Rules Wizard (RWZ) File Format Business Case

Table of Contents

Revision Summary

Date	Comments
15/05/21	Added section on old security vulnerabilities in the RWZ format Added symbol files as a documentation open Fixed typos
09/05/21	Initial Release

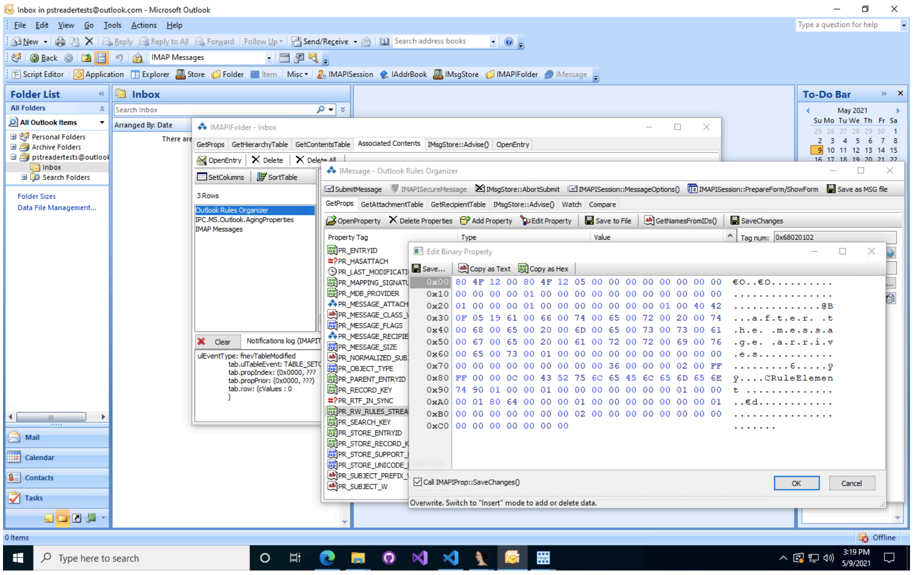
1. Preamble

An Outlook Rule is a set of actions that Outlook performs automatically when certain conditions are met. For example, you can use rules to move, flag, and respond to email messages automatically. You can also use rules to play sounds, move messages to folders, or display new item alerts.[1]

Outlook Rules began as an add-in to Outlook 97[2] called *RulesWiz.dll* and were integrated in-box automatically in Outlook 98[3].

Outlook stores Rules Wizard Files differently depending on the version of Outlook.[4]

- Outlook 2000 and earlier: user-created rules and alerts are stored in their own file ending in .rwz, located in *C:\Documents and Settings\username\Application Data\Microsoft\Outlook*
- Outlook 2002 and later: user-created rules and alerts are stored in the *PR_RW_RULES_STREAM/PidTagRwRulesStream (0x68020102)*[5] property of a message named *Outlook Rules Organizer* of class *IPM.RuleOrganizer* inside the *Associated Contents Table*[6] of the *Inbox* folder


Inbox in pstreadertests@outlook.com - Microsoft Outlook
Folder List
Inbox
To-Do Bar
IMAPIFolder - Inbox
Outlook Rules Organizer
IPC.MS.Outlook.AgingProperties
IMAP Messages
IMessage - Outlook Rules Organizer
Edit Binary Property
Tag num: 0x68020102
PR_RW_RULES_STREAM
Copy as Text
Copy as Hex
Call IMAPIProp::SaveChanges()
OK
Cancel
Overwrite. Switch to "Insert" mode to add or delete data.

```
0x00  80 4F 12 00 80 4F 12 05 00 00 00 00 00 00 00 00   €O..€O..........
0x10  00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00   ................
0x20  01 00 00 00 01 00 00 00 00 00 00 00 01 00 40 42   ..............@B
0x30  0F 05 19 61 00 66 00 74 00 65 00 72 00 20 00 74   ...a.f.t.e.r. .t
0x40  00 68 00 65 00 20 00 6D 00 65 00 73 00 73 00 61   .h.e. .m.e.s.s.a
0x50  00 67 00 65 00 20 00 61 00 72 00 72 00 69 00 76   .g.e. .a.r.r.i.v
0x60  00 65 00 73 00 01 00 00 00 00 00 00 00 00 00 00   .e.s............
0x70  00 00 00 00 00 00 00 00 00 36 00 00 00 02 00 FF   .........6.....ÿ
0x80  FF 00 00 0C 00 43 52 75 6C 65 45 6C 65 6D 65 6E   ÿ....CRuleElemen
0x90  74 90 01 00 00 01 00 00 00 00 00 00 00 01 00 00   t ..............
0xA0  00 01 80 64 00 00 00 01 00 00 00 00 00 00 00 01   ..€d............
0xB0  00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00   ................
0xC0  00 00 00 00 00 00 00                              .......
```

Outlook allows users to import and export Rules to a rules file with the file extension .rwz[7]. The resulting file is known as a Rules Wizard File (shorted to RWZ file). Users can specify backwards compatibility to the latest version of Outlook, Outlook 2002, Outlook 2000 and Outlook 98.

[1] https://support.microsoft.com/en-us/office/manage-email-messages-by-using-rules-c24f5dea-9465-4df4-ad17-a50704d66c59

[2] https://www.computerhope.com/download/updates.htm

[3] https://www.slipstick.com/outlook/rules/rules-wizard/

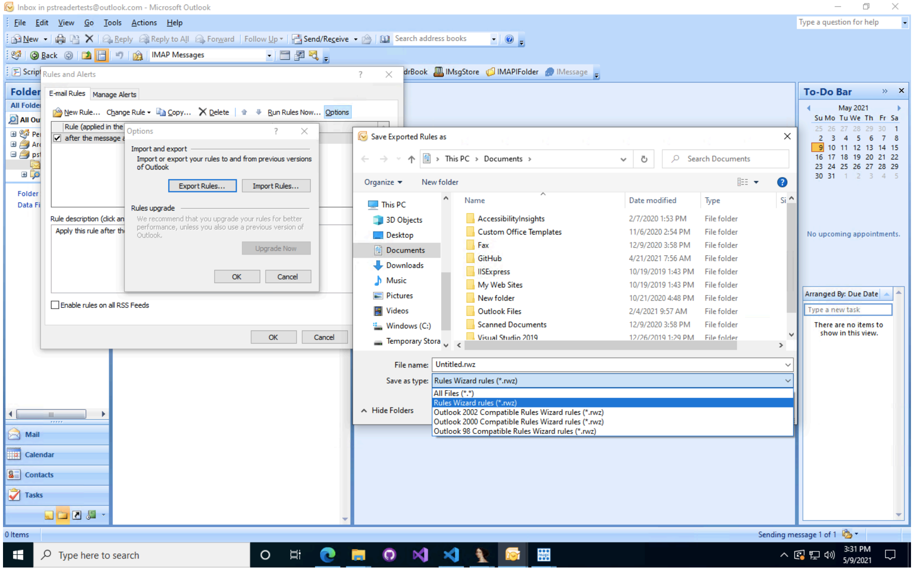
[4] https://www.itprotoday.com/email-and-calendaring/how-do-you-delete-and-recreate-corrupt-outlook-rules

[5] https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxprops/f1fbd19a-9b2c-4c16-a07b-2242b2c0dece

[6] https://docs.microsoft.com/en-us/office/client-developer/outlook/mapi/contents-tables

[7] https://support.microsoft.com/en-us/office/import-or-export-a-set-of-rules-f54b5bd2-40e0-426e-9f25-e51fa14eeb95

The format of *.rwz* files and the corresponding *PR_RW_RULES_STREAM* property is client-specific and opaque to the server[8]. Some values within the header are, for example different between the stream contained in PidTagRwRulesStream and the corresponding RWZ exported files. However, this document refers to RWZ files and the binary value of the PidTagRwRulesStream property interchangeably as, by-and-large, they have the same format.


Inbox in pstreadertests@outlook.com - Microsoft Outlook

Options

Import and export

Import or export your rules to and from previous versions of Outlook

Rules upgrade

We recommend that you upgrade your rules for better performance, unless you also use a previous version of Outlook.

☑ after the message a

Apply this rule after th

□ Enable rules on all RSS Feeds

Save Exported Rules as

Name	Date modified	Type
AccessibilityInsights	2/7/2020 1:53 PM	File folder
Custom Office Templates	11/6/2020 2:54 PM	File folder
Fax	12/9/2020 3:58 PM	File folder
GitHub	4/21/2021 7:56 AM	File folder
IISExpress	10/19/2019 1:43 PM	File folder
My Web Sites	10/19/2019 1:43 PM	File folder
New folder	10/21/2020 4:48 PM	File folder
Outlook Files	2/4/2021 9:57 AM	File folder
Scanned Documents	12/9/2020 3:58 PM	File folder
Visual Studio 2019	12/26/2019 1:29 PM	File folder

File name: Untitled.rwz

Save as type: Rules Wizard rules (*.rwz)

All Files (*.*)
Rules Wizard rules (*.rwz)
Outlook 2002 Compatible Rules Wizard rules (*.rwz)
Outlook 2000 Compatible Rules Wizard rules (*.rwz)
Outlook 98 Compatible Rules Wizard rules (*.rwz)

There have been very few attempts to reverse engineer and document the RWZ file format and the documentation remains incomplete

- Kopano[9], an open-source groupware application, contains a draft but incomplete specification of the file format[10], but does not include an implementation
- OutlookRulesReader[11], an open-source Swift library, contains a draft but incomplete specification of the file format[12], and includes an implementation/API for reading and writing RWZ files

This document describes a business case for documenting the opaque RWZ file format. This document also describes the means by which the file format can be documented. Sources for this business case include online research and discussions/interviews with key stakeholders, including pro-users, MAPI experts and MVPs such as Dmitry Streblechenko (founder of Outlook Spy[13]) and Stephen Griffin (founder of MFCMAPI[14]) and forensics companies such as legal e-discovery firm GoldFynch[15].

