



Release Notes for Cisco Spam & Virus Blocker 6.6.1 Release

Revised: May 20, 2009, OL-19704-01

Contents

The Cisco Spam & Virus Blocker release notes contain the following sections:

- **Introduction.** This section introduces the Cisco Spam and Virus Blocker. See [Introduction, page 1](#).
- **Upgrading to a New Release.** This section describes details relevant during product installation. See [Upgrading to a New Release, page 1](#).
- **Caveats.** This section discusses the fixed and known caveats in this release. See [Caveats, page 2](#).
- **Related Documentation.** This section references other documentation that may be helpful in running and installing the Cisco Spam and Virus Blocker. See [Related Documents, page 5](#).
- **Service and Support.** This section provides information on obtaining service and support for your Cisco Spam & Virus Blocker. See [Service and Support, page 6](#).

Introduction

The Cisco Spam and Virus Blocker is a high-performance appliance designed to eliminate spam and viruses, enforce corporate policy, secure the network perimeter, and reduce the Total Cost of Ownership (TCO) of your email infrastructure.

The Blocker combines hardware, a hardened operating system, application, and supporting services to produce a server appliance dedicated for messaging, spam and virus protection.

Upgrading to a New Release

Upgrade Instructions:

For the 6.6.1 release, please use the following instructions to upgrade your Blocker appliance.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

1. Save the XML configuration file off the Blocker appliance or email the configuration file to yourself.
2. If you are using the Safelist/Blocklist feature, export the Safelist/Blocklist database off the Blocker appliance.
3. From the System Administration tab, select the System Upgrade page.
4. Click the **Available Upgrades** button. The page refreshes with a list of available upgrade versions.
5. Select the appropriate upgrade version.
6. Click the **Begin Upgrade** button and your upgrade will begin. Answer the questions as they appear.
7. When the upgrade is complete, click the **Reboot Now** button to reboot your Blocker appliance.

New and Changed Information

This release contains no new features, but contains some critical bug fixes listed below.

Installation Notes

Please read the following installation notes prior to upgrading to the latest version of the Cisco Spam & Virus Blocker.

Important Note

The Cisco Spam and Virus Blocker uses a self-signed certificate. This certificate may trigger a warning from your web browser. However, the Blocker is secure and you can ignore these warnings. Accept the certificate when you run the installation.

Upgrade Paths

The following upgrade paths are supported:

From: 6.6.0-202 To: 6.6.1-016

From: 6.6.1-014 To: 6.6.1-016

Caveats

The following section describes opened and closed caveats for the Blocker 6.6.1 release.

Open Caveats - Blocker Release **6.6.1**

The following table shows open caveats for this release:

Table 1 Open Caveats

Cisco Spam and Virus Blocker 6.6.1		
DDTS Number	Corrected	Caveat
CSCsv83766	No	<p>Virus counts are sometimes inconsistent if the virus email is also categorized as spam</p> <p>Message counts displayed in the Virus Types pages can appear inconsistent when the message is categorized as both spam- and virus- infected. For more details, refer to the user documentation.</p>
CSCsv83797	No	<p>Verdict cache sometimes includes emails with blank Subject or Body headers.</p> <p>Sometimes emails with blank subject and body are treated as spam.</p>
CSCsv83815	No	<p>Paused upgrade hangs and does not complete</p> <p>When the upgrade process (System Administration > System Upgrade) shows a progress bar with a fixed percentage and increasing completion time, it can be due to failed network connection. If this occurs, perform a system reboot from the UI (System Administration > Shutdown) and restart the upgrade.</p>
CSCsv83821	No	<p>The Active Directory Wizard does not work with Active Directory configured for encrypted connections</p> <p>If your Active Directory is configured for encrypted connections, you cannot configure connections to it using the Active Directory wizard.</p>
CSCsv83836	No	<p>In the System Setup Wizard, the system test performs slowly when multiple MX entries are found for a specific domain</p> <p>The System Test takes longer to complete for a domain that has multiple MX entries. Allow for extra time when testing a domain with multiple MX records.</p>
CSCsv83866	No	<p>System Test appears to erroneously display a successful status when LDAP setting are misconfigured.</p> <p>Misconfiguration in LDAP settings cannot be detected by the System Test. Therefore, if a mail is dropped due to LDAP misconfiguration, no error message is shown. You can test LDAP configuration from System Administration > LDAP > Add LDAP Server Profile.</p>
CSCsv83895	No	<p>Active Directory Wizard does not support multiple Active Directory Server configurations</p> <p>Currently the Active Directory wizard supports a single Active Directory server configuration. To configure multiple Active Directory servers, go to the System Administration > LDAP configuration page.</p>

Table 1 **Open Caveats**

Cisco Spam and Virus Blocker 6.6.1		
DDTS Number	Corrected	Caveat
CSCsv83909	No	System Test shows “Pass” even if TLS negotiation fails. The System Test feature does not verify TLS negotiation failures. One way to tell if a TLS failure occurred is to check for the “Welcome” email in your inbox after configuring the Blocker. If a TLS negotiation failure occurred, the test email delivery will have failed.
CSCsv83918	No	The default Alias Consolidation LDAP query returns the most recently created alias rather than the primary Exchange address By default, Spam quarantine notification emails are sent to the most recently created alias rather than to the primary email address configured on Exchange. A workaround is to specify email attributes in the order of “mail, proxyAddresses” in Active Directory (this ensures that notifications are sent to primary email address).
CSCsv83933	No	Expired Anti-spam feature key causes mail queue to pause If the Anti-spam feature key expires, the Anti-Spam engine will stop (resulting in a halted mail queue). Updating the feature key will resume mail flow.

