



Description: This document contains security-related information pertaining to the AlarmWorX32 MMX Email Agent

General Requirement: AlarmWorX32 Multimedia and an email client must be installed on the server machine. Please contact your IT department to configure security for your email system.

Email Agent Security

1) What is the best method of implementing security with the email client?

Answer: The MMX email agent requires no additional security settings if the existing email system is secure. It uses the default email client on your computer to send and receive all emails. For example, if all emails are sent and received using the same Microsoft Exchange server, then each connection to the Exchange server will be secure if properly configured on the Exchange server. Exchange provides secure connections, however the email sent over that connection is unencrypted.

If client-side encryption is required then this can be configured in Outlook under the "Tools/Options\Security" menu. Another example of a program that offers email encryption is PGP.

Answer: The risks of using unencrypted, unsecured email depend upon the sensitivity of the information being sent through the emails. Unencrypted emails can easily be "sniffed" and intercepted by malicious programs or persons. The repercussions of this depend completely upon the contents of the emails, but in general it is a good idea to use security so that these emails do not fall into the wrong hands.

The advantage to not using security would be a possible increase in the performance of the email system since it does not have to do the extra work associated with security.

3) How will the LAN traffic be affected when alarms are sent out using the email agent?

Answer: The effect of using the MMX email agent upon LAN traffic will vary greatly depending upon the volume of emails that are sent. The more alarms that occur on the system the more emails will be sent from the email agent, and thus greater network traffic will result. This can be avoided by using filters in the MMX Server to only send emails for a subset of alarms. The best way to determine the effect of sending emails on your network is to conduct some tests using the email agent. Try to estimate the maximum number of alarms that will occur on the system. Start out by triggering only a few emails per minute, and then increase the frequency until you have either reached the estimated maximum or a point at which the network traffic becomes unacceptable. If necessary, try to limit the number of alarms that trigger emails by filtering out a subset of alarms.

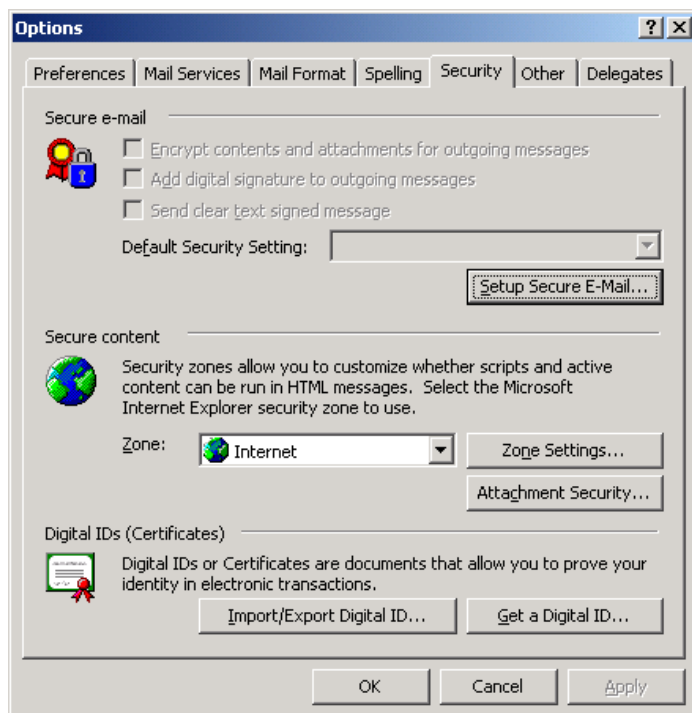


Fig. 1 MS Outlook Security Settings

2) What are the security risks with email clients and using the MMX email agent?