IP and Domain Whitelisting
External Comms

NEWSWEAVER
powering communications

Version 1.7_external_emea

Author: Ian Kenefick

Last Modified: 11 March 2016

Revision History

Version	Author	Comment	Date Modified
1.0	IK	Initial Version	17 July 2013
1.1	IK	Updated Range	02 June 2014
1.2	IK	Additional Considerations	11 July 2014
1.3	IK	Updated IP Addresses	24 September 2014
1.4	IK & DE	Peer Review	25 September 2014
1.5	IK	Updated IP Addresses	14 October 2014
1.6	AW	Updated Domains	22 May 2015
1.7	DE	Remove old IPs (84.45.11.*)	11 March 2016

What is ‘whitelisting’?

The process of identifying mailservers as trusted to guarantee delivery of messages from Newsweaver.

Who is whitelisting for?

Whitelisting is highly recommended for 'internal publications' or in situations where proactive measures to guarantee deliverability can be taken.

Why is whitelisting necessary?

Newsweaver follows best practices regarding email authentication, however there are occasions that a Anti-SPAM software may block messages from our servers. In this case, a whitelist is used to identify the sender as 'trusted' and permits the messages to pass through.

Who should I ask to do this whitelisting?

Your IT department will know how to do this, just pass on this document to them.

Instructions for your IT Department

Please mark the following IP ranges and domains as safe in order to enable Newsweaver to deliver to your employees:

IP Range in CIDR Notation	Envelope Domains to be Whitelisted
5.61.115.0/24	• nw001.com • nw002.com • nw005.com • nw007.com • nw008.com

Additional Considerations

Multi-Layer SPAM filtering

Whitelisting at The Edge
Most companies employ SPAM filtering at the edge, whether this is within the corporate IT infrastructure or using a third party such as Postini, MessageLabs, MIMECAST, ProofPoint etc. Whitelisting should always be implemented at the edge to ensure that messages arrive in a timely fashion and are not misclassified as SPAM.

Whitelisting Internal Mail Servers
Email servers such as Microsoft Exchange (which are located behind the edge) provide additional SPAM filtering. Where applicable, whitelisting should be employed at this layer and any layer thereafter where filtering might occur.

For example, in Microsoft Exchange, adding the Newsweaver IP addresses to the **“IP-Allow list”,** ensures inbox placement of the message by giving the message a **SCL (Spam Confidence Level) score of -1**. Outlook clients interpret this and place the email in the inbox - Overriding Outlook’s local SPAM filter.