



Release Notes for Cisco Spam & Virus Blocker 7.0 Release

Revised: January 11, 2010, OL-21112-01

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 3](#)
- **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 9](#).
- **Service and Support.** This section provides information on obtaining service and support for your Cisco Spam & Virus Blocker. See [Service and Support, page 9](#).

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 7.0 release, 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

Enhanced: System Test

- **Enhanced testing functionality.** Previously, when you installed your Blocker, a system test was performed to see if the Blocker was prepared to receive mail from external senders, but the system test did not actually send mail to your Blocker. Now, as a part of the system test, Cisco sends a test message from a Cisco server to your Blocker. This ensures that your Blocker effectively handles mail and is ready for use.
- **Enhanced testing workflow.** Previously, if the system test encountered an error, you were required to run the System Setup Wizard again in order to repair any errors. Now, if you encounter an error, the Blocker will attempt to direct you to the part of the configuration that may have errors. When an error occurs, the Blocker redirects you to a part of the configuration file opened for editing. You can change the configuration setting and test the changes immediately.
- **Enhanced accessibility.** Previously, the system test was only accessible via the System Setup Wizard. Now, there is a system test page that you can access at any time. To access this page, go to **System Administration > System Test**. This can simplify your troubleshooting, as the system test is designed to locate common configuration errors.

New Feature: Configuration Summary Page

The configuration summary displays the settings you have configured for your Blocker and allows you to modify these settings from one convenient interface page. It's useful to consult this page if you are having problems sending or receiving mail via your Blocker, as sometimes errors occur in the configuration (for example, a typo exists in the Exchange server name that was entered). It's also a good idea to verify your settings on the Configuration Summary page after you upgrade.

New feature: Categorize Marketing Messages as Spam

Often, we receive marketing messages from companies who have obtained our email addresses through legitimate means (for example, you might get messages from a company where you bought shoes online a few years ago). While this mail is legitimate and not technically, "spam", it may be as much of a nuisance as spam from unsolicited sources. The Blocker can now categorize these marketing messages as spam so you can avoid receiving them.

To enable this feature, ensure that Anti-spam settings are enabled on your default mail policy. Then, go to **Mail Policies > Incoming Mail Policies**. Under the incoming mail policy, you can either click the default mail policy to enable this setting by default, or you can create a new mail policy for a specific group of users. Under the Anti-spam setting, click the section for Anti-spam policies. Scroll down to the **Marketing Email Settings** section, and click **Yes**, to enable marketing email settings.

New feature: Release Notification

As a convenience, Cisco now sends current customers a notification when new releases are ready and prompts customers to upgrade their Blocker appliances. This makes it easy to keep up with the latest releases and bug fixes. To allow Cisco to send you these alerts, go to **System Administration > Alerts**, and click the email address for the user who should receive these alerts. Check the **Release and Support Notifications** checkbox.

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 & 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 7.0 release of the Cisco Spam & Virus Blocker is 7.0.1-009. The following upgrade paths are supported:

From: 7.0.0-702 To: 7.0.1-009

From: 7.0.0-551 To: 7.0.1-009

From: 7.0.0-632 To: 7.0.1-009

From: 7.0.0-701 To: 7.0.1-009

From: 7.0.0-517 To: 7.0.1-009

From: 6.6.0-202 To: 7.0.1-009

From: 6.6.1-016 To: 7.0.1-009

Caveats

The following section describes opened and closed caveats for the Blocker 7.0 release.

Open Caveats - Blocker Release 7.0

The following table shows open caveats for this release:

Table 1 **Open Caveats**

Cisco Spam and Virus Blocker 7.0		
DDTS Number	Corrected	Caveat
CSCtc02512	No	<p>Unable to Install TLS Certificates Via the GUI</p> <p>Currently, you cannot install TLS certificates via the GUI on a Blocker appliance. This will be addressed in a later release.</p>
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>
CSCtb64739	No	<p>Language Defaults to English After Running Localized System Setup Wizard</p> <p>After running the system setup wizard in a language other than English, the language defaults to English when you are returned to the Login page.</p> <p>Workaround: Once you log into the Blocker, you can modify the language from the main page of the Blocker interface.</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>
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>

