



Policy for Loading Third-party Anti-virus Software on S8100 Media Servers, IP600 Communications Servers, & DEFINITY ONE[®] Communications Systems

Abstract

This paper provides general guidelines and policies for the use of anti-virus software on the S8100 Media Server, IP600 Internet Protocol Communications Server, and DEFINITY ONE[®] Communications System. In general, Avaya does not guarantee protection of its products against network attacks such as viruses or worms when anti-virus software is installed. Furthermore, the interoperability and impact of anti-virus software with Avaya products is unpredictable and known to cause system degradation in some instances. Avaya does not recommend the use of anti-virus software on real-time communications products.

Table of Contents

1. Introduction.....	3
2. Policy Changes.....	3
3. General Policy.....	3
4. Interoperability with Specific Anti-virus Packages	4
McAfee NetShield Anti-virus	4
5. Special Handling Notes.....	5
6. Conclusion	5

1. Introduction

In light of the ongoing vulnerabilities and exploits of the Microsoft Windows™ operating system, Avaya feels it is important to clarify the risks associated with introducing anti-virus software into the S8100 Media Server, IP600 Internet Protocol Communications Server, or DEFINITY ONE® Communications System. Avaya takes security seriously and is working on solutions that provide the utmost in reliability and security. The introduction of anti-virus software alone, in some instances, may provide a false sense of security or cause serious undesirable side affects.

2. Policy Changes

Avaya is conducting ongoing anti-virus software policy work that covers all Avaya products. This policy applies solely to the aforementioned products that run the Windows operating system and may be superseded by newer global policies issued by Avaya.

3. General Policy

Avaya cautions against loading any third-party anti-virus software on S8100 Media Servers, IP600 Internet Protocol Communications Servers, and DEFINITY ONE® Communications Systems. However, due to the current industry focus on security issues, Avaya understands that in some cases customers may choose to do so. The loading of any additional third-party software beyond anti-virus software will violate the bounds of the maintenance agreement.

The loading of the anti-virus software will be the sole responsibility of the customer. It does not require any update to the operating system unless stated by the software vendor. This can include Microsoft Service Packs and/or Microsoft updates.

It is highly recommended that the customer run the Microsoft Security Baseline Analyzer, which can be obtained from Microsoft, before loading any anti-virus software. This helps improve the overall security of the system (on R10 and later systems, this software is included).

Customers should understand that the anti-virus software can compromise the stability of the S8100 Media Server, IP600 Internet Protocol Communications Server, or DEFINITY ONE® Communications System and that Avaya has communicated that risk through this policy.

If an issue arises with the platform, the first step in troubleshooting is to remove the anti-virus software. Removal of anti-virus software is the sole responsibility of the customer. Therefore, Avaya engineers troubleshooting issues on systems with anti-virus software will request the removal of this software before troubleshooting proceeds.

If the anti-virus software corrupts the overall operation of the S8100 Media Server, IP600 Internet Protocol Communications Server, or DEFINITY ONE® Communications System, Avaya is not responsible for that repair within the bounds of the maintenance contract. Any and all fees will be charged in re-provisioning and/or reinstalling the solution.

Avaya offers a variety of products and services to assist in maximizing the security of each individual communication system. These software products and services can be customized depending on individual voice, data, and multimedia needs and policies. Avaya Security Services can be contacted at <http://www.avaya.com/security>

The customer is responsible for the security of their systems to prevent unauthorized access.

The customer is responsible for the security of their networks, which includes configuration of the network to prevent propagation of virus, worms, denial-of-service, and other network-based threats.

The customer is responsible for reading all installation, instructional, system administration and maintenance documents provided with each product so as to fully understand those features that can introduce security violations, such as unauthorized access, and the steps that may be taken to reduce that risk.

It is recommended that the customer implement their own corporate security policies on all Avaya products; this includes physical and virtual security to the Avaya systems.

Avaya does not provide assistance on loading of anti-virus software nor does Avaya provide suggested anti-virus vendors. Avaya has tested a number of vendors' anti-virus software and can provide the results of that testing for informational purposes only.

4. Interoperability with Specific Anti-virus Packages

Avaya's testing of a particular anti-virus package provides no endorsement of any anti-virus software vendor.

As Avaya tests anti-virus software packages, information about basic interoperability will be made available through ongoing documentation.

Interoperability testing does not guarantee or certify any level of reliability from a support or maintenance perspective.

McAfee NetShield Anti-virus

Avaya's testing of software by a specific vendor does not imply that Avaya recommends or advocates software by any particular vendor.

Avaya has performed basic interoperability testing with McAfee NetShield Anti-Virus 4.5.1 SP1, Virus definitions 4.0.4267, and scan engine 4.2.40. This testing occurred on an S8100 Media Server running Communication Manager 1.3. Further testing was performed on a DEFINITY ONE[®] Communications System running Release 9.5 software.

Testing with 3,000 busy hour calls (medium to heavy call traffic) has shown that anti-virus scanning of all files on the hard drive has a **severe detrimental impact to call processing** for at least 5 to 10 minutes while certain files are scanned. Scanning of all files takes roughly one hour on the system. For this reason, scanning of all files is not recommended unless the customer has at least one hour of very low call volumes at a consistent time every day or every week when scanning can be completed. Testing with very low activity and call volumes on the system did not show negative impact to the system while scanning was performed.

5. Special Handling Notes

To help Avaya Technical Support diagnose problems, knowledge of the presence of anti-virus software will be included in support and maintenance records.

The following special handling notes are added to the maintenance records of any customer that chooses to install third-party anti-virus software.

1. Primary customer contacts with e-mail addresses.
2. Avaya Tier IV contact and Tier III SME contact (if applicable).
3. The following text: “[Customer] will be loading anti-virus software on to the [Avaya Product] and will be responsible for the application of the software and the communication of the anti-virus”.
4. The following text: “[Customer] understands the risk and indemnifies Avaya from failure of the system if caused by the third-party software”.
5. The following text: “[Customer] understands that billing charges do apply if any assistance is needed in troubleshooting issues that may have been caused by the third-party software”.

If Avaya is asked to troubleshoot an issue on a system that has anti-virus software installed, the first step in troubleshooting the issue is to remove the anti-virus software.

6. Conclusion

Avaya understands and acknowledges the desire to install anti-virus software on Avaya products and is providing this policy for guidance in this area. In general, a customer may decide, at their discretion, if anti-virus software is an appropriate measure to protect their communication system. If the decision is made to install anti-virus software, the customer takes responsibility of support and maintenance of that software and the impact it has on the operation of the S8100 Media Server, IP600 Internet Protocol Communications Server, or DEFINITY ONE[®] Communications System.

©2003 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.