



Release Notes for Cisco Spam & Virus Blocker 7.1.2 Release

Published: August 19, 2010, OL-22649-02

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 6](#).
- **Service and Support.** This section provides information on obtaining service and support for your Cisco Spam & Virus Blocker. See [Service and Support, page 7](#).

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 7.1.2 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

New Feature: Network Access

You can control from which IP addresses users can access the Blocker using a network access list. Users can access the Blocker from any machine with an IP address from the network access list. To create a network access list, go to the **System Administration > Network Access** page and click the **Edit Settings** button. Add the IP address, IP address range or CIDR range to the network access list.

Enhancement: Suspend and Resume Mail Operations

Previously, the **System Administration > Shutdown/Reboot** page only allowed you to shut down or reboot the Blocker. This is now the **Shutdown/Suspend** page, which supports suspending and resuming the Blocker's mail operations. Suspending mail operations means that no inbound email connections are accepted and outbound message delivery is halted. If the Blocker has multiple listeners, you can suspend email receiving on individual listeners. You can also choose to suspend outbound message delivery but continue receiving message.

Enhancement: Retry Delivery Now

Messages in the outgoing mail queue that are scheduled for later delivery can now be scheduled for immediate delivery by clicking the **Retry All Delivery** button on the **Monitor > Delivery Status** page. Messages for all domains that are "down" and any scheduled or soft bounced messages are queued for immediate delivery. You can also retry delivery of messages to a specific domain.

New Feature: Packet Capture

Sometimes when you contact Cisco Customer Support with an issue, you may be asked to provide insight into the network activity going into and out of the Blocker. As a convenience, the Blocker now provides the ability to run a packet capture, which intercepts and displays TCP/IP and other packets being transmitted or received over the network to which the Blocker is attached. You can download a packet capture file and forward it in an email to Cisco Customer Support for debugging and troubleshooting purposes. Go to **Support and Help > Packet Capture** to start a packet capture.

Enhancement: TLS Enhancements

The Blocker now offers you more control over how it handles TLS connections.

- **Certificates Management.** The Blocker provides support for managing certificates for TLS connections via the **Network > Certificates** page. You may purchase X.509 certificates and private keys from a recognized certificate authority service to use for receiving and delivery messages and other services. You can also create a your own self-signed certificate from the Blocker.
- **Certificate Authorities Management.** The Blocker now lets you manage the list of trusted certificate authorities that it uses to verify a certificate from a remote domain to establish the domain's credentials. You can import your own custom list and disable the Blocker's default system list via the **Network > Certificates** page.
- **TLS per Listener.** You can assign certificates to individual listeners, as well as other services like HTTPS services on an interface, the LDAP interface, and all outgoing TLS connections to recipient domains.
- **Batch Management.** You can import and export a Destination Controls configuration file for multiple destination domains via the **Mail Policies > Destination Controls** page.
- **Last TLS Error.** If the last outgoing TLS connection to a domain fails, the **Delivery Status Details** page for a specific domain now displays the reason why the connection failed.

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 7.1.2 release of the Cisco Spam & Virus Blocker is 7.1.2-020. The following upgrade paths are supported:

- From: Version 6.6.1-016 to Version 7.1.2-020
- From: Version 7.0.1-010 to Version 7.1.2-020
- From: Version 7.0.1-102 to Version 7.1.2-020
- From: Version 7.0.2-007 to Version 7.1.2-020
- From: Version 7.0.3-005 to Version 7.1.2-020
- From: Version 7.1.0-104 to Version 7.1.2-020
- From: Version 7.1.1-012 to Version 7.1.2-020
- From: Version 7.1.2-019 to Version 7.1.2-020

Caveats

The following section describes opened and closed caveats for the Blocker 7.1.2 release.

