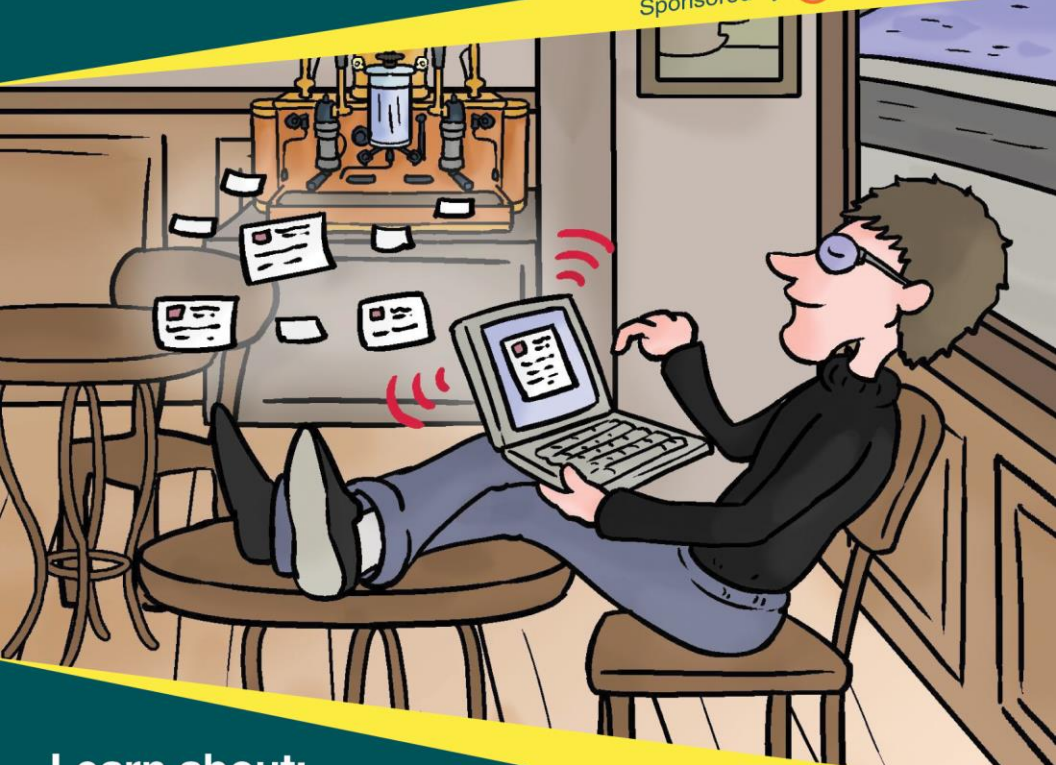


Conversational Office 365 Email Signatures

 A ConversationalGeek®
Book

Sponsored by  exclaimer™



Learn about:

- The importance of uniform email signatures
- Email signature consistency challenges
- Exclaimer's solution for email signatures within Office 365

3rd
Edition

By J. Peter Bruzzese (Microsoft Office Apps and Services MVP)

Sponsored by Exclaimer

Founded in 2001, Exclaimer is the multi-award-winning global market leader in email signature solutions for Office 365, Exchange and G Suite. With over 75 million users worldwide in 150+ countries, its diverse customer base includes renowned international organizations such as Sony, NBC, and the BBC and many more organizations of all sectors and sizes.

Exclaimer solutions are regularly recommended by Microsoft MVPs (Most Valuable Professionals) and have an exceptional reputation within the Microsoft community.



www.exclaimer.com

Conversational Office 365 Email Signatures

By J. Peter Bruzzese

© 2018 Conversational Geek



Conversational**Geek**®

Conversational Office 365 Email Signatures

Published by Conversational Geek® Inc.

www.conversationlgeek.com

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Trademarks

Conversational Geek, the Conversational Geek logo and J. the Geek are trademarks of Conversational Geek®. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author: J. Peter Bruzzese

Project Editor: Michele Touchet

Copy Editor: Steven Zimmerman

Content Reviewers: Rebekah Bell

Note from the Author

Greetings!

I remember the days when a signature was simply your name and title, perhaps some additional contact information. Using Outlook to control your own signature was easy enough for most. Unfortunately, some took the creativity needle and pushed it off the charts with all sorts of weird fonts, graphics, quotes and such (without any concern for consistency).

At some point the email signature became a representation of the company itself. It therefore became necessary to regulate and make it uniform and consistent. In fact, email signatures are now considered part of the PR and marketing of a company, making the need for a consistent, professional signature even more necessary.

