Avaya Modular Messaging 3.x

Security Updates, Operating System Service Packs, Virus Protection, Avaya Modular Messaging Service Packs, and Third Party Software for Modular Messaging 3.x

Issue 1.4
November 1, 2007

Microsoft Windows Security Updates for the Messaging Application Server (MAS)

Microsoft issues Windows Security Updates as needed. These updates should be applied to the MAS as soon as they become available. Avaya communicates these security updates via the Avaya Security Advisory process. These are posted on the Avaya Support site, http://support.avaya.com, and customers can subscribe to receive automatic notification. It is the customer's responsibility to install the Windows Security Updates on the MAS.

Security Advisories that might effect Avaya products as well as "Avaya's Product Security Vulnerability Response Policy" and "Avaya's Security Vulnerability Classifications" are found on the Avaya Support site at:
http://support.avaya.com/japple/css/japple?PAGE=avaya.css.OpenPage&temp.template.name=SecurityAdvisory

Avaya will assist in finding solutions to problems that might arise from applying a security patch from Microsoft. Beginning November 2007, Avaya will no longer maintain the security patch master list for Modular Messaging. Refer to Product Support Notice (PSN) 1639U for Modular Messaging R3.0 and PSN 1642U for Modular Messaging R3.1 located on the Avaya Support site to determine which Microsoft security patches have been installed by Avaya.

Microsoft Windows 2003 Service Pack Updates and Releases for the MAS

Maintaining compatibility between Microsoft Windows service packs and Modular Messaging is a primary objective of Avaya. Microsoft Windows 2003 service packs for the Modular Messaging MAS must be certified by Avaya. The certification communication is done via the Product Support Notice (PSN) process and customers can receive automatic notification by subscribing on the Avaya Support site. Avaya will issue a PSN within 90 days of a Microsoft service pack becoming Generally Available that will provide details as to when it will be compatible with specific Modular Messaging releases. Upon certification, customers must obtain and install the service pack directly from Microsoft due to Microsoft's licensing rules.

New Microsoft Windows releases must also be certified by Avaya. New Microsoft OS releases are certified with a new release of Modular Messaging.

Microsoft Exchange, Office, Windows XP Service Pack Updates and Releases for Modular Messaging

Avaya must certify Microsoft service packs for Microsoft products which are required for Modular Messaging components such as the plug-in clients, thin clients, and Exchange message store. These Microsoft products include Exchange, Office, and Windows XP. Certification communication is done via the Product Support Notice (PSN) process and customers can receive automatic notification by subscribing on the Avaya Support site. Avaya will issue a PSN within 90 days of a Microsoft service pack becoming Generally Available that will provide details as to when it will be compatible with specific Modular Messaging releases. Upon certification, customers must obtain and install the service pack directly from Microsoft due to Microsoft's licensing rules.

Microsoft product releases must also be certified by Avaya. Typically, new Microsoft product releases are certified with a new release of Modular Messaging.

RedHat Linux Security Updates for the Message Storage Server (MSS)

RedHat issues Linux Security Updates as needed. Avaya provides Linux OS security updates or service packs via an Avaya Modular Messaging Service Pack. It is the customer's responsibility to update the MSS. These updates should be performed as soon as they become available. Avaya communicates these security updates via the Avaya Security Advisory process. These are posted on the Avaya Support site and customers can subscribe to receive automatic notification.

Security Advisories that might effect Avaya products as well as "Avaya's Product Security Vulnerability Response Policy" and "Avaya's Security Vulnerability Classifications" are found at: http://support.avaya.com/japple/css/japple?PAGE=avaya.css.OpenPage&temp.template.name=SecurityAdvisory

RedHat Linux Service Pack Updates for the MSS

Avaya provides any Linux OS updates or service packs via an Avaya Modular Messaging Service Pack. Avaya communicates the availability of service packs via the PSN process. These are posted on the Avaya Support site and customers can subscribe to receive automatic notification.

Avaya Service Pack Updates for the MAS and MSS

Service Packs (SPs) are made available from Avaya on a regularly scheduled basis. SPs for the MAS and MSS may be downloaded from the Avaya Support site at: http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=151670&temp.releaseID=287076&temp.bucketID=108025

A list and description of SPs is also available via the above link. Avaya communicates the availability of Modular Messaging SPs via the PSN process. Customers can register for automatic notification on the Avaya Support site. Depending on the size of the SP, it may not be downloadable in which case the PSN will define how to obtain the SP.

Virus Protection for the MAS

It is the customer's responsibility to procure, install and keep current any virus protection software on the MAS. Avaya allows generally available third party anti-virus software to run on the MAS, however, Avaya will not provide support for installation of the anti-virus software or the ongoing maintenance of that software. Customers are responsible for any undesired interactions between the anti-virus software and the MAS.

