



Release Notes for Cisco BBSM 5.2 Service Pack 2

February 2004

These release notes describe the Cisco Building Broadband Service Manager (BBSM) version 5.2 Service Pack 2 (SP2), which resolves caveats and issues in BBSM 5.2. This service pack is cumulative and contains Microsoft security updates and all previously released patches including BBSM Service Pack 1 (SP1). This service pack has no dependencies.



Note

The most current Cisco documentation for released products is available on Cisco Connection Online (CCO) at <http://www.cisco.com>. Online documents may contain updates and modifications made after the paper documents are printed.

Contents

- [Introduction, page 2](#)
- [Installation, page 6](#)
- [Important Notes, page 8](#)
- [Resolved Caveats, page 14](#)
- [Obtaining Documentation, page 16](#)
- [Documentation Feedback, page 17](#)
- [Obtaining Technical Assistance, page 17](#)
- [Obtaining Additional Publications and Information, page 18](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Introduction

BBSM 5.2 SP2 can be installed on any BBSM 5.2 server. This service pack consists of the latest fixes to date including BBSM 5.2 SP1 and these subsequent patches:

- [FidelioPMSPatch.exe—Patch 5212](#)
- [AironetPacketInactivity.exe—Patch 5213](#)
- [Cisco4x0x.exe—Patch 5214](#)
- [PatchMS03007.exe—Patch 5215](#)
- [PMSPosting.exe—Patch 5217](#)
- [AccessCodesPatch.exe—Patch 5220](#)
- [BBSM5.0to5.2DLLPatch.exe—Patch 5223](#)
- [BBSM52-UpdatedSSLPatch.exe—Patch 5230](#)
- [APsAndSwitches.exe—Patch 5232](#)
- [MDACSecurity.exe—Patch 5233](#)
- [RPCSSBufferOverrun.exe—Patch 5239](#)

FidelioPMSPatch.exe—Patch 5212

This patch resolves a Micros-Fidelio certification problem in both the one-way and two-way PMS interfaces. You need to install this patch only if you are using Micros-Fidelio PMS protocols.

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5212.pdf>

AironetPacketInactivity.exe—Patch 5213

This patch adds new Cisco Aironet access point types to the BBSM 5.2 server, which are available on the Cisco Access Point Type drop-down menu. The menu is located on the Network Elements - Access Points web page in WEBconfig:

- Aironet 340 Packet
- Aironet 350 Packet
- Aironet 1100 Packet
- Aironet 1200 Packet



Note

Clients that are connected and browsing the Internet using these access points are automatically disconnected if their idle time exceeds the number of seconds that are specified by the administrator in the Packet Inactivity Period field.

For additional Cisco Aironet information, refer to this website:

<http://www.cisco.com/en/US/products/hw/wireless/index.html>

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5213.pdf>

Cisco4x0x.exe—Patch 5214

This patch provides support for Cisco Catalyst 4000 and Catalyst 4500 series switches. These switches can be configured to support the private VLAN security feature. If this feature is used, the SNMP password that is configured in BBSM must be appended with @<primary VLAN ID>, which enables BBSM to discover ports in the private VLAN.

For example, if the SNMP password configured in the switch is private and its primary VLAN ID is 100 for the private VLAN, the SNMP password in BBSM would be *private@100*. The IP address for this switch must be configured in the primary VLAN. All client ports must be a part of the private VLAN, and BBSM must be connected to its private VLAN promiscuous port.

This patch replaces the switch type entry *Cisco 400x* with *Cisco 4x0x* in the Cisco Switch Type drop-down menu, which is located on the Network Elements - Switches web page in WEBconfig. This patch has been successfully tested with these new switches:

- Cisco Catalyst 4507 - Supervisor 4 - Cisco IOS Release 12.1(12c)EW
- Cisco Catalyst 4006 - Supervisor 3 - Cisco IOS Release 12.1(12c)EW & Cisco IOS Release 12.1(14)E1
- Cisco Catalyst 4006 - Supervisor 4 - Cisco IOS Release 12.1(12c)EW

For additional information about configuring private VLANs, refer to this Cisco website:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_14/config/pvlans.htm

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5214.pdf>

PatchMS03007.exe—Patch 5215

This patch installs Microsoft patches and corrects a Microsoft vulnerability on the BBSM 5.2 server. A Windows component that is used by WebDAV contains a security vulnerability that exists because the component contains an unchecked buffer. This vulnerability can be exploited if an attacker sends a specially formed HTTP request to a computer running Microsoft Internet Information Services (IIS). This request can cause the server to fail or to run code of the attacker's choice, which would run in the security context of the IIS service.