In addition, the need to add disclaimers and the importance of having consistent signatures across devices (desktop vs. mobile) added the need for IT to provide such uniformity over and above what Outlook could do.

Although there are built-in tools for both Exchange and Office 365's Exchange Online, there are times when a third-party solution may be needed to ensure your company is getting the full value from the signatures your employees send with each and every email correspondence.

J. Peter Bruzzese



The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.



Greetings. They call me J. Within these boxes I can share just about anything on the subject at hand. Read ‘em!

The Hidden Value of Email Signatures



An email signature, when done right, is of tremendous benefit to organizations. So it surprises me sometimes when I receive and read an email message wherein the content comes across as professional, and then I glance at the signature which screams “amateurish”, “unprofessional” and/or “blah”.

At the same time, I also find that inconsistent email signatures jar my perception of the sender. One moment I get an email that has a signature and the next I get the “Sent from my iPhone” mobile flavor of the email.

I’m not judging folks for stepping out, and I certainly appreciate that they value me enough to email me on the go, but it’s a combination of the loss of professionalism the signature should provide combined with the TMI factor (i.e. I don’t want to know what device you’re using unless the real message is ‘please forgive all the typos and acronyms... I’m on my phone’).

I find I like it when I see a signature with the company logo. I find I dislike it when I see a signature that has a place for the logo but the jpg didn’t come through. Ugh. I’m somewhat on the fence with signatures that contain the Twitter, Facebook, etc. logos, but I am definitely turned off when those graphics don’t render.

Key Uniform Email Signature Goals

There are three key goals a company should seek to achieve through a uniform email signature:

The Disclaimer: It’s common to see these at the bottom of emails with a mixture of language that hits confidentiality, privacy and/or legal concerns. Typically, disclaimers go to outside recipients and aren’t necessary for internal email correspondence.

The Professional Impression: Having each individual within an organization present their own “style” in an email signature may not give the image you want. Quotes, personal comments, graphics and so forth may be a display of an employee’s ‘personality’ but are not necessarily professional. Having a consistent email signature across the organization makes a better impression overall. It helps maintain the professionalism of your brand.

The PR Value: An email signature can be a form of marketing. Perhaps you want to include social media icons, award logos or other dynamic content. Often times when I have speaking engagements, I will put them in my signature to get the word out. Sometimes I'll use a banner or graphic that links to the event itself.

No doubt, your company may have similar events, news, product announcements and so forth that could be spread to a wider audience by simply using employees' email signatures to do it.

But again, this cannot be left up to the whim and will of each end user. You have to ensure it's done right, is centrally manageable, and is consistent from one device and email application to another.



Think about it... if your people use PCs, tablets, and mobile devices throughout their day but only the PC email application has a signature, you are not providing a consistent, professional impression. And you're losing out on marketing/PR opportunities in the process.

The Big Takeaways

Email is the most common form of communication in any business. It's not only mission critical from the perspective of needing to be available, it's essential that emails coming from your company convey a uniform professionalism and maintain regulatory compliance standards.

I read a statistic that says the average employee sends 35 emails daily. So in a 100-person company that's 3,500 emails every single day! A company can use that high volume email load as a low-cost marketing tool, but only if they know how.

The hidden value in email signatures can only be unlocked if they aren't left to chance. Consistent (whether in the office or on the road), professional in appearance, uniform throughout your organization... these are key aspects of email signatures that deliver value.

Challenges of Email Signature Consistency



Centrally managed email signatures are not as easy to establish as you might think. There is a technical side to it, as well as a design element that must be taken into consideration.

Manual Methods for Email Signatures

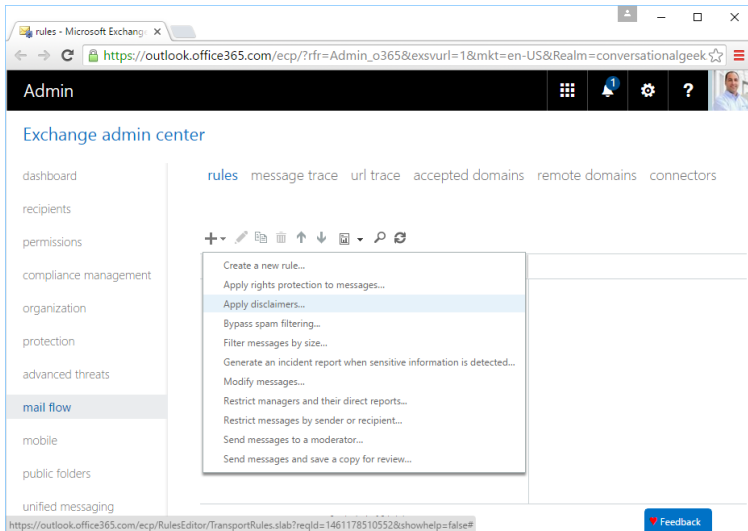
Aside from telling your end users to just create their own signatures in Outlook (which will not carry over to their other devices, mind you), IT admins can try and use transport rules within Exchange and/or Office 365 Exchange Online to create basic disclaimers.