Open Caveats - Blocker Release 7.1.2

The following table shows open caveats for the 7.1.2 release:

Table 1 **Open Caveats**

Cisco Spam and Virus Blocker 7.1.2		
DDTS Number	Corrected	Caveat
CSCtb97572	No	<p>System Test Checks for Domain Not in Recipient Access Table</p> <p>The System Test can perform a check on an email address for a domain that is not configured in the Blocker's Recipient Access Table. This test should only be run for an email address that belongs to your domain.</p>
CSCtc64448	No	<p>System Test Should State that the Email Address is for a Configured Domain</p> <p>The text "Enter an email address that contains a valid domain" that appears on the System Test Page does not indicate that the email address has to be for a domain configured in the Blocker's Recipient Access Table.</p>
CSCtc93691	No	<p>Blocker Displays Incorrect Link When the System Test Fails Due to LDAP Error</p> <p>When the System Test fails due to an LDAP error, the Blocker displays a link to "Check RAT Configuration" instead of a link to the LDAP Page.</p>
CSCtc54183	No	<p>System Setup Wizard Shows Deutsche as Default Language</p> <p>The welcome page of the System Setup Wizard shows Deutsche as the selected language by default, but after you click "Get Started," the content of the System Setup Wizard is in English.</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>
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>

Table 1 **Open Caveats**

Cisco Spam and Virus Blocker 7.1.2		
DDTS Number	Corrected	Caveat
CSCtd71183	No	Troubleshooting Information on Configuration Summary Page is Not Localized Some of the troubleshooting information on the Configuration Summary Page appear in English instead of the selected localized language.
CSCtd38067	No	Registration Status Message on System Status Page is Not Localized The registration status message on the System Status Page appears in English instead of the selected localized language.
CSCtc86985	No	System Test Error Message is Not Localized The error messages on the System Test Page appear in English instead of the selected localized language.

Resolved Caveats - Blocker Release 7.1.2

The following table shows resolved caveats for the 7.1.2 release:

Table 2 **Resolved Caveats for Cisco Spam & Virus Blocker 7.1.2**

Cisco Spam and Virus Blocker 7.1.2		
DDTS Number	Corrected	Caveat
CSCtc76305	Yes	Non-ASCII Character in Recipient Address Causes App Fault Fixed an issue where a non-ASCII character in the envelope recipient address caused an app fault.

Resolved Caveats - Blocker Release 7.1.1

The following table shows resolved caveats for the 7.1.1 release:

Table 3 *Resolved Caveats for Cisco Spam & Virus Blocker 7.1.1*

Cisco Spam and Virus Blocker 7.1.1		
DDTS Number	Corrected	Caveat
CSCtc02512	Yes	<p>Unable to Install TLS Certificates Via the GUI</p> <p>In previous releases, you could not install TLS certificates via the GUI on a Blocker appliance. This issue has been resolved.</p>
CSCtc00172	Yes	<p>Localized Welcome Email Appears Garbled</p> <p>In previous releases, the welcome email that was sent when you completed the System Setup wizard appeared garbled if the appliance GUI was run in a language other than English. This issue has been resolved.</p>
CSCtc02474	Yes	<p>Success Message After System Setup Wizard Not Localized</p> <p>In previous releases, the success message displayed after running the System Setup Wizard appeared in English instead of the selected localized language. This issue has been resolved.</p>
CSCtb80669	Yes	<p>Support for User-Entered Certificate Authorities</p> <p>The Blocker now lets you manage the list of trusted certificate authorities that it uses to verify a certificate from a remote domain to establish the domain's credentials. You can import your own custom list and disable the Blocker's default system list via the Network > Certificates page.</p>
CSCsz74482	Yes	<p>Multiple Support Requests Opened via the GUI</p> <p>When sending a support request via the GUI in previous releases, the Blocker did not do anything to indicate that it was generating and sending the request, such as displaying a message or disabling the Send button. This led many customers to click Send again because it appeared that the Blocker was not sending the request. Instead of sending one service requests, customers sent multiple. This issue has been addressed. Now, the Send button becomes disabled after the first support request is sent.</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 7.1 User Guide*. This guide provides basic instructions for setting up and maintaining your Blocker appliance.
- *Cisco Spam and Virus Blocker 7.0 QuickStart Guide*. This guide provides step-by-step instructions for installing 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.