For any questions, email hughbellars@gmail.com.

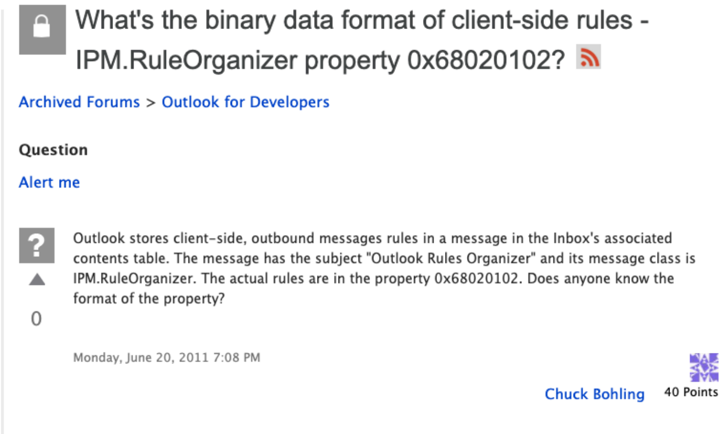
[8] https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxorule/ee0fd52b-1161-49b8-adab-6b8c2e31c3f3
[9] https://github.com/Kopano-dev/kopano-core
[10] https://github.com/Kopano-dev/kopano-core/blob/master/doc/ol_rule_spec.txt
[11] https://github.com/hughbe/OutlookRulesReader
[12] https://github.com/hughbe/OutlookRulesReader/blob/master/docs/RWZ%20Format.pdf
[13] https://www.dimastr.com/outspy/home.htm
[14] https://github.com/stephenegriffin/mfcmapi
[15] https://goldfynch.com/

2. Business Case

2.1. Users want to know the format of RWZ files

Before detailing more real-world applications of the file format, there is clear interest from online discussions and conversations that users want to decipher this file format.

E.g. https://social.msdn.microsoft.com/Forums/office/en-US/d1cbdc2e-b63d-4fe6-b062-d6ceb16b2abd/whats-the-binary-data-format-of-clientside-rules-ipmruleorganizer-property-0x68020102



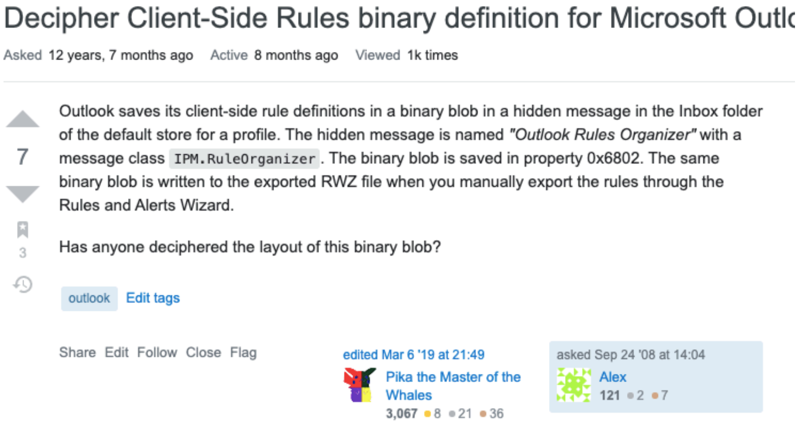
What's the binary data format of client-side rules - IPM.RuleOrganizer property 0x68020102?

Outlook stores client-side, outbound messages rules in a message in the Inbox's associated contents table. The message has the subject "Outlook Rules Organizer" and its message class is IPM.RuleOrganizer. The actual rules are in the property 0x68020102. Does anyone know the format of the property?

Monday, June 20, 2011 7:08 PM

Chuck Bohling 40 Points

E.g. https://stackoverflow.com/questions/127336/decipher-client-side-rules-binary-definition-for-microsoft-outlook



Decipher Client-Side Rules binary definition for Microsoft Outlc

Asked 12 years, 7 months ago Active 8 months ago Viewed 1k times

Outlook saves its client-side rule definitions in a binary blob in a hidden message in the Inbox folder of the default store for a profile. The hidden message is named *"Outlook Rules Organizer"* with a message class `IPM.RuleOrganizer`. The binary blob is saved in property 0x6802. The same binary blob is written to the exported RWZ file when you manually export the rules through the Rules and Alerts Wizard.

Has anyone deciphered the layout of this binary blob?

edited Mar 6 '19 at 21:49
Pika the Master of the Whales
3,067 ● 8 ● 21 ● 36

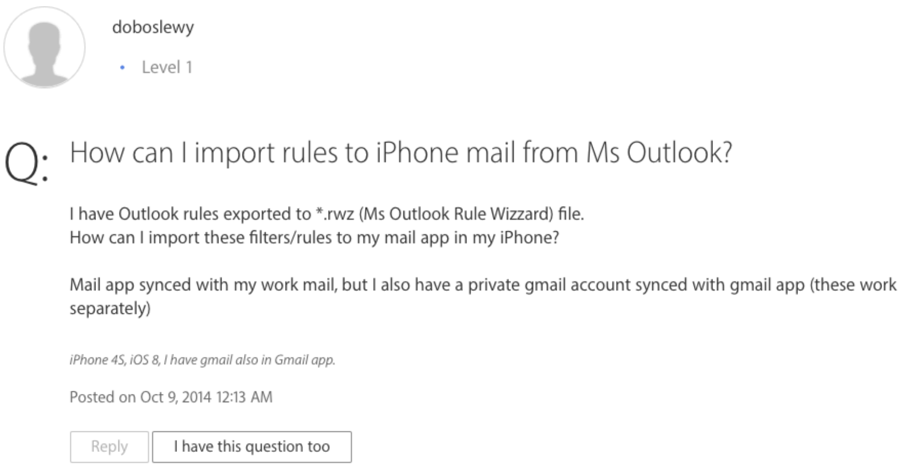
asked Sep 24 '08 at 14:04
Alex
121 ● 2 ● 7

2.2. Users want to import and export rules between applications

Documenting the RWZ file format would allow interoperability between mail applications. For example, if enabled, users could import rules from Outlook into email clients such as Gmail, iPhone mail, etc.

This is one of the reasons why open-source groupware Kopano has begun attempts to document the RWZ file format.

E.g. https://discussions.apple.com/thread/6588002



doboslewy

- Level 1

Q: How can I import rules to iPhone mail from Ms Outlook?

I have Outlook rules exported to *.rwz (Ms Outlook Rule Wizzard) file.
How can I import these filters/rules to my mail app in my iPhone?

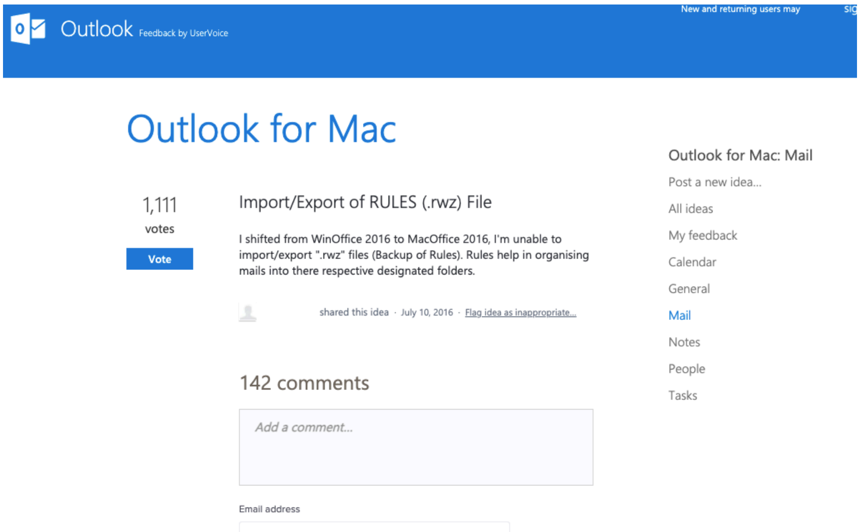
Mail app synced with my work mail, but I also have a private gmail account synced with gmail app (these work separately)

iPhone 4S, iOS 8, I have gmail also in Gmail app.