While Avaya has performed interoperability testing with McAfee VirusScan Enterprise Edition, Symantec Antivirus Corporate Edition, and Trend Micro OfficeScan Corporate Edition, Avaya does not certify these vendors nor endorse their products. Customers should verify that they use the correct edition of anti-virus software pertinent to the product.

Recommendations Regarding Installation and Use of Anti-Virus Software

Disable anti-virus software during installation of Avaya messaging products

It is best to install anti-virus software only after the Avaya messaging products are installed. If anti-virus software is already installed prior to installing any Avaya messaging application, be certain to disable the anti-virus software before proceeding, and do not re-enable it until after the installation is complete and the correct operation of the Avaya product has been verified.

Scanning Cautions

Consider the impact that anti-virus scanning may have on the performance of the Avaya messaging servers prior to scanning for viruses in a certain way. Many anti-virus software products provide both 'on-access' scanning, and 'on-demand' scanning. For example, 'on-access' scanning performs a scan anytime a file changes for any reason. This type of scan may have a negative impact on the relative server performance. As such, Avaya recommends the use of 'on-demand' scanning, where scans are run on scheduled intervals. It is not recommended to employ any message scanning that could drastically impact the performance of the Avaya servers.

Anti-Virus Software Administration

When administering the anti-virus software, set it up to scan the hard disk once per week. There is little impact on performance when the scan runs, but it is still best to have the scan run during off peak hours. If desired, it is also acceptable to run the anti-virus scan every day, but still pick an off peak time to run the scan. In the case of Avaya Modular Messaging where multiple MAS servers are used, it is also acceptable to run the anti-virus scan on each system at the same time. Note that it is best to avoid scheduling the anti-virus scan at the same time as when a backup occurs on the MAS (which by default is 11pm every night). If a virus is found in a file then the anti-virus software should be set to attempt to clean the file first, and if that fails, to move the file to a different directory.

Some anti-virus software applications default to scan on startup. This feature should be disabled or it will interfere with the time that it takes a system to come back online after a reboot.

It is further recommended to schedule virus definition updates to automatically occur at least once per week. The updates should occur before the next scheduled scan time to ensure the latest DAT files are used during the scan, but updates should be avoided during a virus scan. Setting virus definition updates to occur every day is also acceptable.

Port Blocking
Some anti-virus software products have additional functionality to block unwanted traffic on specific TCP/IP and UDP ports. Refer to the LAN port usage document to understand which ports should not be blocked. The LAN port usage document is located on Avaya's Enterprise Portal – please contact your Avaya Representative or Authorized BP to obtain this document.

Third Party Monitoring and Administration Software for the MAS

Avaya allows third party software to run on the MAS for monitoring the health and performance of the installed Operating System and to allow network administrators to perform basic clerical activities such as asset tracking; however, Avaya will not provide support for installation of the software or the ongoing maintenance of that software.

In addition, Avaya allows customers to create additional monitors against the Windows Application Events and Performance Counters generated by MM but will not provide documentation for this or enable additional methods for accessing any of the MM operation information. Avaya will not provide any assistance in the development of these monitors or be responsible for the accuracy of the data obtained.

The customer is responsible for maintaining any third party software packs installed for either the Operating System or the Application and is responsible for the integrity of the pack(s) by incorporating any changes Avaya has made to the MM application or the source data made available by the MM application. Avaya makes no obligation to inform the customer that changes have been made to the Windows Application Events or Performance Counters.

The customer agrees not to use third party software to manipulate, recover or in any other way interfere with the operation and/or recovery of the MM application. Any attempt to do so may result in a period of non-operation or total system outage. The cost of returning the system to working order following this or any other unauthorized use of the third party software will be the customer's responsibility.

At any time where it is demonstrated or suggested that the use of third party software is impacting the operation or performance of the MM application, Avaya will request its removal and the customer agrees to remove or permanently disable the software immediately.

Third Party Patch Management Software for the MAS

Avaya allows third party patch management software to run on the MAS for deployment and loading of Microsoft patches, anti-virus updates, and monitoring software. However, Avaya will not provide support for installation of the patch management software or the ongoing maintenance of that software. Customers should review the Microsoft Security Patch and Service Pack updates of this section prior to use of this type of software.

Third Party Software for the MSS

Avaya does not allow third party software on the MSS.

DISCLAIMERS AND NOTICES

ALL INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS". AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE USE OF THIRD PARTY SOFTWARE WILL ADEQUATELY MONITOR THE HEALTH AND PERFORMANCE OF CUSTOMER'S SYSTEMS OR ELIMINATE SECURITY OR VIRUS THREATS. THE CUSTOMER'S DECISION TO ACQUIRE OR USE SUCH THIRD PARTY SOFTWARE IS THE CUSTOMER'S SOLE RESPONSIBILITY. AVAYA IS NOT RESPONSIBLE FOR, AND WILL NOT BE LIABLE FOR, THE QUALITY OR PERFORMANCE OF SUCH PRODUCTS OR THEIR SUPPLIERS.