For additional information, refer to Microsoft Security Bulletin MS03-007 at this website:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-007.asp>

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/pch5215a.pdf>

PMSPosting.exe—Patch 5217

This patch enables you to post charges to the Property Management System (PMS) if you did not use the Map Rooms tool on the BBSM 5.2 Dashboard to map rooms to ports. With this patch, you can map rooms using the Map Rooms tool or by updating the Port Location field with an actual room number or location identifier on the Port Control - Port Settings web page.

**Caution**

The only way to ensure that your port-room mapping is accurate is to use the Map Rooms tool to map locations or rooms. If you enter port locations for the first time using the Port Location field in Port Control, there is no way to verify that ports are mapped to the correct room numbers. After rooms are mapped, you can update port locations using the Port Control.

This patch updates all of the Time_Of_Last_Configure NULL values in the Port_Map table in the BBSM database. The Time_Of_Last_Configure value is updated every time a port is mapped from either the Map Rooms or Port Control web pages. To disable PMS billing for a port, set the Port Location field to unmapped on the Port Control - Port Settings web page.

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5217.pdf>

AccessCodesPatch.exe—Patch 5220

This patch adds support for the English (United Kingdom) regional settings when using access codes, but it does not add support for any other regional settings. Prior to this patch, if the BBSM server regional settings were set to English (United Kingdom), the access code dates were transposed and not processed correctly. For example, if access codes were generated for use between May 3 (5/3) and May 4, (5/4), BBSM would report that the access codes were valid between March 5 (3/5) and April 5 (4/5). This patch applies to all new access codes that are generated after the patch is installed, but it does not fix existing access codes that have incorrect dates.

**Caution**

After this patch is installed, you must regenerate any access codes that have incorrect dates.

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5220.pdf>

BBSM5.0to5.2DLLPatch.exe—Patch 5223

After you upgrade the BBSM server from software release 5.0 to 5.1 and then to BBSM 5.2, a duplicate DLL file exists, which prevents clients from connecting. Instead, they receive an error message in place of the Start page. To resolve this problem, you must delete the GenericSwitchNoLinkStatus.DLL file in the c:\atcom\install\switches directory. The latest version of this file is in the c:\atcom\install directory. Do not delete the DLL file from this directory. If you do not have direct access to the upgraded BBSM 5.2 server, you must install this patch remotely to delete the DLL file.

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5223.pdf>

BBSM52-UpdatedSSLPatch.exe—Patch 5230

This patch updates and replaces Patch 5224, modifies BBSM to prevent unauthenticated web proxy browser clients from browsing to external SSL websites, and resolves the BBSM reboot problem that occurs when a Macintosh iBook client connects to the BBSM network. For additional information about the Macintosh iBook problem, refer to DDTS incident CSCeb58473.

Prior to this patch, some browser configurations allowed end users to access an SSL web page (https) before they were authenticated. BBSM would not redirect these clients to the start page, and they could access an SSL page without logging in. After this patch is applied, the Macintosh iBook reboot problem is resolved, and clients cannot access SSL pages unless they are authenticated.



Note

Clients that have an SSL page configured as the home page on their browser receive a browser error page when they first launch their browser. They must access an http page to be redirected to the BBSM Start page.

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5230.pdf>

APsAndSwitches.exe—Patch 5232

This patch adds new access point and switch types to the BBSM 5.2 server, resolves problems with Cisco Aironet 1100 and 1200 Series (using Cisco IOS software) Access Points, and replaces Patches 5213 and 5218.

This patch adds these Cisco Catalyst switch types to the Cisco Switch Type drop-down menu, which is located on the Network Elements - Switches web page in WEBconfig:

- Cisco 2924 Packet
- Cisco 3524 Packet
- Cisco 3548 Packet

This patch adds these Cisco Aironet access point types to the Cisco Access Point Type drop-down menu, which is located on the Network Elements - Access Points web page in WEBconfig:

- Aironet 340 Packet
- Aironet 350 Packet
- Aironet 1100 Packet
- Aironet 1200 AP (IOS)
- Aironet 1200 AP (VxWorks) (Listed as Aironet 1200 AP before the patch is applied.)
- Aironet 1200 Packet (IOS)
- Aironet 1200 Packet (VxWorks)

Clients that are connected and browsing the Internet using packet-type switches or access points are automatically disconnected if their idle time exceeds the number of seconds that is specified by the administrator in the Packet Inactivity Period field, which is located on the Network Elements - Switches web page or the Network Elements - Access Points web page in WEBconfig.

For additional Cisco Aironet information, refer to this website:

<http://www.cisco.com/en/US/products/hw/wireless/index.html>



Caution

This patch changes the port index references on Cisco Aironet 1100 and 1200 Series (using Cisco IOS software) Access Points that are used by BBSM. This prevents BBSM from functioning properly with regard to previously generated port settings (port maps). If you already have Cisco Aironet 1100 and 1200 Series (using Cisco IOS software) Access Points configured, or you add or delete VLANs on access points, you must reconfigure the BBSM port settings for these devices after you install this patch.