Posted on Oct 9, 2014 12:13 AM

Benefits are not just limited to interoperability between Outlook and other non-Microsoft mail clients, but also between Outlook for Mac and Windows. For example, it may be possible to create an add-in for Outlook for Mac to allow importing RWZ files into Outlook for Mac and exporting from Outlook for Mac to Outlook for Windows.

E.g. https://outlook.uservoice.com/forums/293343-outlook-for-mac/suggestions/15139845-import-export-of-rules-rwz-file



Outlook for Mac

1,111 votes

Import/Export of RULES (.rwz) File

I shifted from WinOffice 2016 to MacOffice 2016, I'm unable to import/export ".rwz" files (Backup of Rules). Rules help in organising mails into there respective designated folders.

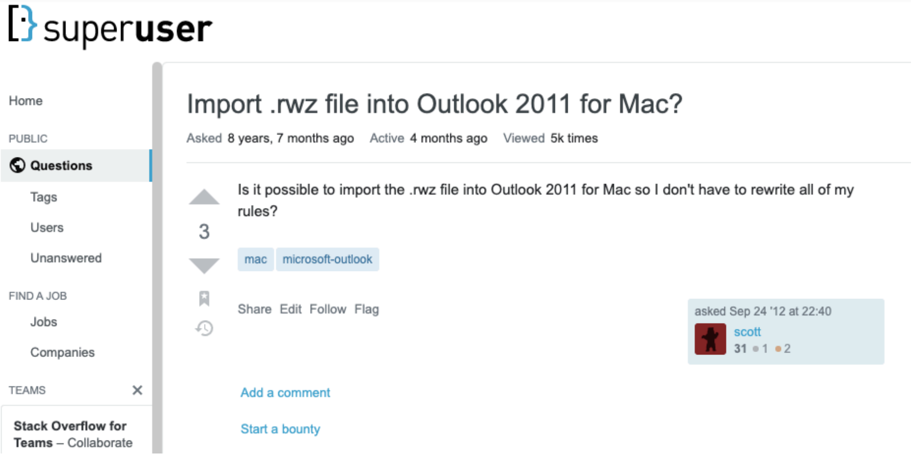
shared this idea · July 10, 2016 · Flag idea as inappropriate...

142 comments

Add a comment...

Email address

E.g. https://superuser.com/questions/479154/import-rwz-file-into-outlook-2011-for-mac



Import .rwz file into Outlook 2011 for Mac?

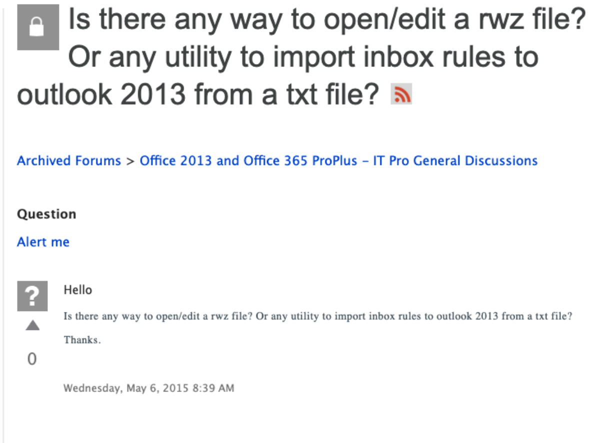
Asked 8 years, 7 months ago Active 4 months ago Viewed 5k times

3

Is it possible to import the .rwz file into Outlook 2011 for Mac so I don't have to rewrite all of my rules?

asked Sep 24 '12 at 22:40
scott
31 ● 1 ● 2

E.g. https://social.technet.microsoft.com/Forums/office/en-US/2554d185-e015-4ff1-a07d-1140bbccf200/is-there-any-way-to-openedit-a-rwz-file-or-any-utility-to-import-inbox-rules-to-outlook-2013-from?forum=officeitpro



Is there any way to open/edit a rwz file? Or any utility to import inbox rules to outlook 2013 from a txt file?

Archived Forums > Office 2013 and Office 365 ProPlus – IT Pro General Discussions

Question

Alert me

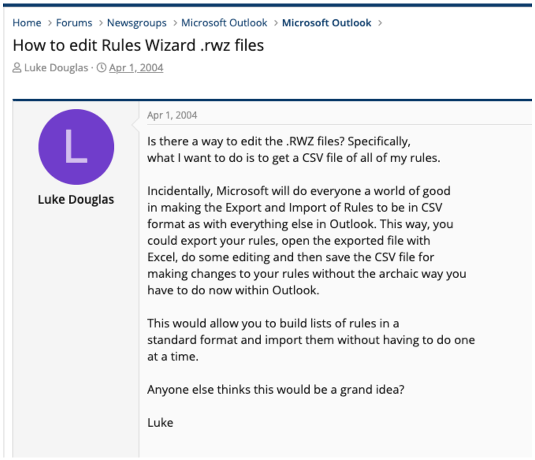
Hello

Is there any way to open/edit a rwz file? Or any utility to import inbox rules to outlook 2013 from a txt file?

Thanks.

Wednesday, May 6, 2015 8:39 AM

E.g. https://www.pcreview.co.uk/threads/how-to-edit-rules-wizard-rwz-files.775604/



Home > Forums > Newsgroups > Microsoft Outlook > Microsoft Outlook >

How to edit Rules Wizard .rwz files

Luke Douglas · Apr 1, 2004

Luke Douglas

Apr 1, 2004

Is there a way to edit the .RWZ files? Specifically, what I want to do is to get a CSV file of all of my rules.

Incidentally, Microsoft will do everyone a world of good in making the Export and Import of Rules to be in CSV format as with everything else in Outlook. This way, you could export your rules, open the exported file with Excel, do some editing and then save the CSV file for making changes to your rules without the archaic way you have to do now within Outlook.

This would allow you to build lists of rules in a standard format and import them without having to do one at a time.

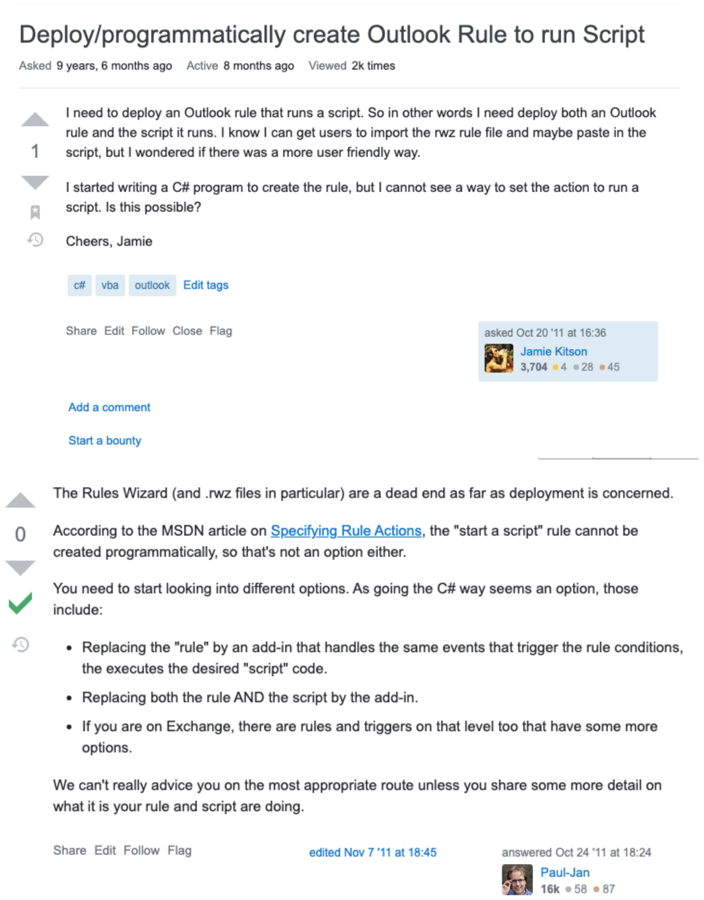
Anyone else thinks this would be a grand idea?

Luke

2.3. IT Pros want to automate and script tasks relating to rules

Documenting the RWZ file format would allow Systems Managers and IT Pros to automate tasks relating to the creation and managing of Outlook Rules. For example, pros want to create templates that can be automatically imported.

E.g. https://stackoverflow.com/questions/7839204/deploy-programmatically-create-outlook-rule-to-run-script



Deploy/programmatically create Outlook Rule to run Script

Asked 9 years, 6 months ago Active 8 months ago Viewed 2k times

I need to deploy an Outlook rule that runs a script. So in other words I need deploy both an Outlook rule and the script it runs. I know I can get users to import the rwz rule file and maybe paste in the script, but I wondered if there was a more user friendly way.

I started writing a C# program to create the rule, but I cannot see a way to set the action to run a script. Is this possible?

Cheers, Jamie

asked Oct 20 '11 at 16:36
Jamie Kitson
3,704 ●4 ●28 ●45

The Rules Wizard (and .rwz files in particular) are a dead end as far as deployment is concerned.

According to the MSDN article on Specifying Rule Actions, the "start a script" rule cannot be created programmatically, so that's not an option either.

