

A wide orange banner at the top of the page containing faint icons of an envelope, a globe, and binary code.

How to Interpret Changes to AOL Authentication and Whitelist Standards

Recently AOL announced changes to how the company will authenticate inbound e-mail, in addition to changes to the company's whitelist program. In essence, these changes will reduce whitelisting to a process by which mailers will be asked to introduce themselves to AOL and provide information regarding the types of e-mail the mailer will be sending.

Simplified whitelisting process

In the future, AOL will ask mailers for two pieces of information: the domain and IP information for each mail stream, and the type of e-mail that is being sent via each mail stream. This information will then be entered into AOL's reputation system. Delivery issues will only occur if the type of e-mail being sent differs greatly from what is expected in a given mail stream.

IP addresses that are currently whitelisted with AOL will be subject to this new process for determining reputation. There is no need to reapply. It is also AOL's belief that few if any current IP addresses will be affected by these changes, since reputations are typically within guidelines.

DKIM implementation

AOL is now using domain keys identified mail (DKIM) for authentication, joining Yahoo and Google as the three major North American ISPs that have implemented DKIM. Like other authentication platforms, DKIM does not guarantee delivery; it simply authenticates that the e-mail is from the domain it claims as its origin.

However, it does mean mailers will be required to take into account both IP and domain reputation. AOL and the other major ISPs will be weighing all available information – domain, IP, URL, and more – before making a delivery decision on a given message.



What do these changes mean to you?

These changes will have little impact on clients that adhere to good e-mail marketing practices. It means your reputation is already first-rate in the eyes of AOL and other major ISPs. Maintaining sound delivery metrics (e.g. bounces, complaints, traps) will ensure high deliverability no matter what changes the ISPs make.

What these changes do indicate, however, is a major shift towards emphasizing IP reputation, with authentication as a key variable. As your ESP, e-Dialog has plans to implement DKIM with clients that meet the criteria. If we are currently signing domain keys, you qualify. If you are still sending e-mail from ed10.net we cannot authenticate with DKIM or Sender ID, and we recommend that you move to your own marketing subdomains with the help of your e-Dialog account teams.

If you have any questions regarding these changes or would like additional information regarding DKIM please contact Rick Buck, director of privacy and ISP relations, at rbuck@e-dialog.com or contact your e-Dialog account team.