

microsoft.public.exchange2000.transport: RE: No IP address logging on internal email.

RE: No IP address logging on internal email.

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.transport/2004-10/0020.html>

From: Darin Roulston [MSFT] (*darinr_at_online.microsoft.com*)

Date: 10/07/04

Date: Thu, 07 Oct 2004 16:27:00 GMT

Hi Scott,

The behavior you are seeing is normal. The headers you describe are SMTP headers meaning that every SMTP host that a message passes through will stamp it's IP address. This includes the originating machine if the client sends via SMTP. However when you are sending with a MAPI client to someone the same server MAPI doesn't add anything to the SMTP header. There is no option to make MAPI write SMTP headers as they are two entirely different entities (it doesn't make an SMTP 'hop'). In a MAPI environment (Corporate mode) you rely on the NT permissions to lock down who can send as who. If the messages are being sent with Outlook in MAPI mode, which it sounds like they are, then someone would have to either know the mailbox owners NT password or perhaps the user left their workstation unlocked. I would review your password complexity/duration policy and remind folks not to leave workstations unlocked while away, paying special priority on those that have been already compromised. One other possibility is someone with "Send-As" permission is sending-as these users, so check mailbox rights. Also anyone with send-as/receive-as permission on the mailbox database in question would be able to open the mailbox of anyone in that store (no such accounts by default). You can turn up Mailbox Logons under diagnostic logging to give you more information on someone logging in to someone else's mailbox because they have been given permission to.

hth

Darin Roulston
Microsoft

--

Get Secure! - www.microsoft.com/security

--

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.

--

This posting is provided "AS IS" with no warranties, and confers no rights.

=====

Content-Class: urn:content-classes:message
From: "Scott Phillips" <confirm@corn-bread.org>
Sender: "Scott Phillips" <confirm@corn-bread.org>
Subject: No IP address logging on internal email.

RE: No IP address logging on internal email.

microsoft.public.exchange2000.transport: RE: No IP address logging on internal email.

Date: Thu, 30 Sep 2004 15:28:40 -0700
Lines: 28
Message-ID: <1d2401c4a73c5d5d307f05a401280a@phx.gbl>
MIME-Version: 1.0
Content-Type: text/plain;
 charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Newsreader: Microsoft CDO for Windows 2000
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4910.0300
Thread-Index: AcSnPNXTnUU3vpy2T2yg0crYS1510Q==
Newsgroups: microsoft.public.exchange2000.transport
Path: cpmsftngxa06.phx.gbl
Xref: cpmsftngxa06.phx.gbl microsoft.public.exchange2000.transport:6642
NNTP-Posting-Host: tk2msftngxa12.phx.gbl 10.40.1.164
X-Tomcat-NG: microsoft.public.exchange2000.transport
I am running exchange server 2000 (with service pack 3) on
a windows 2000 server (with service pack 4).
Here's the deal: I need to track down which workstation
is sending some messages. I have the offending emails in
my possession. When I look at the headers, it shows the
name that send the email. However it does not show the IP
address of the machine that submitted the email. This
ONLY happens when sending email directly to the mail-store.
Other IP addresses are logged (if an email is received
from an external user, then the IPs will be there). And,
if I configure outlook to send email to the exchange users
via SMTP (as opposed to using the exchange MAPI protocols)
then the internal IP is logged. But if that email is sent
via the exchange mail-store, nada.
The bottom line: I want to be able to look at the headers
(or search by message ID) and see which local workstation
submitted a given email, whether that email was submitted
via smtp or the mail-store.
How do I turn this functionality on?
Thanks.
Scott.
confirm@corn-bread.org