You need to start looking into different options. As going the C# way seems an option, those include:

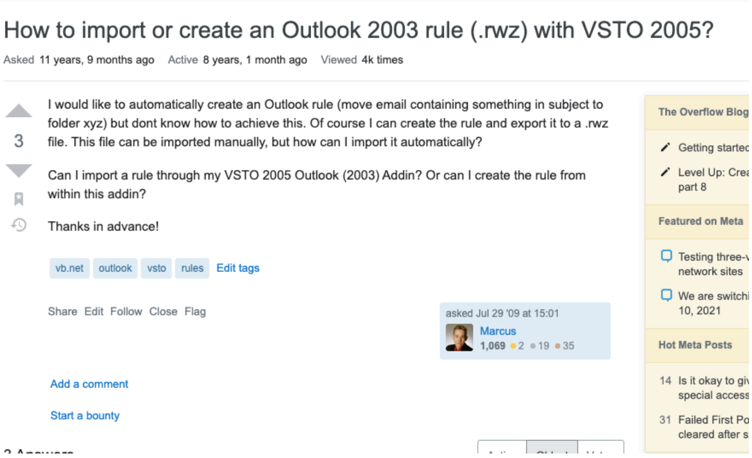
- Replacing the "rule" by an add-in that handles the same events that trigger the rule conditions, the executes the desired "script" code.
- Replacing both the rule AND the script by the add-in.
- If you are on Exchange, there are rules and triggers on that level too that have some more options.

We can't really advice you on the most appropriate route unless you share some more detail on what it is your rule and script are doing.

edited Nov 7 '11 at 18:45

answered Oct 24 '11 at 18:24
Paul-Jan
16k ●58 ●87

E.g. https://stackoverflow.com/questions/1200919/how-to-import-or-create-an-outlook-2003-rule-rwz-with-vsto-2005



How to import or create an Outlook 2003 rule (.rwz) with VSTO 2005?

Asked 11 years, 9 months ago Active 8 years, 1 month ago Viewed 4k times

I would like to automatically create an Outlook rule (move email containing something in subject to folder xyz) but dont know how to achieve this. Of course I can create the rule and export it to a .rwz file. This file can be imported manually, but how can I import it automatically?

Can I import a rule through my VSTO 2005 Outlook (2003) Addin? Or can I create the rule from within this addin?

Thanks in advance!

asked Jul 29 '09 at 15:01
Marcus
1,069 ●2 ●19 ●35

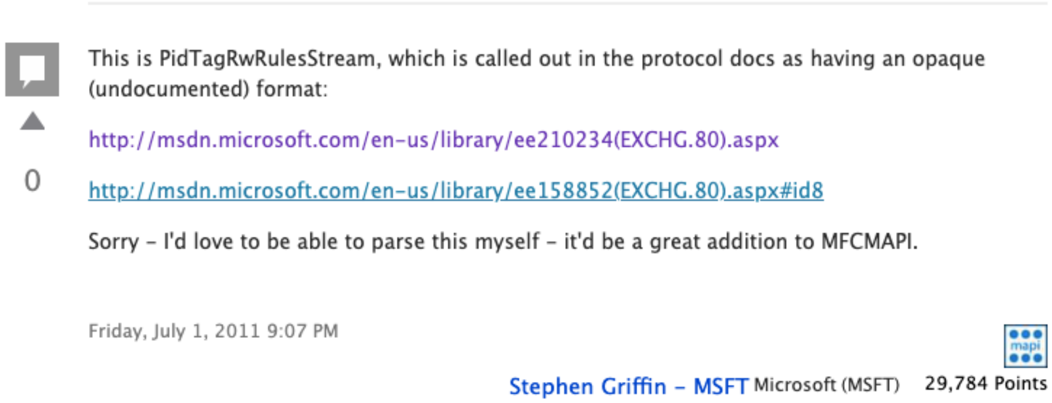
2.4. Popular Outlook tools want to use the use the RWZ format

Outlook tools such as Redemption[16], Outlook Spy[17] and MFCMAPI[18] do not have the capability to perform actions with the RWZ format.

For example, there is demand for MFCMAPI to add parsing of PidTagRwRulesStream but this is not possible until the format is documented.

[16] https://www.dimastr.com/redemption/home.htm
[17] https://www.dimastr.com/outspy/
[18] https://github.com/stephenegriffin/mfcmapi

E.g. https://github.com/stephenegriffin/mfcmapi/issues/465



0

This is PidTagRwRulesStream, which is called out in the protocol docs as having an opaque (undocumented) format:

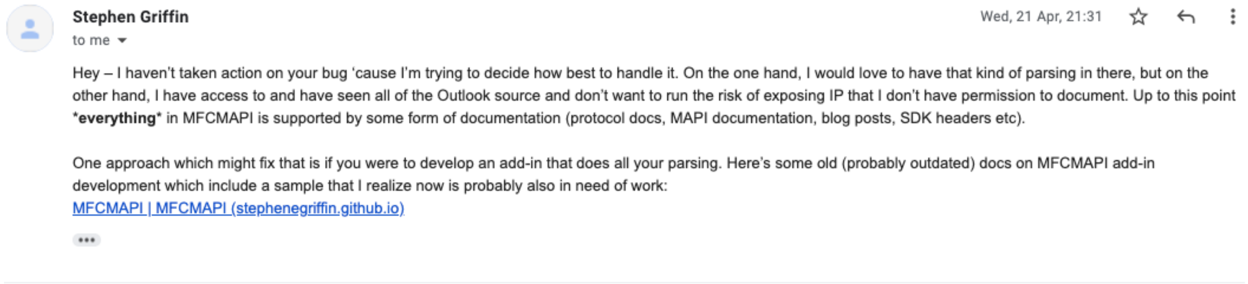
http://msdn.microsoft.com/en-us/library/ee210234(EXCHG.80).aspx

http://msdn.microsoft.com/en-us/library/ee158852(EXCHG.80).aspx#id8

Sorry - I'd love to be able to parse this myself - it'd be a great addition to MFCMAPI.

Friday, July 1, 2011 9:07 PM

Stephen Griffin - MSFT Microsoft (MSFT) 29,784 Points



Stephen Griffin
to me

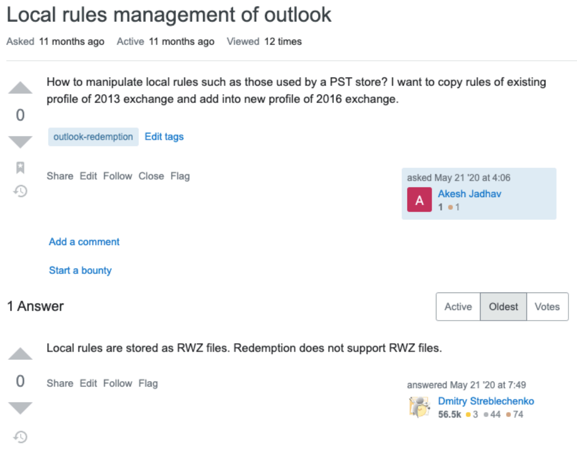
Wed, 21 Apr, 21:31

Hey – I haven't taken action on your bug 'cause I'm trying to decide how best to handle it. On the one hand, I would love to have that kind of parsing in there, but on the other hand, I have access to and have seen all of the Outlook source and don't want to run the risk of exposing IP that I don't have permission to document. Up to this point ***everything*** in MFCMAPI is supported by some form of documentation (protocol docs, MAPI documentation, blog posts, SDK headers etc).

One approach which might fix that is if you were to develop an add-in that does all your parsing. Here's some old (probably outdated) docs on MFCMAPI add-in development which include a sample that I realize now is probably also in need of work:
MFCMAPI | MFCMAPI (stephenegriffin.github.io)

For example, users cannot manage their Outlook Rules using Redemption (although this feature may be supported in Redemption in the future, given). In addition to the following example, conversations with Dmitry Streblechenko (MVP, founder of Outlook Spy and Redemption), revealed that this was a common request of Redemption.

E.g. https://stackoverflow.com/questions/61927073/local-rules-management-of-outlook



Local rules management of outlook

Asked 11 months ago Active 11 months ago Viewed 12 times

0

How to manipulate local rules such as those used by a PST store? I want to copy rules of existing profile of 2013 exchange and add into new profile of 2016 exchange.

outlook-redemption Edit tags

Share Edit Follow Close Flag

asked May 21 '20 at 4:06
Akesh Jadhav
1 •1

Add a comment

Start a bounty

1 Answer

Active Oldest Votes

0

Local rules are stored as RWZ files. Redemption does not support RWZ files.

