



## ***WASP: Protecting GroupWise from Viruses through WebAccess***

GroupWise WebAccess has been an extremely popular feature of GroupWise since it was introduced in 1994 in GroupWise 4.1. The ease of being able to access your GroupWise anytime and anywhere has contributed to its popularity. Some organizations however, concerned about security, have hesitated in deploying GroupWise WebAccess to their mobile users. The main concern has been the inability to ensure that remote desktops uploading files have adequate Anti-Virus protection. Without adequate Anti-Virus control on the desktop, it is possible for email attachments uploaded through WebAccess of being infected with a virus.

Anti-Virus protection for GroupWise generally occurs in three places. First, the SMTP Gateway, where the majority of email passes into your GroupWise system, second the MTA where GWAVA monitors GroupWise traffic passing through the GroupWise system, and third, at the desktop, where anti-virus software scans as email attachments are opened.

For many organizations, it is the inability to control the desktop of remote users that cause them to worry about GroupWise WebAccess inadvertently allowing a virus to enter in the GroupWise system. GroupWise WebAccess is the web interface that allows mobile and deskless users to access their GroupWise Email and Calendar from any remote computer.

Often the computers used to access WebAccess exist outside an organization's control. They are located in homes, kiosks, airports, or other far flung locales. When WebAccess is used in this manner, any email attachments involved by-pass all the normal defenses for anti-virus protection for GroupWise. WebAccess by-passes the SMTP gateway, it by-passes the MTA running GWAVA, and it is often not scanned by the desktop uploading the file because it is often a home machine or a public kiosk. This means that an infected email attachment is delivered directly into your GroupWise database, waiting to be sprung open by an unsuspecting end-user.

WASP from GWAVA is the first and only solution that monitors incoming WebAccess attachments and scans them before they enter into your GroupWise system. WASP resides on the WebAccess server and acts as a defense against this open hole in your security.

The majority of GroupWise systems that use WebAccess run WebAccess on the NetWare platform. To ensure that a WebAccess user does not send a virus into your GroupWise system, you run WASP on the NetWare web server. You need WASP because most virus-protection agents that run on NetWare only scan files that come in through a web server.

This is why WASP is needed:

- You have a NetWare 6 server running your WebAccess Application.
- The server is running an Anti-Virus agent
- A user logs in and attaches a file to a message. The file has a virus. It's placed by the WebAccess Application on the WebAccess server while the user composes their message.
- The A/V agent isn't even aware of the virus, when the user clicks on send, the virus is in your GroupWise system.

Many GroupWise Administrators have implemented A/V solutions. WASP is able to work with many of these A/V solutions so that you don't need to buy more A/V products.

WebAccess is an incredibly powerful tool, and those companies that have resisted using it have been aware of the loss of productivity that they have placed on their workers. But now, with WASP from GWAVA, every GroupWise customer can deploy GroupWise WebAccess in confidence, knowing that each email attachment coming in through the WebAccess Gateway is protected from Viruses, keeping the GroupWise clean and safe.