To accomplish this, you need to know how to create a transport rule. It's basically a set of conditions, actions and exceptions, which are optional. So when a condition is met (say "All email going outside the organization"), an action is taken (say "Append this text" and then insert text) unless this exception applies (say "the disclaimer has already been applied").



A common complaint with transport rule disclaimer signatures is that with replies and such, the signature will continue to get applied each time, but at the bottom of the email chain. You can avoid this by using an exception to examine if the disclaimer text is already applied.

In the Office 365 dashboard you need to go to your Exchange Admin Center tools. From here you select the 'mail flow' feature, and then under 'rules' you can create a new rule or simply choose the 'Apply disclaimers' template.



It sounds easy enough right? Well, it is if all you're looking to do is add some text to the bottom of every email leaving your organization. To format the text, or include more information in it, you have to use HTML to make it work. The content will also be added at the very bottom of the entire email conversation – not underneath your most recent message, but at the bottom of the whole chain instead.

Images can be inserted but not directly, so you have to point to them on a public website through a link. That means they may not appear in many email clients. Instead, they will appear as red 'X' squares until the user clicks to 'Download additional content'.

For a little automatic personalization, you can use special tags to pull in Active Directory attributes of your users and then insert those using double % symbols (like %%displayName%% for their name or %%PhoneNumber%% to insert their number).

You can use the transport rules to create multiple disclaimers and set the condition(s) to apply to a specific user or group of users in order to apply different disclaimers to different persons/teams. But this requires quite a bit of effort on the part of an already overworked IT admin.

Built-in Exchange Functionality Limits

Transport rules will certainly work if a simple disclaimer is all you're looking for, but as we discussed earlier, when used properly, email signatures can benefit your organization big time. Uniformity is key, as is a professional look.

When you are working with transport rules to establish basic disclaimer email signatures, there are a variety of important limitations to consider, beyond the extra work involved. For example, the fact that the only way to enhance the look of your email signature is through HTML mark-up. Without a visual editor you'll be learning (or re-learning for those of us who have been playing in the IT world since the '90s like myself) HTML.

And what about mobile devices? For example, iOS devices tend to use email clients that send in plain text. If your HTML code is applied to that plain text email, it definitely won't be formatted correctly, and it's possible the recipient will see a block of raw HTML code instead of a signature.

There is no way to test your rule without enabling it and then sending a test email. Again, that's extra work. There are no templates to choose from to help you with the look and feel of your signature. IT folks are not known to be universally proficient with graphic artistry. Much less proficient enough to make it all come together through HTML. So now you're looking for a graphics person and a web designer who can write solid HTML/CSS to make the signature look polished.

Connectors Assist Office 365

Much like with an on-premises deployment of Exchange, if you wish to add functionality within the mail flow, you need to use third-party solutions and daisy chain these together with connectors.

Inbound and outbound connectors can be quite useful for enhancing the email system (whether on-prem or in the cloud) with security, archiving and more, including email signature support.



On-premises, you can daisy chain multiple solutions together quite easily and without too much concern of added latency. However, one challenge with the cloud is that the more services you daisy chain the greater the email latency and the greater the complexity of the solution (which also adds to the difficulty in troubleshooting).

Creating inbound and outbound connectors is not incredibly difficult in Office 365 if you have the proper permissions to do so. To accomplish this, you log in and from your Apps Launcher you choose Admin. On the bottom left is an icon for Admin Centers. Hover over that icon and choose Exchange.



Once you are in the Exchange Admin Center you want to find the 'mail flow' feature from the Features pane. Then select the Connectors tab at the top.

The screenshot shows the Exchange Admin Center interface. At the top, there is a dark navigation bar with the word "Admin" on the left and several icons (grid, notification, settings, help) on the right. Below this is the "Exchange admin center" header. On the left is a vertical navigation pane with various categories: dashboard, recipients, permissions, compliance management, organization, protection, advanced threats, **mail flow** (highlighted), mobile, public folders, unified messaging, and hybrid. The main content area shows the "connectors" tab selected. It contains a heading "rules message trace url trace accepted domains remote domains connectors" with "connectors" being the active link. Below the heading is a paragraph of text explaining connectors and a link to "check to see if you should create a connector". There is also a feedback link: "Want to help us improve connectors? Just send us feedback and let us know what you liked, didn't like, or what we can do to make your experience better." Below the text are three icons: a plus sign, a trash can, and a refresh icon. At the bottom, there is a table with columns for STATUS, NAME, FROM, and TO. The table is currently empty, with the text "There are no items to show in this view." centered below the header row.