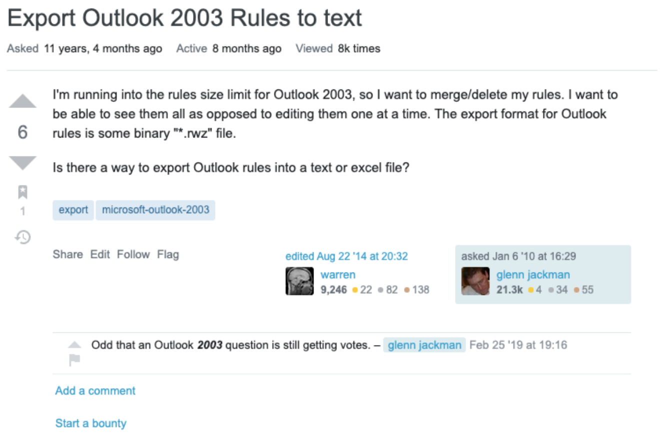
Share Edit Follow Flag

answered May 21 '20 at 7:49
Dmitry Streblechenko
56.5k •3 •44 •74

2.5. Users want to parse, edit and view rules without Outlook

Users want to be able to view Outlook rules – for example to a text format or csv format for displaying outside of Outlook (e.g. text files, excel, presentations or printed). Documenting the format will allow the development of third-party tools that can enable users to do this

E.g. https://superuser.com/questions/92197/export-outlook-2003-rules-to-text



Export Outlook 2003 Rules to text

Asked 11 years, 4 months ago Active 8 months ago Viewed 8k times

6

I'm running into the rules size limit for Outlook 2003, so I want to merge/delete my rules. I want to be able to see them all as opposed to editing them one at a time. The export format for Outlook rules is some binary "*.rwz" file.

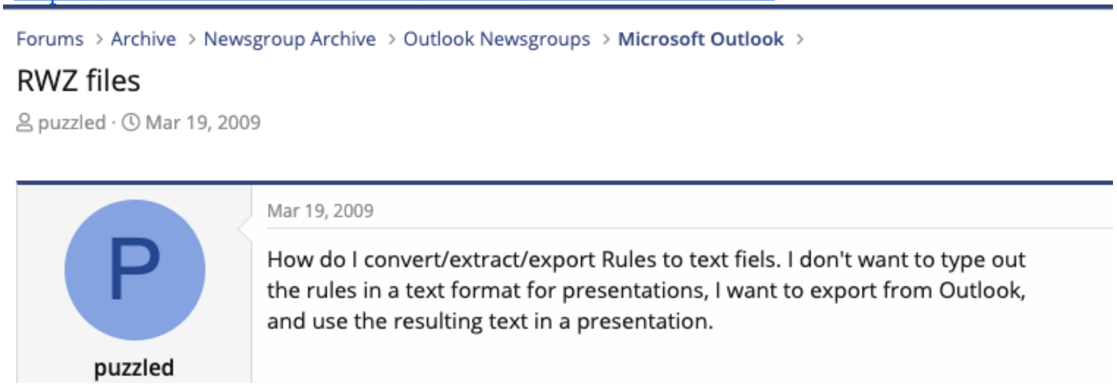
Is there a way to export Outlook rules into a text or excel file?

edited Aug 22 '14 at 20:32 warren 9,246 ●22 ●82 ●138

asked Jan 6 '10 at 16:29 glenn jackman 21.3k ●4 ●34 ●55

Odd that an Outlook ***2003*** question is still getting votes. – glenn jackman Feb 25 '19 at 19:16

E.g. https://www.office-forums.com/threads/rwz-files.1483435/



Forums > Archive > Newsgroup Archive > Outlook Newsgroups > Microsoft Outlook >

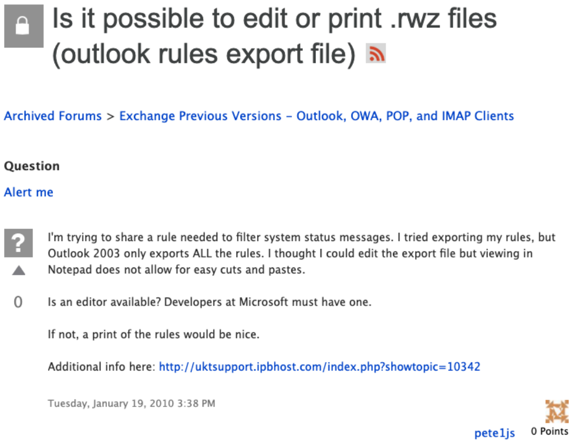
RWZ files

puzzled · Mar 19, 2009

Mar 19, 2009

How do I convert/extract/export Rules to text fiels. I don't want to type out the rules in a text format for presentations, I want to export from Outlook, and use the resulting text in a presentation.

E.g. https://social.technet.microsoft.com/Forums/exchange/en-US/a78d158a-9278-45ee-aeff-a7f18fee41f6/is-it-possible-to-edit-or-print-rwz-files-outlook-rules-export-file?forum=exchangesvrclientslegacy



Is it possible to edit or print .rwz files (outlook rules export file)

Archived Forums > Exchange Previous Versions – Outlook, OWA, POP, and IMAP Clients
Question
Alert me
0

I'm trying to share a rule needed to filter system status messages. I tried exporting my rules, but Outlook 2003 only exports ALL the rules. I thought I could edit the export file but viewing in Notepad does not allow for easy cuts and pastes.

Is an editor available? Developers at Microsoft must have one.

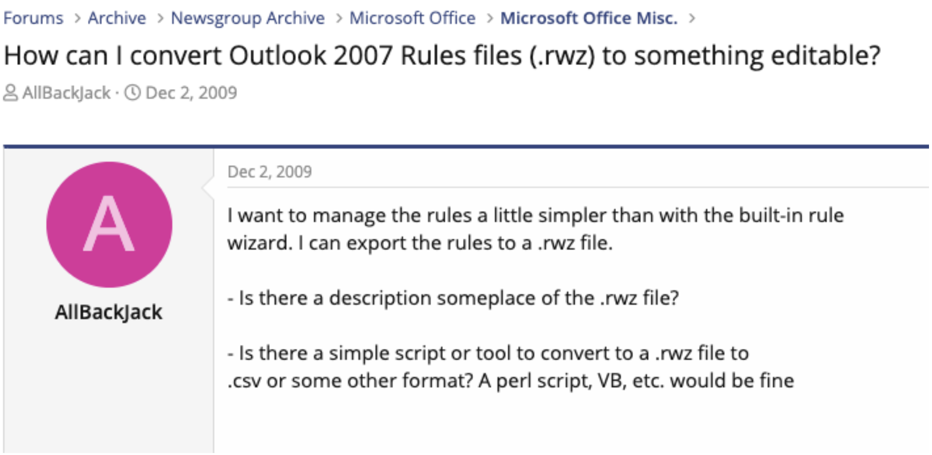
If not, a print of the rules would be nice.

Additional info here: http://uktsupport.ipbhost.com/index.php?showtopic=10342

Tuesday, January 19, 2010 3:38 PM

pete1js 0 Points

E.g. https://www.office-forums.com/threads/how-can-i-convert-outlook-2007-rules-files-rwz-to-something-editable.2239888/ & https://groups.google.com/g/microsoft.public.office.misc/c/D-_o46u_Hcs



Forums > Archive > Newsgroup Archive > Microsoft Office > Microsoft Office Misc. >

How can I convert Outlook 2007 Rules files (.rwz) to something editable?

AllBackJack · Dec 2, 2009

AllBackJack

Dec 2, 2009

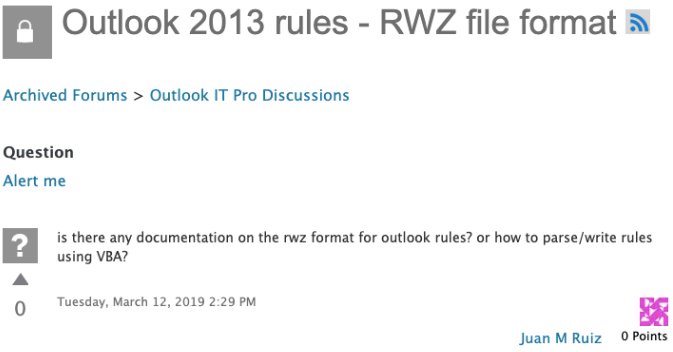
I want to manage the rules a little simpler than with the built-in rule wizard. I can export the rules to a .rwz file.

- Is there a description someplace of the .rwz file?

- Is there a simple script or tool to convert to a .rwz file to .csv or some other format? A perl script, VB, etc. would be fine

Users also want to overcome limitations of the Outlook rules editor. For example, they want to merge rules, sort rules, import & export only selected rules, etc. Documenting the file format would allow third parties to offer such functionality.
Note: although the Outlook object model enabled some functionality, there are some problems with this. Firstly, it requires Outlook to be installed (which excludes servers/Linux/installations without Windows) and the object model is not comprehensive (e.g. it does not allow for custom actions)

E.g. https://social.technet.microsoft.com/Forums/en-US/0cb9d0d6-9c7d-4d47-852b-2a0b63438975/outlook-2013-rules-rwz-file-format?forum=outlook



Outlook 2013 rules - RWZ file format

Archived Forums > Outlook IT Pro Discussions

Question

Alert me

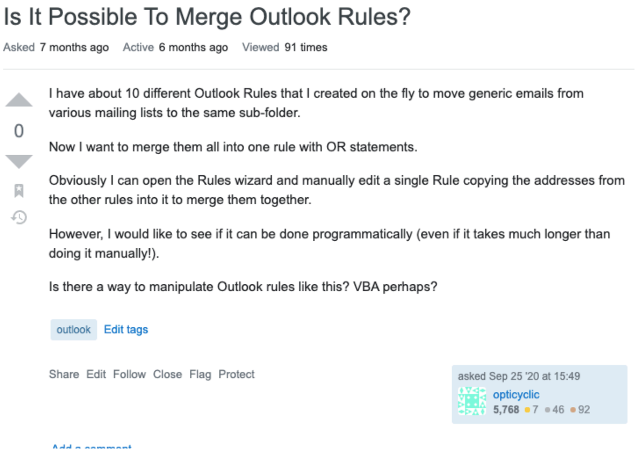
is there any documentation on the rwz format for outlook rules? or how to parse/write rules using VBA?