Support for the Cisco Aironet 1100 Series Access Points and Cisco Aironet 1230 Access Points was introduced in BBSM 5.2 SP1. However, when a default VLAN was configured on either access point, BBSM could not find clients associated with the access point. This patch resolves this problem.

If you experience a problem disconnecting a client that is using the Cisco Aironet client adapter, upgrade the client adapter software to the latest available version on CCO.

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/ptch5232.pdf>

MDACSecurity.exe—Patch 5233

This patch eliminates a Microsoft Data Access Components (MDAC) security vulnerability on the BBSM 5.2 server. MDAC is a collection of components that is used to provide database connectivity on Windows platforms. This security vulnerability exists because of an unchecked buffer in a specific MDAC component. Attackers could exploit this vulnerability and cause a buffer overrun to occur in a specific MDAC component, which would enable the attacker to take any action on the system. This patch prevents an attacker from exploiting this vulnerability.

For additional information, refer to Microsoft Security Bulletin MS03-033 at this website:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-033.asp>

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/pch5233a.pdf>

RPCSSBufferOverrun.exe—Patch 5239

This patch replaces Patch 5231 and eliminates Microsoft security vulnerabilities on the BBSM 5.2 server. These Microsoft vulnerabilities have been identified in the part of RPCSS Service that deals with Remote Procedure Call (RPC) messages for Distributed Component Object Model (DCOM) activation. These vulnerabilities result from incorrect handling of malformed messages and could allow arbitrary code execution and denial of service.

An attacker could exploit these vulnerabilities by creating a program that sends a malformed RPC message that targets the RPCSS Service on a vulnerable system. If successful, the attacker could run code with Local System privileges on the affected system or cause the RPCSS Service to fail. This would enable the attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it.

For additional information, refer to this Microsoft website:

<http://www.microsoft.com/technet/security/bulletin/MS03-039.asp>

For additional information about this patch, refer to this Cisco website:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/relnote/pch52392.pdf>

Installation

This service pack can be installed locally onto any BBSM 5.2 server with Internet access or remotely onto multiple BBSM servers from another computer. Because this service pack includes an IIS patch, Internet service is interrupted during the installation, and you do not see a success message upon completion.

If you are installing the service pack remotely, you see this message: *The page cannot be displayed...* The operating system and browser version that you are using can also affect the type of message that you see. In either case, the connection to the server is lost. However, the patch installation continues, and the server restarts upon completion.



Caution

We recommend terminating all client sessions during BBSM service pack and patch upgrades and installations. For additional information, refer to the *Cisco BBSM 5.2 User Guide*.

Follow these steps to install BBSM 5.2 SP2 onto your BBSM server:

Step 1 Using the Internet Explorer (IE) web browser, go to the Cisco BBSM 5.2 Software Download website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm52>



Note

You must use the IE browser when using WEBpatch because of some known issues and incompatibilities with Netscape Navigator.

Step 2 Download **BBSM52SP2.exe** to a temporary location on your computer.

- For a local BBSM installation, go to [Step 6](#).
- For a remote BBSM installation, continue with [Step 3](#).



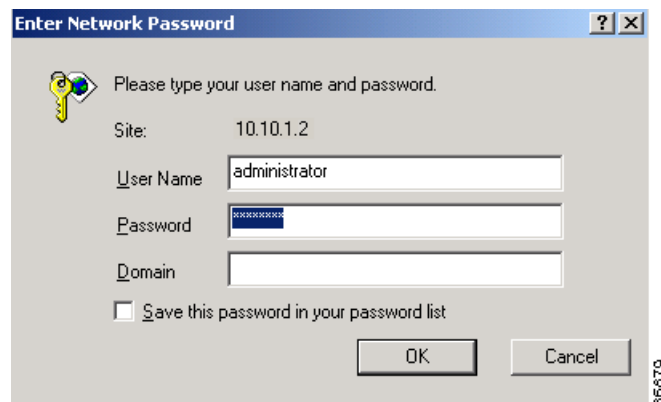
Note

If you are using the Windows 2000 (SP2 or later) or Windows XP operating systems to install this patch remotely, the WEBpatch web pages load very slowly. To prevent this problem, uncheck the **Client for Microsoft Networks** check box in the NIC Properties window on your remote computer.

Step 3 In the IE browser field, enter **http://<address>:9488/www** where <address> is either the external NIC address of the BBSM server (if you are accessing it externally) or the internal IP address of the BBSM server (if you are accessing it from within the BBSM subnet).