Note: From within the Connectors section you can add incoming and outgoing connectors that go to on-premises email servers (like in a hybrid environment), to and from Partner organizations (i.e. business partners and/or service providers), to and from the Internet and so on.

Depending on the direction from the vendor you're working with, you can establish these connectors to alter mail flow with the intent of adding special features to Office 365 (like a signature solution, security solution, archive solution and so on).

Key Takeaways

Office 365 through Exchange Online does have the ability to provide a measure of email signature uniformity through the use of transport rules and disclaimers. Beyond the basic inclusion of text, you have to look at using HTML to fancify your signatures and/or look for email signature resources (ie. pre-built HTML templates) you can use.

However, when compared to third-party email signature tools that provide a visual editor with no IT experience needed, a built in set of templates and more, you may find you want and need to use an additional solution for your email signature needs when working with Office 365.

Vendor Sponsor: Exclaimer Cloud



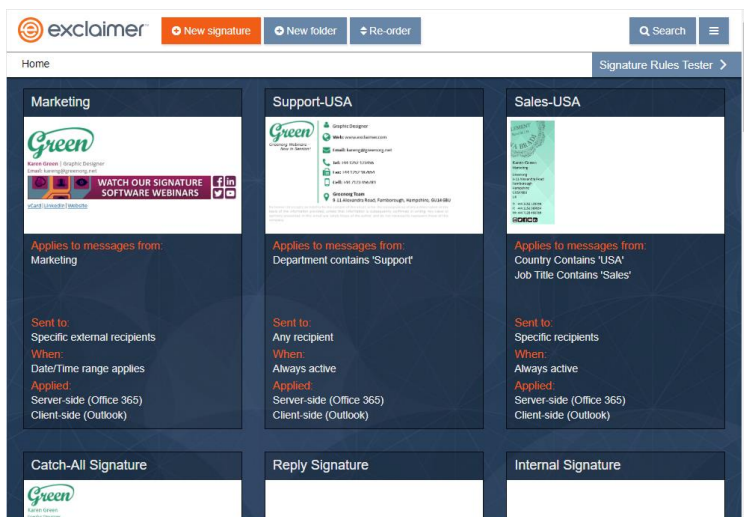
It's safe to say, if you're an IT/Exchange admin, you would love to have a way to not only resolve the email signature uniformity conundrum but also delegate it to someone else.

Exclaimer Cloud does just that. Through a web-based user interface, you can create professional email signatures or delegate the process to someone with absolutely no IT expertise. From a single system, a non-IT user with no HTML skills can design and apply multiple signatures for all Office 365 users.

The person designated to design the signatures will use the web-based UI where they can create email signatures using a drag-and-drop editor, or choose from a range of professional signatures in the template library. Contact details for the users will be pulled from Office 365's Directory for fields like name,

job title, phone number and so on. You'll also have the ability to use custom attributes in signatures, and any fields that aren't populated for a particular user in your directory will automatically be hidden without messing up the design.

The drag-and-drop signature editor allows you to easily add elements such as logos, promotional banners, user photos and social media icons. Once you've finished creating the signature, you can then apply it to users based on details such as an Office 365 Group, the sender/recipient domain, or specific user attributes like job title or country.



When it comes to managing and deploying the signatures to your users, there's a range of options available. You can create different signatures for different departments/groups. For example, the Sales team can have a signature with a banner for an event your company is attending, and then a time-and-date range can be specified. You also have the ability to choose for certain signatures to only apply if the email recipient is internal or external, or if the email is a reply message.

Multiple users can be given access to your Exclaimer Cloud account, and you can assign them either admin or editor

permissions. This ensures the correct person deals with the correct signatures, whether that be department or country-specific. This means that you don't have to rely on a single person to manage company-wide signatures.

How Exclaimer Cloud Works

Exclaimer Cloud is extremely flexible, providing multiple setup options depending on your particular needs.

1. **Server-side configuration:** Mail flow is configured through connectors to go from Office 365 to Exclaimer's regional Azure servers. The signature is added and then passed back to Office 365 for sending.
2. **Client-side only configuration:** With this setup, mail flow does not pass through Microsoft Azure. An agent is installed which deploys signatures to your users' Outlook, where they can choose a specific email signature template created in Exclaimer Cloud.
3. **Client and server-side (the best of both worlds):** Email signatures are deployed to Outlook, and emails are also passed through Azure. This means your users still have the option to choose their signature, and they'll also get signatures stamped on emails sent from mobile devices and Macs.