0

Tuesday, March 12, 2019 2:29 PM

Juan M Ruiz 0 Points

E.g. https://stackoverflow.com/questions/64067406/is-it-possible-to-merge-outlook-rules



Is It Possible To Merge Outlook Rules?

Asked 7 months ago Active 6 months ago Viewed 91 times

0

I have about 10 different Outlook Rules that I created on the fly to move generic emails from various mailing lists to the same sub-folder.

Now I want to merge them all into one rule with OR statements.

Obviously I can open the Rules wizard and manually edit a single Rule copying the addresses from the other rules into it to merge them together.

However, I would like to see if it can be done programmatically (even if it takes much longer than doing it manually!).

Is there a way to manipulate Outlook rules like this? VBA perhaps?

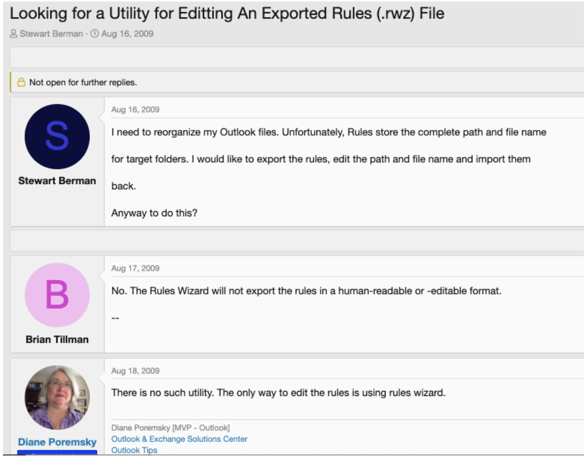
outlook Edit tags

Share Edit Follow Close Flag Protect

asked Sep 25 '20 at 15:49
opticyclic
5,768 ●7 ●46 ●92

Add a comment

E.g. https://forums.slipstick.com/threads/18711-looking-for-a-utility-for-editting-an-exported-rules-rwz-file/



Looking for a Utility for Editting An Exported Rules (.rwz) File

Stewart Berman · Aug 16, 2009

Not open for further replies.

Stewart Berman

Aug 16, 2009

I need to reorganize my Outlook files. Unfortunately, Rules store the complete path and file name for target folders. I would like to export the rules, edit the path and file name and import them back.

Anyway to do this?

Brian Tillman

Aug 17, 2009

No. The Rules Wizard will not export the rules in a human-readable or -editable format.

--

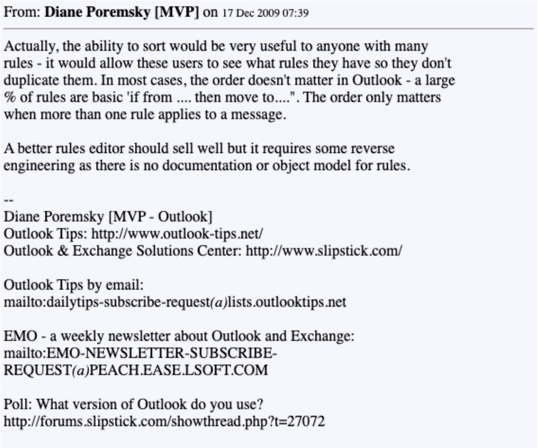
Diane Poremsky

Aug 18, 2009

There is no such utility. The only way to edit the rules is using rules wizard.

Diane Poremsky [MVP - Outlook]
Outlook & Exchange Solutions Center
Outlook Tips

E.g. http://www.adras.com/rwz-viewer-for-outlook-rules.t34546-14.html



From: **Diane Poremsky [MVP]** on 17 Dec 2009 07:39

Actually, the ability to sort would be very useful to anyone with many rules - it would allow these users to see what rules they have so they don't duplicate them. In most cases, the order doesn't matter in Outlook - a large % of rules are basic 'if from .... then move to....". The order only matters when more than one rule applies to a message.

A better rules editor should sell well but it requires some reverse engineering as there is no documentation or object model for rules.

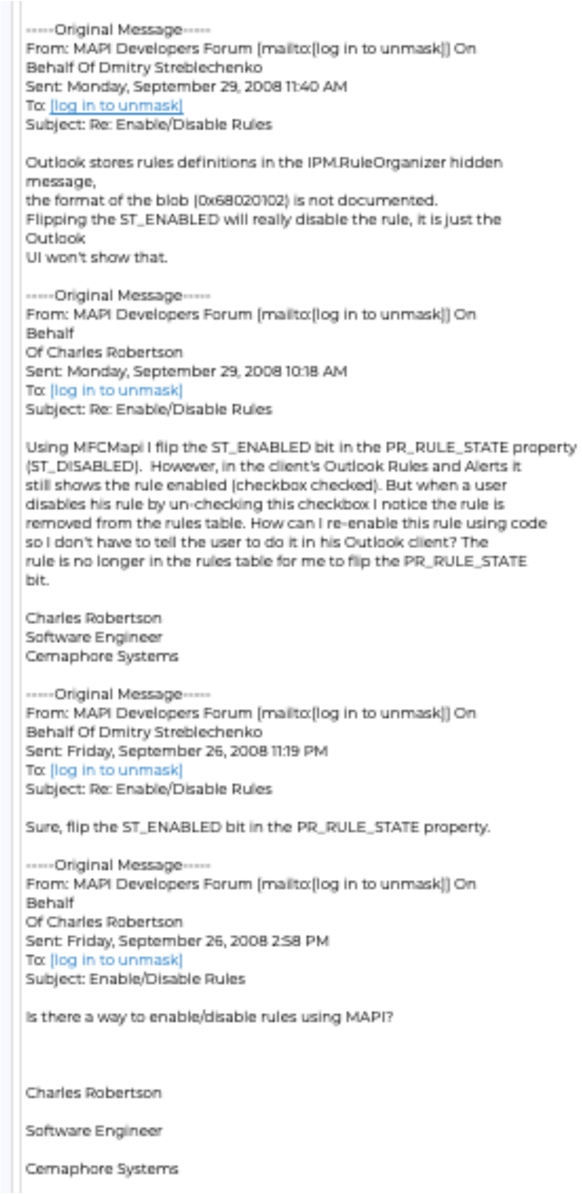
--
Diane Poremsky [MVP - Outlook]
Outlook Tips: http://www.outlook-tips.net/
Outlook & Exchange Solutions Center: http://www.slipstick.com/

Outlook Tips by email:
mailto:dailytips-subscribe-request(a)lists.outlooktips.net

EMO - a weekly newsletter about Outlook and Exchange:
mailto:EMO-NEWSLETTER-SUBSCRIBE-REQUEST(a)PEACH.EASE.LSOFT.COM

Poll: What version of Outlook do you use?
http://forums.slipstick.com/showthread.php?t=27072

E.g. https://peach.ease.lsoft.com/scripts/wa-PEACH.exe?A2=MAPI-L;e6463a34.0809&S=



-----Original Message-----
From: MAPI Developers Forum [mailto:[log in to unmask]] On
Behalf Of Dmitry Streblechenko
Sent: Monday, September 29, 2008 11:40 AM
To: [log in to unmask]
Subject: Re: Enable/Disable Rules

Outlook stores rules definitions in the IPM.RuleOrganizer hidden
message,
the format of the blob (0x68020102) is not documented.
Flipping the ST_ENABLED will really disable the rule, it is just the
Outlook
UI won't show that.

-----Original Message-----
From: MAPI Developers Forum [mailto:[log in to unmask]] On
Behalf
Of Charles Robertson
Sent: Monday, September 29, 2008 10:18 AM
To: [log in to unmask]
Subject: Re: Enable/Disable Rules

Using MFCMapi I flip the ST_ENABLED bit in the PR_RULE_STATE property
(ST_DISABLED). However, in the client's Outlook Rules and Alerts it
still shows the rule enabled (checkbox checked). But when a user
disables his rule by un-checking this checkbox I notice the rule is
removed from the rules table. How can I re-enable this rule using code
so I don't have to tell the user to do it in his Outlook client? The
rule is no longer in the rules table for me to flip the PR_RULE_STATE
bit.

Charles Robertson
Software Engineer
Cemaphore Systems

-----Original Message-----
From: MAPI Developers Forum [mailto:[log in to unmask]] On
Behalf Of Dmitry Streblechenko
Sent: Friday, September 26, 2008 11:19 PM
To: [log in to unmask]
Subject: Re: Enable/Disable Rules

Sure, flip the ST_ENABLED bit in the PR_RULE_STATE property.

