Value: http://static-news-neu.s-msn.com/sc/d7/97297b.ico
```

Filter Functions

A common scenario is to examine the records between specific days of the week and between specific times. In NetAnalysis® v2.11 we have added some new Filter files which demonstrates this.

The first example is a filter which will only show entries where the Date Visited falls between Monday and Friday, and the local time is between 08:00 and 16:59 hours. As this filter uses the Function facility, it will not be able to display the results in the expression tree.

This Filter uses the GetHour() and GetDayOfWeek() functions. The GetDayOfWeek() function returns an integer which corresponds to the day of the week. Monday = 1, Tuesday = 2 and so on. The GetHour() function also returns an integer which represents the hour in the 24-hour clock.



Change Log

To review the full list of changes for this release, please see: [Change Log v2.11](#).