The Azure Configuration Setup

Exclaimer Cloud is hosted within the Microsoft datacenter world (the Azure side). As a result, your Office 365 emails are all processed within the Microsoft Cloud infrastructure. That's comforting on multiple levels.

Certainly from a security perspective and a desire to avoid email tampering, having the process contained is a plus. But

also from a latency perspective, having the solutions “near” each other physically and in similar datacenter/network spheres can help reduce excessive latency concerns.

On the Azure side, setup is done so you have a high-availability, load-balanced configuration. The send (outbound) connector will pass the email from Office 365 to a regional Exclaimer Azure server. After the signature is applied, it will use the receive (inbound) connector to pass the email back before it gets sent out.



As for ‘how’ the signature is applied, when the email reaches the Azure server, Exclaimer Cloud examines the message ‘envelope’, which includes the sender’s details and intended recipients, determining which signature to apply to the email.

The sender’s attributes are pulled from the cached Azure AD data, which is used to populate the selected signature, e.g. name, job title, phone number, etc. Exclaimer Cloud then ascertains where the signature is to be inserted. It decodes the MIME (Multipurpose Internet Mail Extensions)/TNEF (Transport Neutral Encapsulation Format) carrier to do this.

The signature is then inserted in the appropriate location and this new email is sent back to Office 365. It passes through the Receive connector, which forwards the email onto its original recipient/s.

Exclaimer Cloud does not save any email content to an external location. This is due to the SMTP mode of integration with Office 365 not requiring emails to be stored prior to being forwarded back to Office 365.

All it does is look for a reply separator in order to apply the signature correctly. It also scans the message body for any unique strings to determine if a signature is already present i.e. during email conversations.

Strict Security Maintained

The connectors we spoke of earlier will protect the integrity of the mail flow. SSL certificates and TLS encryption are used to provide a secure connection between Office 365 and Exclaimer Cloud.

Overall, because the email stays in the Microsoft Cloud loop, and proper connector protocols are used to ensure security, that email is not compromised, nor compromisable in transit through the signature “stamping” process.

Getting Into the Nitty Gritty of Security

Data is encrypted using a combination of RSA-2048-bit asymmetric encryption and a one-time use Rijndael symmetric session key. Rijndael is an algorithm selected by the U.S. National Institute of Standards and Technology (NIST) as the Advanced Encryption Standard (AES). Keys issued are managed through certificates, with several of these being used for encipherment (converting a message into a cipher for encryption and decryption) purposes.

When Exclaimer Cloud processes an email, it examines the message to decipher the sender's details so it can apply the relevant signature as configured within the UI. It also scans the mail for common strings that represent a reply separator, so the signature can be inserted in the correct location.

Exclaimer Cloud does not actually 'read' the message in the traditional sense, and the email content is not saved (persisted to disk) or available to Exclaimer personnel.

Exclaimer Cloud is hosted in 14+ regional Microsoft Azure locations globally. Each region has a primary and secondary datacenter, ensuring your mail flow is constant, even in the rare event of an issue occurring in the primary datacenter.

The ISO 27001:2013 Certification

Exclaimer Cloud has achieved the ISO 27001:2013 Certification for Information Security Management, which was awarded by Alcumus ISOQAR and the United Kingdom Accreditation Service (UKAS). The ISO 27001:2013 Certification means a third-party accredited independent auditor has performed a thorough assessment and has confirmed it is operating in alignment with ISO cloud standards.



Certificate Number 14108
ISO 27001: 2013

These signatures are giving me a
HEADACHE!

Choose the pain-free way of
managing email signatures

Get your
14 day free
trial today

www.exclaimer.com/cloud-signatures



Certificate Number 14108
ISO 27001: 2013

Easily “converse” about Office 365 email signatures in any setting.

If you are moving to or already on Office 365 it's essential to understand the value of email signature consistency and the possible ways of achieving such uniformity. There are built-in methods that provide less-than-stellar results. Looking to a third-party solution may be a better choice to provide your organization what it needs.



About J. Peter Bruzzese

J. Peter, an Office Servers and Services MVP (Exchange/Office 365) and MCSE/MCITP: Messaging, is an internationally published author and conference speaker, an InfoWorld journalist, and co-founder of both Conversational Geek and ClipTraining. Follow him on Twitter @JPBruzzese.



ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.