-----Original Message-----
From: MAPI Developers Forum [mailto:[log in to unmask]] On
Behalf
Of Charles Robertson
Sent: Friday, September 26, 2008 2:58 PM
To: [log in to unmask]
Subject: Enable/Disable Rules

Is there a way to enable/disable rules using MAPI?

Charles Robertson

Software Engineer

Cemaphore Systems

2.6. Forensics companies want to recover and analyse rules

Interviews with stakeholders revealed that forensics companies want to be able to recover, read and analyse rules. For example, e-discovery firm GoldFynch[19] has developed a solution for legal clients that allow lawyers to analyse PST dumps. Documenting the RWZ and PidTagRwRulesStream format will allow forensics companies the ability to get a better picture of their legal problems in question[20, 21].

For example, rules may explain why certain emails were not actioned or received (e.g. there was a rule to mark them as read, move them or even permanently delete them). Rules can reveal deliberate or accidental non-compliant or illegal behaviour such as forwarding sensitive or restricted information to personal accounts or to unauthorized individuals[22]. Rules can also help show "the big picture" within a company by providing a glimpse of relationships between employees.

[19] https://goldfynch.com/
[20] https://www.pstwalker.com/email-investigations-and-forensic-analysis-of-outlook-exchange-email-files.html
[21] https://www.forensicfocus.com/forums/general/outlook-rule-settings-file/
[22] https://www.crypsisgroup.com/insights/microsoft-365-inbox-and-forwarding-rule-forensics

2.7. Security companies want to detect rules exploits

Business email compromise (BEC) attacks cost companies $3.5bn globally annually, according to 2019 FBI analysis[23]. This number will only increase as a result of the COVID-19 pandemic, increased online usage over time and the development of more sophisticated attacks that are more complex and harder to detect.

Outlook Rules exploits are well recognised. Rules and Custom Forms Injection attacks exist, whereby malicious attackers can setup forwarding rules and trigger custom actions[24]. Hidden rules attacks have been revealed in the past[25, 26]. Malicious Outlook rules have been used to get shell access[27, 28, 29, 30].

Outlook Rules also form a key part of exploit chains involving Outlook & Exchange. According to Cypsis, a breach response and risk management cybersecurity firm, "Once threat actors have access to a mailbox, we commonly observe them leveraging the mailbox rule capabilities of either Inbox, Simple Mail Transfer Protocol (SMTP) forwarding, and Transport policy to forward emails to an external email address or to hide or delete emails from the original intended recipients."[31] Tools also exist, such as XRulz[32]. XRulz's developers state that "Outlook rules can be used to achieve persistence on Windows hosts by creating a rule that executes a malicious payload. The rule can be setup to execute when the target receives an email with a specific keyword in the subject. An attacker can then drop shells on a target as and when they require by simply sending an email. In the past, this technique could only be done via the Outlook GUI. However, XRulez achieves this from the command line."[33]

Documenting the file format will allow cybersecurity and security penetration companies to develop general software for detecting and fixing common exploitation patterns and develop bespoke software for clients to ensure that certain policies are followed (e.g. there are no rules for printing or forwarding sensitive information etc.).

In 2018, researchers at FortiGuard Labs discovered and responsibly disclosed four remote code execution vulnerabilities[34] (CVE-2018-8522[35], CVE-2018-8524[36], CVE-2018-8576[37] and CVE-2018-8582) and a heap corruption vulnerability[38] (CVE-2018-8587[39]) in Outlook relating to importing malformed RWZ files. These are exploitable vulnerabilities that allowed malicious actors to execute code remotely in the context of the current user[40].

[23] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

[24] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide

[25] https://blog.compass-security.com/2018/09/hidden-inbox-rules-in-microsoft-exchange/

[26] https://www.crypsisgroup.com/insights/discovering-hidden-rules-business-email-crypsis

[27] https://www.blackhillsinfosec.com/malicious-outlook-rules-action/

[28] http://www.cunaceocouncil.net/cuna/assets/files/155211_Email-Phishing.pdf

[29] https://www.n00py.io/2017/03/from-osint-to-internal-gaining-access-from-the-outside-the-perimeter/

[30] https://gist.github.com/monoxgas/7fec9ec0f3ab405773fc

[31] https://www.crypsisgroup.com/insights/microsoft-365-inbox-and-forwarding-rule-forensics

[32] https://labs.f-secure.com/archive/malicous-outlook-rules/

[33] https://github.com/FSecureLABS/XRulez

[34] https://www.fortinet.com/blog/threat-research/patch-your-microsoft-outlook--fortinet-discovered-four-outlook-r

[35] https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2018-8522

[36] https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2018-8524

[37] https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2018-8576

[38] https://www.fortinet.com/blog/threat-research/a-deep-analysis-of-the-microsoft-outlook-vulnerability-

[39] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2018-8587

[40] https://security.stackexchange.com/questions/213840/microsoft-outlook-vulnerability-cve-2018-8587-how-likely-is-exploitation

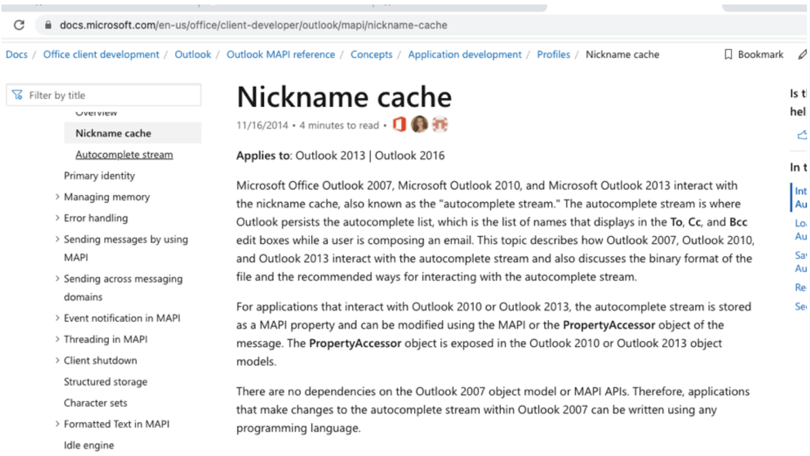
Security researchers may be able to use the documentation of the RWZ format to write fuzzers against Outlook, as Outlook Rules represent a surface area for attack. Transparency benefits the community – documenting the format may avoid future (or as yet unknown) attacks on the RWZ parser/surface area. The Rules Wizard code is old, is over 20 years old and appears to have been developed originally by a contracting software company, and not Microsoft. Code like this has caused problems in Office in the past, for example in the 17-year-old Equation Editor[41].

3. Documentation Options

There exist multiple options for documentation. The following list is not prescriptive and alternative options can be explored. This document does not suggest any one idea but does give examples of some options. It is acknowledged that there may exist some or significant developer time associated with any documentation option and some may not be feasible or in fact desirable. Any action taken should not disproportionately exceed the benefits of documenting the format listed in this document.

3.1. Office Developer Microsoft Docs

The format could be documented in the Office Developer Microsoft Docs. This has been used for the documentation of the Outlook Nickname Cache (NK2) file format[42]. The documentation should detail the format of the file header and footer, each rule's header and each element contained within a rule.


docs.microsoft.com/en-us/office/client-developer/outlook/mapi/nickname-cache
Docs / Office client development / Outlook / Outlook MAPI reference / Concepts / Application development / Profiles / Nickname cache
Bookmark
Filter by title
Overview
Nickname cache
Autocomplete stream
Primary identity
Managing memory
Error handling
Sending messages by using MAPI
Sending across messaging domains
Event notification in MAPI
Threading in MAPI
Client shutdown
Structured storage
Character sets
Formatted Text in MAPI
Idle engine
Is t
hel
In t
Int
Au
Lo
Au
Sa
Au
Re
Se

Nickname cache

11/16/2014 • 4 minutes to read •

Applies to: Outlook 2013 | Outlook 2016

Microsoft Office Outlook 2007, Microsoft Outlook 2010, and Microsoft Outlook 2013 interact with the nickname cache, also known as the "autocomplete stream." The autocomplete stream is where Outlook persists the autocomplete list, which is the list of names that displays in the **To**, **Cc**, and **Bcc** edit boxes while a user is composing an email. This topic describes how Outlook 2007, Outlook 2010, and Outlook 2013 interact with the autocomplete stream and also discusses the binary format of the file and the recommended ways for interacting with the autocomplete stream.

For applications that interact with Outlook 2010 or Outlook 2013, the autocomplete stream is stored as a MAPI property and can be modified using the MAPI or the **PropertyAccessor** object of the message. The **PropertyAccessor** object is exposed in the Outlook 2010 or Outlook 2013 object models.

There are no dependencies on the Outlook 2007 object model or MAPI APIs. Therefore, applications that make changes to the autocomplete stream within Outlook 2007 can be written using any programming language.

This may require some time to document and there may not be sufficient demand within the product group.

