



Release Notes for BBSM Release 5.3, Patch 5327

January 2006
OL-8848-01

These release notes describe Cisco Building Broadband Service Manager (BBSM) patch 5327, which includes six resolved caveats.

Contents

- [System Requirements, page 1](#)
- [New and Changed Information, page 2](#)
- [Resolved Caveats, page 2](#)
- [Documentation Updates, page 2](#)
- [Related Documentation, page 3](#)
- [Obtaining Documentation, page 3](#)
- [Documentation Feedback, page 4](#)
- [Cisco Product Security Overview, page 5](#)
- [Obtaining Technical Assistance, page 5](#)
- [Obtaining Additional Publications and Information, page 7](#)

System Requirements

This patch requires that BBSM 5.3 SP2 (patch 5325) be installed first.



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

© 2006 Cisco Systems, Inc. All rights reserved.

New and Changed Information

This patch makes minor changes in the software installation procedure and to the procedure for deactivating client sessions. Two user documents, the *Cisco BBSM 5.3 Software Installation Guide* and the *Cisco BBSM 5.3 Operations Guide*, change as a result. (See the section on “[Documentation Updates](#)” for precise information these changes.)

Resolved Caveats

Patch 5327 resolves the following caveats:

Table 1 **Resolved Caveats**

DDTS Number	Description
CSCsb66934	Previously, the BBSM would not route walled-garden entries even when the transparent proxy feature was enabled. The transparent proxy feature now works for walled-garden entries.
CSCsb87734	Clients configured for domains and connecting to BBSM were hanging at the desktop. The BBSM now has improved startup time for clients configured for AD Domain log in.
CSCsb93453	Client-session deactivation was not effective when the network included routers without SNMP. This has been fixed so that only those clients having a valid MAC addresses can be permanently deactivated.
CSCsc10809	The QoS Packet Handler was not activating automatically during installation. This has been fixed by slightly augmenting the process to install the BBSM AtNAT driver.
CSCsc18754	GetOriginalURL() was storing the IP address instead of the DNS name. The BBSM now includes an enhanced BBSM SDK GetOriginalURL API that returns the original DNS name instead of dot IP address.
CSCsc20603	WEBConfig automatically appended @<mngmt_vlan> instead of @<client_vlan>. By default the BBSM now appends “@” to the SNMP password after BBSM switch discovery.

Documentation Updates

This patch makes minor changes in the software installation procedure and to the procedure for deactivating client sessions. Two user documents, the *Cisco BBSM 5.3 Software Installation Guide* and the *Cisco BBSM 5.3 Operations Guide*, change as a result.

Cisco BBSM 5.3 Software Installation Guide

In the *Cisco BBSM 5.3 Software Installation Guide*, in the section on “Installing the BBSM AtNAT Driver,” add these four steps after Step 9 (“Click **Close**”):

- 9a. From the Network and Dial-up Connections window, right-click the AtNatMP icon.
- 9b. Select **Properties**.

9c. In the AtNatMP Properties dialog box, uncheck the **QoS Packet Scheduler** check box.

9d. Click **Close**.

Steps 10 and 11 follow as usual. The new steps are required to configure the AtNatMP.

The *Cisco BBSM 5.3 Software Installation Guide* is at

http://www.cisco.com/en/US/products/sw/netmgts/ps533/prod_installation_guide09186a00801d8cdc.html.

The direct link to the section on n the section on “Installing the BBSM AtNAT Driver” is

http://www.cisco.com/en/US/products/sw/netmgts/ps533/prod_installation_guide09186a00801d8cdc.html#wp21606.

Cisco BBSM 5.3 Operations Guide

In the *Cisco BBSM 5.3 Operations Guide*, in the section on “Deactivating and Reactivating Clients” under the heading “Deactivating Client Sessions,” this information is added:

- You now can deactivate clients with MAC address of FFFFFFFF.
- The checkbox to permanently deactivate clients is disabled for active clients with a MAC address of FFFFFFFF. Only clients with valid MAC addresses can be permanently deactivated.

The *Cisco BBSM 5.3 Operations Guide* is at

http://www.cisco.com/en/US/products/sw/netmgts/ps533/products_user_guide_book09186a00801dc7cb.html.

The direct link to the section on “Deactivating and Reactivating Clients” is

http://www.cisco.com/en/US/products/sw/netmgts/ps533/products_user_guide_chapter09186a00801da1b3.html.

Related Documentation

These documents provide complete information about BBSM:

- *Cisco BBSM 5.3 Operations Guide* (order number DOC-7816161)
- *Cisco BBSM 5.3 Software Installation Guide* (order number DOC-7815714)
- *Cisco BBSM 5.3 SDK Developer Guide* (available on Cisco.com)

To ensure you have the latest information on BBSM, refer to release notes on Cisco.com before installing, configuring, or upgrading the BBSM server.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Reminder Concerning BBSD

The Building Broadband Service Directory (BBSD) is not supported in BBSM 5.3 or later.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)

© 2005 Cisco Systems, Inc. All rights reserved.