



Release Notes for *Cisco Spam and Virus Blocker* Version 6.6.0-202

Revised: January 27, 2009, OL-18047-02

Contents

- **Introduction.** This section introduces the Cisco Spam and Virus Blocker. See [“Introduction”](#)
- **Installation Notes.** This section describes details relevant during product installation. See [“Installation Notes”](#)
- **Fixed Caveats.** This section discusses caveats that have been resolved in this release. See [“Fixed Caveats - Release 6.6.0-202”](#)
- **Open Caveats.** This section discusses caveats that have not been resolved in this release. See [“Fixed Caveats - Release 6.6.0-202”](#).
- **Related Documentation.** This section references other documentation that may be helpful in running and installing the Cisco Spam and Virus Blocker. See [“Related Documentation”](#)
- **Service and Support.** This section provides other places to look for service and support of your Cisco Spam and Virus Blocker. See [“Service and Support”](#)

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.



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

Installation Notes

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

Version 6.5.0-202 is the Blocker hot patch release of the Cisco Spam& Virus Blocker operating system.

The qualified upgrade paths to this release are:

From: Version 6.6.0-118 To: Version 6.6.0-202.

From: Version 6.6.0-131 To: Version 6.6.0-202.

From: Version 6.6.0-201 To: Version 6.6.0-202.

From: Version 6.6.0-202 To: Version 6.6.0-201.

Upgrade Instructions

For the 6.6 release, please use the following instructions to upgrade your Blocker appliance.

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.

Fixed Caveats - Release 6.6.0-202

The following table shows fixed caveats for this release:

Table 1 Fixed Caveats

Cisco Spam and Virus Blocker 6.6		
DDTS Number	Corrected	Caveat
CSCsx29313	Yes	<p>Fixed: OpenSSL Security Vulnerability</p> <p>A security vulnerability was identified in OpenSSL that affected the IronPort Email Security appliance. Due to this vulnerability, the appliance could incorrectly accept an invalid SSL signature that used a DSA key. This issue has been fixed.</p>

Open Caveats - Release 6.6.0-202

The following table shows open caveats for this release:

Table 2 Open Caveats

Cisco Spam and Virus Blocker 6.6		
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>

Table 2 Open Caveats

Cisco Spam and Virus Blocker 6.6		
DDTS Number	Corrected	Caveat
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>
CSCsv83861	No	<p>The Options menu is empty on the Spam Quarantine page</p> <p>The Spam Quarantine Page does not provide options to logout or change your password. The page erroneously displays the empty menu.</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>
CSCsv83909	No	<p>System Test shows “Pass” even if TLS negotiation fails.</p> <p>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.</p>
CSCsv83918	No	<p>The default Alias Consolidation LDAP query returns the most recently created alias rather than the primary Exchange address</p> <p>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).</p>

Table 2 **Open Caveats**

Cisco Spam and Virus Blocker 6.6		
DDTS Number	Corrected	Caveat
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.
CSCsv83938	No	Clicking <i>Enter</i> on the Test page of the Active Directory wizard erroneously opens the Active Directory wizard Start page. A workaround is to click on the Finish button to complete the Active Directory wizard.

Related Documentation

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

You can request customer support by visiting: <http://www.cisco.com/support>.

Additional information about the Blocker can be found at: www.cisco.com/go/blocker.

For telephone numbers or to email customer support, click on the **Email or phone Technical Support** link from the support portal.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0809R)

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. © 2008 Cisco Systems, Inc. All rights reserved.

