Brand Identity Protection: Optimise the deliverability of your mailings

Smart Guide

This Smart Guide helps you to improve the deliverability of your mailings. You can create the optimal conditions for ensuring that your emails actually reach the recipient and are not classified as spam by specifying the right settings in the *Brand Identity Protection* agent [1]. This way, you will strengthen your brand and your reputation as a sender.

Note: You authenticate a subdomain in order to optimise your deliverability. You will use the authenticated subdomain for sending your emails in Inxmail Professional. More information.

Three implementation scenarios

The factors listed above related to the deliverability of your mailings give rise to three different implementation scenarios for setting up your *Brand Identity Protection* agent. The scenarios depend on whether you only sign your own sender domain with DKIM or also opt for domain alignment and, finally, whether you delegate your sender domain to Inxmail.

Scenario 1 | Authentication & domain alignment (with domain delegation)

1. In Inxmail Professional, start the *Brand Identity Protection* agent.
2. Select the *Optimum deliverability (domain alignment)* option.
3. Select the *Delegate domain to Inxmail (recommended)* check box.
4. In the *Your domain* input field, enter the (sub)domain that you want to use as the sender and bounce domain.
5. In the *Email address for forwarding replies* input field, enter an email address. All replies to the mailings that you have sent will be forwarded to this address.

   The (sub)domain of the reply address should not match the previously entered sender or bounce domain.

   You must set up a mailbox of the same name with your ISP or email provider. This is where the replies to your mailings will go. After you have set up scenario 1, the replies to your mailings will no longer appear in the Inbox & bounces agent in Inxmail Professional. Instead, you will receive the replies directly in the inbox of your stored forwarding address. You can change and add reply and forwarding addresses at any time during operation, see here.
6. Click *Authenticate domain*.
7. The authenticate domain site appears.
8. The necessary steps have been completed in Inxmail Professional. You must now store the DNS entries with the ISP. More information.

Upgrade information for customers with sending domains that have already been stored: If you have already used an earlier version of the agent, you will not be able to upgrade to domain delegation. If you would like to use domain delegation, use a new sender domain. If you would like to use your previous subdomain for the domain delegation to Inxmail, please contact Support.

[1] HOW DOES THE AGENT HELP?

- Use *SPF (Sender Policy Framework)* to ensure that only authorised senders can send emails from your domain.
- Authenticate your senders with *DKIM (DomainKeys Identified Mail)* and ensure that the content of your emails cannot be tampered with.
- Use *DMARC (Domain-based Message Authentication, Reporting and Conformance)* to control what to do with dispatches from your domain for which authentication using SPF or DKIM fails.
- Use *BIMI (Brand Message Identification)* so that the recipient can recognise authenticated dispatches from your domain at first glance by your company logo.

[I] ADVANTAGES SCENARIO 1

Scenario 1 means that you have the least maintenance effort in the long term. You store DNS entries once and delegate the domain to Inxmail. Inxmail carries out any adjustments and you do not need to do anything if there are any changes to the domain entries in the future.

- All email authentication technologies are included: SPF, DKIM and DMARC. This domain is therefore protected against external misuse by cybercriminals. Prerequisite: The receiving mail server or spam filter interprets DMARC.
- A matching sender and bounce domain ('domain alignment') is rated by many Internet Service Providers (ISPs) as a positive characteristic when classifying emails.

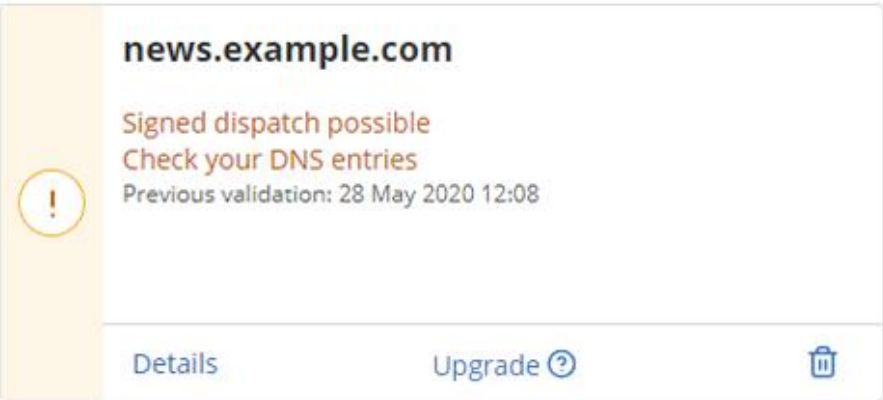
Scenario 2 | Authentication & domain alignment (without domain delegation)

1. In Inxmail Professional, start the *Brand Identity Protection* agent.
2. Select the *Optimum deliverability (domain alignment)* option.
3. In the *Your domain* input field, enter the (sub)domain that you want to use as the sender and bounce domain.
4. In the *Email address for forwarding replies* input field, enter an email address. All replies to the mailings that you have sent will be forwarded to this address.

   The (sub)domain of the reply address should not match the previously entered sender or bounce domain.

