VUTURE **GUIDE**

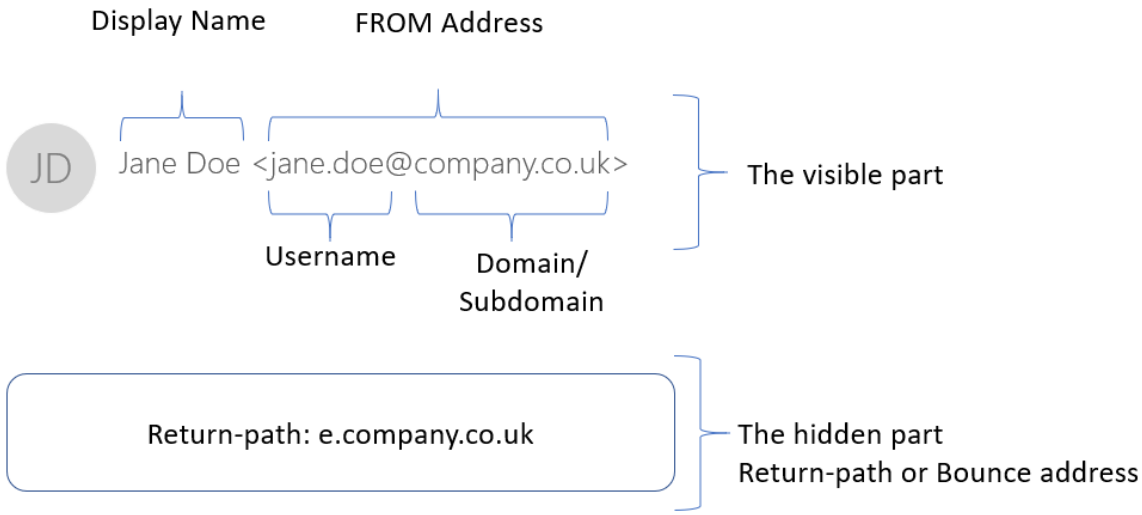
A complete guide to the custom return-path and email authentication

The custom return-path and email authentication can be quite technical and complex for the uninitiated. In this guide we aim to clear the fog on the custom return-path and email authentication.

Disclaimer: Though we aim to give you the very latest information some things do change quickly in this industry.

Contents

What's in an email?



The visible part

Display name: is the friendly name your clients will see when they receive your email. This can be anything from the name of your business to the name of an individual within your business. Vuture allows you to completely customise this display name.

From Address: Is the visible email address your recipients will see in their inbox.

Username: is the part of the email before the @sign. You can set up whatever you like for this username. It can be generic such as events@ or it could be an individual's name such as jane.doe@

Domain (Root domain): Is the part of the email after the @ sign. Typically, this will be the primary domain for your business e.g. @company.com

Subdomain: is a domain that is part of the root domain. E.g. @events.company.com is a subdomain.

The hidden part

The hidden part of an email is called the return-path, bounce address or envelope from. This part isn't visible to the end recipient but is the real and actual email address from which your emails are sent. By default, Vuture creates a generic return-path for you when your system is first setup. This will be something like bouncebacks@888.vx-email.com where 888 is the ID of your Vuture instance. The return-path is 888.vx-email.com.

> Note: When you send an email and write your own Display name and from address this only changes the visible part of the email. This doesn't change the return-path.

What is a custom return-path?

A custom return-path replaces the generic Vuture return-path with a domain or subdomain of your choice. By having a custom return-path it allows us to align the domain of the visible and the hidden part of your email.

Why should you use a custom return-path?

- The most important reason to set up a return-path is that it will help with getting your email into the inbox.
- It allows us to implement security authentications on a custom return-path SPF, DKIM, DMARC and BIMI. It is best practice to configure these on a custom return-path because of domain alignment.
- These authentications are what many organisations are using to filter emails coming into their networks. Some organisations don't allow emails through that don't have these authentications.
- Using a custom return-path allows you to build up your sending reputation more easily.
- Using a custom return-path means that you can align the visible and the hidden parts of your emails. This helps with preventing you looking like a phisher or spammer.
- Removes the "via" message in Gmail that shows both the Return-Path address and the FROM address if the domains are not the same or are not sub-domains.

What are email authentications?

Sender Policy Framework (SPF)

SPF stands for Sender Policy Framework. It is an open standard used to help the fight against spam. SPF allows the domain owner to specify which mail servers will be used when they send emails from that domain. When configuring SPF on e.company.co.uk you would specify that Vuture will be sending from the return-path.

In other words, it's like registering your car to your driver's license. Anyone who did a check on the car would know that you can drive it. If they found someone else driving your car they'll know they shouldn't be doing so.

This information is published in the Domain Name System (DNS) which is the online library of all the machines connected to the internet. A little like the DVLA or DMV databases.

Why is SPF important?

During an SPF check, the email servers verify the SPF record by looking up the domain name listed in the return-path address in the DNS.

If the IP address sending email on behalf of the return-path domain isn't listed in that SPF record, the message fails SPF authentication. You can apply the SPF to both your display from domain and your custom return-path.

An SPF protected domain is something that phishers are less likely to use and is therefore less likely to be blacklisted by spam filters, ensuring legitimate email from that domain is delivered. In other words, you are more likely to end up in the inbox.

Domain Key Identified Mail (DKIM)

DKIM is a method of cryptographically signing emails. It allows the receiving server to verify that the email has not been tampered with in transit and that the sender is who they say they are. It is arguably the most complicated authentication protocol. You use a private key to encrypt the emails you send. The recipient's server uses a public key to decrypt the email.