Resolved Caveats - Blocker Release 6.6.1

The following table shows resolved caveats for this release:

Table 2 **Resolved Caveats for Cisco Spam & Virus Blocker 6.6.1**

Cisco Spam and Virus Blocker 6.6.1		
DDTS Number	Corrected	Caveat
CSCsz79323	Yes	Fixed: IronPort Spam Quarantine Allows Scripting Fixed an issue in which the IronPort Spam Quarantine didn't sufficiently encode JavaScript. This is now implemented.
CSCsz76874	Yes	Fixed: Invalid Bounce Message Not Rejected Fixed an issue in which an invalid bounce message was accepted, and the corresponding mail logs did not flag the message as bounced. This issue has been resolved.
CSCsz79300	Yes	Fixed: OpenSSL Security Advisory Applied a patch included in the following OpenSSL Advisory: http://www.openssl.org/news/secadv_20090325.txt

Table 2 *Resolved Caveats for Cisco Spam & Virus Blocker 6.6.1*

Cisco Spam and Virus Blocker 6.6.1		
DDTS Number	Corrected	Caveat
CSCsx40945	Yes	Fixed: Application Error Occurs When One of Two DNS Servers Goes Down Fixed an issue in which application errors occurred when one of two DNS servers configured in the System Setup Wizard went down.
CSCsx08229	Yes	Fixed: A DNS Bootstrap Reply Prevents DNS Lookups on Email Security Appliances Previously, a DNS bootstrap reply prevented DNS lookups on Email Security appliances while requesting nonauthoritative DNS servers. This issue has been resolved.
CSCsx08238	Yes	Fixed: Next Policy Quarantine Page Not Displayed Fixed an issue in the GUI where AsyncOS displayed a “page not found” error if you clicked the link for the “Next” page or any of the following pages in the Policy Quarantine.
CSCsx32197	Yes	Fixed: Address Duplication in Notification URL Prevents Safelist/Blocklist Updates Previously, some users could not add email addresses to their safelist or blocklist or delete them from these lists, if they accessed the End User Quarantine from a link in a notification email. This was due to the email address being repeated in the link’s URL. The duplication of email addresses in the URL occurred because of duplicate addresses in the LDAP cache table. This issue has been fixed. Now, the URL does not include duplicate addresses.
CSCsv83861	Yes	Fixed: End User Quarantine Options List Fails to Open Fixed an issue in which the Options list of the End User Quarantine failed to open when clicked on.
CSCsx32150	Yes	Fixed: Systems Configured for SMTP Authentication Unable to Accept Mail Fixed an issue in which some systems configured for SMTP authentication were unable to accept incoming mail.
CSCsx32152	Yes	Fixed: Smart Identifier False Positives on Decimal Numbers Fixed an issue in which smart identifiers erroneously identified the digits following a decimal point as a credit card number.

Related Documents

The following guides may help you to install and run your Cisco Spam and Virus Blocker appliance.

- *Cisco Spam and Virus Blocker 6.6 FAQ*. This guide provides answers to frequently asked questions.

- *Cisco Spam and Virus Blocker 6.6 QuickStart Guide*. This guide provides step-by-step instructions for installing your Blocker appliance.
- *Cisco Spam and Virus Blocker 6.6 User Guide*. This guide provides basic instructions for setting up and maintaining your Blocker appliance.

Service and Support

This section contains Cisco Spam & Virus Blocker Support Contacts.

Country	Toll-Free Number
United States	1 866 606 1866 (English) 1 866 293 8884 (Japanese) 1 866 293 6725 (Mandarin) 1 866 293 8903 (Portuguese, Brazillian)
Austria	0800296029 (German [Deutsch])
Belgium	80080546 (Dutch [Nederlands])
Canada	1 866 606 1866 (English)
France	0805540272 (French [Français])
Germany	0800 6649307 (German [Deutsch])
Ireland	1800818077 (English)
Italy	800 924679 (English)
Japan	0120 996790 (Japanese)
Netherlands	0800-0292080 (Dutch [Nederlands])
Poland	0-800702019 (English)
Russia	81080023921044 (English)
Saudi Arabia	8008446843 (English)
Spain	900 814 934 (Spanish [Español])
Switzerland	0800564828 (English)
United Kingdom	0800 917 2337 (English)
**For any country not listed above, please call one of the United States telephone numbers.	

This document is to be used in conjunction with the documents listed in the “[Related Documents](#)” section.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