   You must set up a mailbox of the same name with your ISP or email provider. This is where the replies to your mailings will go. After you have set up scenario 1, the replies to your mailings will no longer appear in the Inbox & bounces agent in Inxmail Professional. Instead, you will receive the replies directly in the inbox of your stored forwarding address. You can change and add reply and forwarding addresses at any time during operation, see here.
5. Click *Authenticate domain*.
6. The authenticate domain site appears.
7. The necessary steps have been completed in Inxmail Professional. You must now store the DNS entries with the ISP. More information.

Upgrade information for customers with sending domains that have already been stored: If you have already used an earlier version of the agent and have not entered any bounce domains, you can upgrade your sender domain to domain alignment. If you have this constellation, an upgrade button will be displayed in the domain overview.



A dialog box with instructions will guide you through the further setup.

- Link tracking URL also points to the same domain (= 'full domain alignment').
- Authenticating your sender domain eliminates the need to display the Inxmail sender domain.
- Domain delegation makes it easier to maintain your domains. You only need to store so-called NS entries once with your ISP or DNS. Inxmail takes care of everything else for you, such as the maintenance of the DKIM keys.
- You can control your BIMI logo directly via XPRO without having to store a DNS entry with your ISP.

[I] ADVANTAGE SCENARIO 2

Differs from scenario 1 in the type of DNS entries. You use CNAME and TXT entries here. In practical terms this means that in the long run, you are responsible for maintaining and, if necessary, updating your DNS entries (= no domain delegation).

- All email authentication technologies are included: SPF, DKIM and DMARC. This domain is therefore protected against external misuse by cybercriminals. Prerequisite: The receiving mail server or spam filter interprets DMARC.
- A matching sender and bounce domain ('domain alignment') is rated by many Internet Service Providers (ISPs) as a positive characteristic when classifying emails.
- Link tracking URL also points to the same domain (= 'full domain alignment').
- Authenticating your sender domain eliminates the need to display the Inxmail sender domain.

Scenario 3 | Authentication of your sender domain

Important: In this scenario, you must manually specify many settings yourself. The changes should only be made by experienced IT/mail server administrators. If you set up things incorrectly, you risk damaging your reputation and this will affect your main domain or subdomain.

Why shouldn't I implement scenario 3?

If you implement scenario 3, it means that you are using a main domain to send your emails in Inxmail Professional. Or using a subdomain that you use outside of Inxmail Professional for other purposes.

It means that you use the same domain for different sources to send emails, such as: Newsletters, Transaction emails like order and invoice confirmations and/or your emails for daily business correspondence.

You can run into major problems with your reputation by mixing these things. For example, if a loss of reputation arises from sending your newsletters, this loss of reputation will also affect your emails for daily business correspondence.

On the other hand, if you differentiate the email types from each other, each domain builds its own reputation and the different sources to send emails do not affect one another.

Why is it so complicated and eror-prone to set up scenario 3?

There are many systems that send emails using your company name within the company. These include job portals, social media services and acquisition channels. These channels often exist in your company without the knowledge of your IT department. It is also referred to as shadow IT. Not all of these services sign your emails using DKIM, or even adhere to the other technical standards regarding deliverability.

If you want to implement scenario 3, you need to set the DMARC policy of your main domain to 'reject', or at the very least to 'quarantine'. To do so, you need to ensure that all systems sending emails using your company name adhere to your deliverability standards. This generally means that: you need to generate and evaluate complex XML reports in which you use the IP address to determine all programs and services that send emails using your company name. You need to communicate with third-party service providers and require them to sign your emails using DKIM and adhere to your deliverability standards.

This process is very involving and can take years depending on your IT infrastructure.

Conclusion: The easiest and most secure way of protecting your domain is to set up your own subdomain that you only use for Inxmail Professional. Implement either scenario 1 or scenario 2 to do so.

If you still want to set up scenario 3:

1. In Inxmail Professional, start the *Brand Identity Protection* agent.
2. Select the *Improved deliverability (use differing domains for sender domain (From) and bounce domain (Return-Path))* option.
3. In the *Sender domain (From)* input field, enter the (sub)domain that you want to use as the sender domain.
4. In the *Bounce domain (Return-Path)* input field, you can optionally enter a (sub)domain that you want to use as a bounce domain. In this way, you can avoid Inxmail sender domains such as inxserver.com or inxserver.de being shown in the technical email header.
5. Click *Authenticate domain*.
6. The authenticate domain site appears.
7. The necessary steps have been completed in Inxmail Professional. You must now store the DNS entries with the ISP. More information.

[!] ADVANTAGE SCENARIO 3

Please only use scenario 3 as an absolute exception. We do not recommend it. If you set up things incorrectly, you risk damaging your reputation and this will affect the domain you use.

- In this scenario you have the assurance that the SPF and DKIM technologies are included for email authentication. DMARC authentication is valid under certain circumstances, depending on how your domain outside of Inxmail Professional has been authenticated via DMARC. This must be checked by an experienced IT/mail server administrator. If set up correctly, your domain is protected against external misuse by cybercriminals. Prerequisite: The receiving mail server or spam filter interprets DMARC.
- Authenticating your sender domain eliminates the need to display the Inxmail sender domain.
- You have the option to use your main domain as a sending domain.
- You can use your sending domain (main domain or subdomain) outside of Inxmail Professional for other purposes.