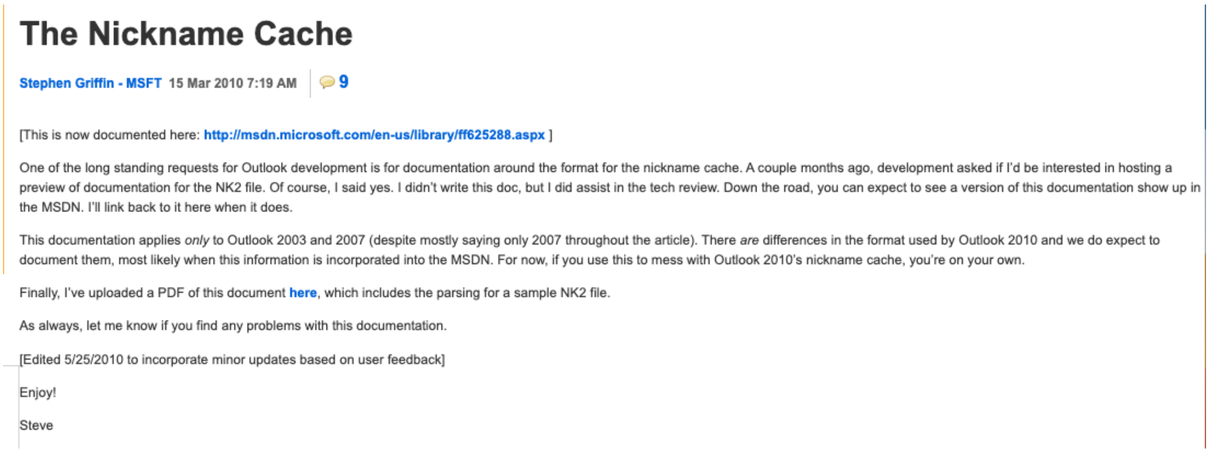
3.2. Blog Post

The format could be documented in a blog post. For example, MFCMAPI developer Stephen Griffin, posted a blog post describing the Outlook Nickname Cache (NK2) file format[43]. It is notable that this blog post led to increased demand for documentation, and accordingly the format was subsequently officially documented in the Office Developer Microsoft Docs. This path may be a good stopgap measure to fix ongoing incomplete implementations in current open-source projects.

[41] https://securityboulevard.com/2018/01/microsoft-kills-old-office-equation-editor-due-to-new-flaw/

[42] https://docs.microsoft.com/en-us/office/client-developer/outlook/mapi/nickname-cache

[43] http://web.archive.org/web/20120325162100/http://blogs.msdn.com/b/stephen_griffin/archive/2010/03/15/the-nickname-cache.aspx



The Nickname Cache

Stephen Griffin - MSFT 15 Mar 2010 7:19 AM 9

[This is now documented here: http://msdn.microsoft.com/en-us/library/ff625288.aspx]

One of the long standing requests for Outlook development is for documentation around the format for the nickname cache. A couple months ago, development asked if I'd be interested in hosting a preview of documentation for the NK2 file. Of course, I said yes. I didn't write this doc, but I did assist in the tech review. Down the road, you can expect to see a version of this documentation show up in the MSDN. I'll link back to it here when it does.

This documentation applies *only* to Outlook 2003 and 2007 (despite mostly saying only 2007 throughout the article). There *are* differences in the format used by Outlook 2010 and we do expect to document them, most likely when this information is incorporated into the MSDN. For now, if you use this to mess with Outlook 2010's nickname cache, you're on your own.

Finally, I've uploaded a PDF of this document here, which includes the parsing for a sample NK2 file.

As always, let me know if you find any problems with this documentation.

[Edited 5/25/2010 to incorporate minor updates based on user feedback]

Enjoy!

Steve

This may require some time to document and there may not be sufficient demand within the product group.

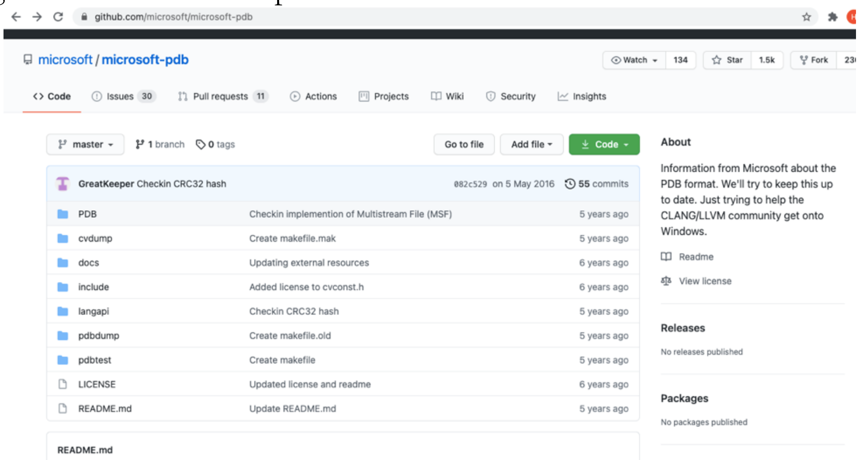
3.3. Test Cases/Dumping Tool

The format could be documented through the release of some test cases and perhaps a tool that releases corresponding textual dump. For example, Microsoft has released tools for dumping PDB and PST files[44].

There may exist no test cases or dumping tool for RWZ files.

3.4. Source Code Dump

In the past, Microsoft have released source code dumps to assist parsing file formats that are requested by the community. For example, the microsoft-pdb project was released help the CLANG/LLVM community get onto Windows[45]. The following comment describes the aim of releasing the source code: "With this information we are now building the information for other compilers (and tools) to efficiently write a PDB. The PDB format has not been officially documented, presenting a challenge for other compilers and toolsets (such as Clang/LLVM) that want to work with Windows or the Visual Studio debugger. We want to help the Open-Source compilers to get onto the Windows platform."



GreatKeeper Checkin CRC32 hash 082c529 on 5 May 2016 55 commits

PDB	Checkin implemention of Multistream File (MSF)	5 years ago
cvdump	Create makefile.mak	5 years ago
docs	Updating external resources	6 years ago
include	Added license to cvconst.h	6 years ago
langapi	Checkin CRC32 hash	5 years ago
pdbdump	Create makefile.old	5 years ago
pdbtest	Create makefile	5 years ago
LICENSE	Updated license and readme	6 years ago
README.md	Update README.md	5 years ago

README.md

About

Information from Microsoft about the PDB format. We'll try to keep this up to date. Just trying to help the CLANG/LLVM community get onto Windows.

Readme

View license

Releases

No releases published

Packages

No packages published

This may conflict with some source licensing restrictions. Furthermore, due to the Rule Wizard's tight integration, release of source code may be impossible.

[44] https://github.com/microsoft/microsoft-pdb/blob/master/pdbdump/pdbdump.cpp
[45] https://github.com/microsoft/microsoft-pdb

3.5. Publish Outlook Symbol Files

Microsoft could release symbol (PDB) files for Office libraries and executables, for example outlook.exe and olmapi32.dll. This would allow reverse engineers to be able to understand the file format better as symbols can explain what various unknown functions do and give insights into the file format parser.

This may require approval within the product group as Office symbols are not currently released. Further, PDB files may need to be cleaned up to remove language inappropriate for public consumption and to exclude code from third-party vendors[46].

3.6. Work with Open-Source projects on an ad-hoc basis

As discussed previously, there exists some documentation of the RWZ file format by the Kopano developers[47] and a more comprehensive specification and implementation in OutlookRulesReader[48]. Outlook developers could help certain open-source projects in answering specific questions, for example in revealing the meaning of unknown fields. Given their access to the source code, they may be able to answer some questions easily.

This may risk stratifying the community by creating a "preferred" project for reading/writing Outlook Rules. Furthermore, it is not in the spirit of open-source and does not convey the benefits to the open-source community as it would not be usable by tools such as MFCMAPI who only parse documented formats in their source base.

3.7. Release an Open Specification

Microsoft could release an open specification for the RWZ file format, similar to the MSG[49], PST (Personal Storage Table)[50] and OAB (Offline Address Book)[51] file format.

This may require some time to document and there may not be sufficient demand within the product group.

3.8. Do Nothing

The OutlookRulesReader project already contains a ~80-90% reverse engineering effort of the RWZ file format. Considering the progress already made and the effort required by the Microsoft product group to document the format exceeds the benefits.

This may risk incomplete or incorrect documentation becoming the de-facto source of truth. Furthermore, it is not in the spirit of open-source and does not convey the benefits to the open-source community as it would not be usable by tools such as MFCMAPI who only parse documented formats in their source base.

[46] https://docs.microsoft.com/en-us/archive/blogs/mpower/outlook-symbols

[47] https://github.com/Kopano-dev/kopano-core/blob/e23230568e679c5879bf0a027754854576be5060/doc/ol_rule_spec.txt

[48] https://github.com/hughbe/OutlookRulesReader

[49] https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxmsg/b046868c-9fbf-41ae-9ffb-8de2bd4eec82

[50] https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-pst/141923d5-15ab-4ef1-a524-6dce75aae546

[51] https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxoab/b4750386-66ec-4e69-abb6-208dd131c7de