You can think of DKIM like a safe and combination lock. Each email is secured inside a unique safe with a common publicly available combination that can open each of these safes. There are details inside the safe that prove the domain is owned by the sender.

Why is DKIM important?

DKIM can help spammers from forging your domains. Along with SPF records DKIM can improve overall delivery rates by ensuring that recipient servers know you are a legitimate sender.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

DMARC is an email validation system designed to detect and prevent email spoofing. It is built on top of two existing mechanism to help in the fight against spam SPF and DKIM. The DMARC authentication tries to block fraudulent activity from an organisation's domains.

Why is DMARC important?

DMARC is the first and only widely deployed technology that can make the from address trustworthy. This helps to protect you and your clients. It also discourages cybercriminals who are less likely to go after a brand with a DMARC record. It is helping in the fight against spam and is far more likely for your emails to land in your recipient's inboxes. It allows you to tell any email receiver that looks at DMARC that you protect your messages with SPF and DKIM. This means a receiver can decide what to do with emails that fail DMARC. This typically includes passing the message to the recipient's junk folder or better, rejecting it and the recipient never seeing it.

> When you consider your DMARC strategy it's worth looking at your root domain as well as your marketing domain to make sure they are both aligned. This is something that your IT department will be able to support you with.

Brand Indicators for Message Identification (BIMI)

BIMI is the newest effort for an industry-wide standard that will use brand logos as indicators to help people avoid fraudulent email. Though BIMI has not officially launched yet, it is being driven by several largest mailbox providers and organizations worldwide like Google, Microsoft, Oath (Yahoo, AOL, and Verizon), Comcast, Agari, PayPal and Return Path.

Transport Layer Security (TLS)

TLS Is a way of encrypting emails from the point of send to the point of receipt. It uses symmetric cryptography to encrypt the data transmitted.

With opportunistic TLS Vuture will ping the recipient's server to ask whether they can communicate over TLS. If the server says yes, then Vuture will send the email encrypted. If not, then Vuture will send the email normally. Some organisations only allow encrypted emails into their networks.

What to consider with a custom return-path?

Choosing your custom return-path

The first step to consider is to decide what you would like your custom return-path ought to be. You cannot use your root domain because you need to point that domain to our servers so that we can use it to send. You wouldn't be able to do this with your root domain.

We recommend choosing a subdomain off your root domain such as:

- e.domain.com
- marketing.domain.com
- emarketing.domain.com
- email.domain.com
- invite.domain.com

Once you have chosen this you will be able to replace any existing from addresses with this subdomain.

What you send from

When you send your emails, you can choose your display from address. If you don't intend on personalising your emails we suggest that you use an email address that incorporates your custom return-path e.g. event@e.company.co.uk. If you want to personalise your emails so that they come from named individuals you can use your root domain.

How you want to manage your replies

When you send emails from your custom return-path you want to make sure that you continue to receive auto-replies and any emails not sent to your designated reply-to address. You also want to make sure that you put a plan in place for anyone that emails your custom

return-path directly from their email client. If you send from your root domain, you don't need to worry about this step.

There are a few options that you can choose.

I. We can set up a rule to automatically forward emails in the format first.last@e.company.com to first.last@company.com. You can let us know the way we should map the replies.

II. We can forward specific From Addresses you have setup to other mailboxes, for example we could forward events@e.company.com and news@e.company.com to marketing@company.com. We can set up as many of these individual rules as you need.

III. We can forward any remaining emails that don't match and that don't look like bounces to a generic mailbox.

IV. You can setup mailboxes at your side using the custom return-path and have the replies be sent to those mailboxes.

Which authentication you want to setup

Though you don't need to setup all of the authentications listed in this document the more you setup the more likely you are to avoid deliverability issues in the future. At the very minimum we suggest SPF and DKIM.

Personalising emails

When you set up a custom return-path you will need to make sure that you only personalise by name rather than name and email when you send your emails. As far as your recipients will see they will see the Display name but the email will be your custom return-path.

Useful Links

We have some useful articles that go into how to set up a custom return-path along with some extra info for you.

How to setup a custom return-path

How to set up an approved domain

How to set up DMARC

Demystifying the DMARC Record from Return Path

What is a DMARC record and how do I create it on DNS server?

Frequently asked questions

Q: Can I have more than one custom return-path?	**A:** Yes. You can have up to 3.
Q: What happens if someone emails that custom return-path?	**A:** We can forward these emails to an email that you choose so that you don't miss any important emails.
Q: What if someone replies to a custom return-path?	**A:** We can forward these emails to a mailbox you choose.
Q: Why can't I have my own company name as the custom return-path?	**A:** It isn't best practice to use your company domain as the custom return-path. It reduces the level of risk using a subdomain. If you use your company domain and you end up on a blacklist you could cause wider problems for your business. We suggest keeping them different.
Q: What happens if I am already using a subdomain with another provider?	**A:** We suggest that you use a new subdomain as it is more straightforward. However, we can use the existing subdomain if you need us to. It will take more coordination and you will need to stop sending for a few days.
Q: How can I set up a custom return-path?	**A:** Get in touch with your Account Manager and they can guide you through the process.

If you want to know more, or you want to get a custom return-path please either get in touch with your Account Manager or drop an email to client.success@vutu.re

WRITTEN BY: Lili Boev Director of Client Success	CREATED ON: 31/10/201
	DOC REF.: VG1810

REVISION #	REVISION DATE	REVISED PAGE / SUMMARY
A	31/10/2018	Created