Table 1 Open Caveats

Cisco Spam and Virus Blocker 7.0		
DDTS Number	Corrected	Caveat
CSCtb94003	No	<p>System Test Errors can appear confusing if you configured a DNS Override.</p> <p>If you configured a DNS override, errors that occur during the system test may point you to the standard DNS configuration rather than the override value. If you encounter an error during the system test in delivering mail, you may need to check your DNS override value. The Configuration Summary page does not display the override value even if you have configured one.</p>
CSCtd15499	No	<p>Spam Quarantine Notification Defaults to “Weekly”</p> <p>In the "Network" section of System Setup Wizard, if you select <i>Block and Quarantine</i> option with “send daily digest”, the value is shown correctly in the Configuration Summary page but defaults to “weekly” in the standard UI. This issue will be fixed in a later release.</p> <p>Workaround: From the Monitor > Quarantine > Edit Spam Quarantine page, manually select “daily” as the value for the quarantine schedule.</p>
CSCsx05421	No	<p>Outgoing Mail Reports Scheduled By Default</p> <p>Daily outgoing email reports are scheduled by default regardless of whether the appliance is configured for outbound email. These reports can be ignored if your machine is not configured for outbound email.</p> <p>Workaround: Remove the unwanted scheduled reports</p> <p>To delete a scheduled report:</p> <p>From Monitor > Scheduled Reports, select the Outgoing Mail Daily Report and click Delete.</p>
CSCtc02621	No	<p>Connection Status Messages in the Active Directory Wizard are Partially Localized</p> <p>Some of the connection status messages appear in English instead of the selected localized language.</p>
CSCtc00172	No	<p>Localized Welcome Email Appears Garbled</p> <p>The Welcome email that is sent when you complete the System Setup wizard can appear garbled if the appliance GUI is run in a language other than English.</p>

Table 1 **Open Caveats**

Cisco Spam and Virus Blocker 7.0		
DDTS Number	Corrected	Caveat
CSCtb94894	No	<p>Updater Logs Contain Entries for Non-existent Features</p> <p>The Updater logs may contain entries for features that do not exist on your Blocker appliance. The code for the Updater logs is based on an Email Security appliance that contains some features such as McAfee and PostX that are not included on the Blocker platform. This issue will be fixed in a later release.</p>
CSCtb94062	No	<p>Application Error Occurs When Running System Test on a Listener for Which the IP Interface was Deleted</p> <p>If you delete an IP interface associated with a given listener and then attempt to run a system test against that listener, the Blocker returns an application error.</p>
CSCtd15615	No	<p>System Test Results May Be Inconsistent When Multiple DNS Servers are Assigned the Same Priority Level</p> <p>By default, when you have multiple DNS servers with the same priority, a DNS query will randomly select from among the DNS servers. If you are attempting to run a system test against a specific DNS server, the results will be inconsistent.</p> <p>Workaround: Specify a different priority for your DNS servers. If DNS servers are specified with different priority and if the primary DNS is unreachable, a secondary DNS will be picked up automatically.</p>

Resolved Caveats - Blocker Release 7.0

The following table shows resolved caveats for this release:

Table 2 **Resolved Caveats for Cisco Spam & Virus Blocker 7.0**

Cisco Spam and Virus Blocker 7.0		
DDTS Number	Corrected	Caveat
CSCtd72039	Yes	<p>Reduce the interval in which the Blocker checks for new feature keys</p> <p>In a previous release, the Blocker checked for new features keys every 24 hours. This interval has been reduced in the current release.</p>
CSCtc00034	Yes	<p>Feature Key Expiration Notice Contains Insufficient Information</p> <p>In a previous release, the feature key expiration notice did not contain sufficient information. The alert now contains helpful links and contact information.</p>

Table 2 *Resolved Caveats for Cisco Spam & Virus Blocker 7.0*

Cisco Spam and Virus Blocker 7.0		
DDTS Number	Corrected	Caveat
CSCsw88519	Yes	Security Certificate is Incorrect for Blocker In a previous release, the Blocker security certificate displayed information for IronPort products. This issue has been addressed.
CSCtc30746	Yes	System Setup Wizard Banner and Images not Localized Fixed an issue in which the Blocker System Setup Wizard did not display a localized banner or images (when localized languages were selected).
CSCtc06840	Yes	Error Delivering via Configured SMTP Routes Fixed an issue in which an error occurred when routing mail for configured SMTP routes.
CSCtb64721	Yes	Blocker System Test Stops if the Blocker is not Configured as the Primary MX Record Fixed an issue in which the Blocker system test would exit if the Blocker is not configured as the primary MX record. This no longer occurs.
CSCtc02744	Yes	System Test fails When SMTP Routes Configured to use A record Override Feature Fixed an issue in which if you configured SMTP routes to use an A record override feature, the system test failed. For example, if you specified the Mail server as “[mailserver.com]” and ran System Test, the System Test attempted to look up for [mailserver.com] in the DNS and failed.
CSCtb64669	Yes	Error Message When Testing LDAP Acceptance May Be Misleading Fixed an issue that occurred when performing the Blocker system test. Sometimes you may have received an error that was misleading due to incorrect configuration of the LDAP settings. The error directed you to change your RAT entry whereas the problem lay in your LDAP configuration.
CSCtc02507	Yes	Time format in Review page of System Setup Wizard Inconsistent with Other Time Zone Formats in the GUI Fixed an issue in which the time zone format in the System Setup Wizard was not synchronized with the time zone formats in the Configuration Summary page and the Time Zone settings page.
CSCtb93641	Yes	Redirection to the “Reset Configuration” screen After Running System Setup Wizard on IE7.0 Fixed an issue in which when you ran the System Setup wizard on IE7.0, you were redirected to run the System Setup wizard again, after clicking “install.”

Table 2 Resolved Caveats for Cisco Spam & Virus Blocker 7.0

Cisco Spam and Virus Blocker 7.0		
DDTS Number	Corrected	Caveat
CSCtc00050	Yes	<p>Unable to Generate Archived Report and Preview PDF for Scheduled Reports</p> <p>When viewing archived reports, sometimes errors occurred when generating scheduled reports. This issue has been resolved.</p>
CSCtc00082	Yes	<p>Support Request Verification Contains Untranslated Text</p> <p>When requesting support for a localized machine, the verification text for your support request contains untranslated text. This issue has been resolved.</p>
CSCtc00074	Yes	<p>Issues related to Localization using Deutsche language on Config Summary View page</p> <p>On the Config Summary page, some of the text was not localized, and some of the text was missing in places. This issue has been resolved.</p>
CSCtb64733	Yes	<p>Deprecated XML Element Warning Messages When Running Loadconfig After Upgrade</p> <p>When running the loadconfig command (loading the XML configuration file), warning messages about deprecated XML elements and config variables are displayed. These messages should not impact your upgrade and can be ignored.</p>
CSCtb64750	Yes	<p>Configuration Summary Page Displays RAT Entry for Data 2 Port Only</p> <p>The system test configuration summary page is designed to test the Data 2 RAT entries configured during product installation. For that reason, the summary configuration page displays only entries for the Data 2 port regardless of other RAT entries you may have created. This issue will be addressed in a later build.</p>
CSCtb66470	Yes	<p>Error Occurs When Releasing Spam from Spam Quarantine</p> <p>When releasing spam from the Spam Quarantine, you may receive the following error:</p> <p>"Error -too many values to unpack"</p> <p>When this error occurs, spam may not be released from the quarantine.</p>
CSCsv83815	Yes	<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>

Related Documents

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

- *Cisco Spam and Virus Blocker 7.0 QuickStart Guide*. This guide provides step-by-step instructions for installing your Blocker appliance.
- *Cisco Spam and Virus Blocker 7.0 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, Brazilian)
Austria	0800296029 (German [Deutsche])
Belgium	80080546 (Dutch [Nederlands])
Canada	1 866 606 1866 (English)
France	0805540272 (French [Français])
Germany	0800 6649307 (German [Deutsche])
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.

© 2010 Cisco Systems, Inc. All rights reserved.