For example, enter **http://10.10.1.2:9488/www**, and press **Enter**. The Enter Network Password window appears. (See [Figure 1](#).)

Figure 1 Enter Network Password Window



Step 4 Enter your username and password. (Do not enter any information in the Domain field.)



Note You must have administrator privileges to use WEBpatch.

Step 5 Click **OK**. The remote BBSM Dashboard appears.

Step 6 From the BBSM Dashboard, use the WEBpatch utility to install this patch.



Note Refer to the *Cisco BBSM 5.2 User Guide* for instructions on transferring and installing BBSM patches and service packs. This service pack automatically reboots your BBSM server.

Important Notes

The following sections provide updated BBSM information.

Single-VLAN Configuration Note

If you are using a single-VLAN configuration and Cisco Ethernet switches and want to use a non-default management VLAN ID, you must change the Ethernet switch's VLAN ID. The switch's SNMP password configured in WEBconfig must be appended with @<management VLAN #>, which enables BBSM to discover ports in the VLAN. For example, if the switch's SNMP read-write community string is *private* and its management VLAN # is *100*, change the switch's BBSM SNMP password to *private@100*. You can also use the Switch Discovery Wizard to specify the management VLAN when you are adding switches to BBSM.

Indexed SNMP passwords are not supported on Cisco Aironet access points. Do not append @<VLAN ID> to the SNMP passwords of the access points on BBSM even if the access point management VLAN ID is not 1. If a non-default management VLAN ID is used on the access points, make sure that the management VLAN is set up as a native VLAN on the access points and on the switch trunk that the access points are connected to. For more information, see CSCed74734.

Access points are not configured automatically with a default VLAN. If you add, remove, or change any VLAN configuration from an access point, you must reconfigure the access point port settings by using WEBconfig. For additional information, refer to the *Cisco BBSM 5.2 User Guide*.

Port Hopping Note

Configuring port hopping on a "Null: Clients connect to router" or a packet inactivity status detection type Cisco Aironet access point breaks packet inactivity functionality. When this happens, BBSM does not disconnect clients in time. The workaround is to disable port-hopping on those network elements. If the packet inactivity status detection type is used, there is no need to turn on port-hopping since packet inactivity allows clients to port-hop.

CyberSource Note

BBSM software includes a credit card accounting policy that invokes an application program interface (API) that is provided by CyberSource to interface with the CyberSource ICS credit card processing system. Included in the CyberSource API is a digital certificate, `CyberSource_SJC_US.crt`, which authenticates a CyberSource ICS server and a command line application, `Ecert`, to configure ICS merchant IDs from that ICS server. On January 16, 2004, the digital certificate expired and CyberSource changed its merchant ID configuration logic so that `Ecert` is now obsolete.



Note

BBSM servers that were previously configured with CyberSource ICS merchant IDs for BBSM credit card accounting still operate correctly. It is not necessary for existing customers that are using the ICS accounting policy to make any changes on their BBSM server.

BBSM administrators who want to use the BBSM ICS credit card accounting policy must configure an ICS merchant ID on the BBSM server before end users can use any of the BBSM ICS credit card accounting page sets. One of the steps in configuring the merchant ID is to run `Ecert` with the merchant ID as a command line parameter. `Ecert` communicates with a CyberSource server, authenticated with the previously mentioned digital certificate, and generates a public/private key pair and corresponding digital certificate for the BBSM server and the specified merchant ID. The CyberSource ICS API, when invoked from BBSM, uses the generated keys and certificate to communicate credit card information with a CyberSource ICS server.

Follow these steps to obtain and use the current versions of the CyberSource server digital certificate and the `Ecert` application:

- Step 1** From the BBSM server, go to `c:\opt\ics\keys`, and rename the `CyberSource_SJC_US.crt` file to **CyberSource_SJC_US.crt.old**.
- Step 2** Go to the CyberSource website (http://www.cybersource.com/support_center/management/keyupdate).



Note You need a CyberSource account to access this page.

- Step 3** Locate and download the following files to `c:\opt\ics\keys`:
- `CyberSource_SJC_US.cer`
 - `ecert-nt-3.4.10.exe`
- Step 4** Open a DOS window, and enter **`cd c:\opt\ics\keys`**.
- Step 5** Press **Enter**.
- Step 6** Enter **`ecert-nt-3.4.10.exe <merchantID>`**, where `<merchantID>` is your CyberSource merchant ID number, and press **Enter**.
- Step 7** Enter **`copy c:\opt\CyberSource\SDK<merchantID>.*`** and press **Enter**.
- Step 8** Enter **`copy c:\opt\CyberSource\SDK\CyberSource_SJC_US.crt`** and press **Enter**.
- Step 9** Close the DOS window.
- Step 10** Configure BBSM to do credit card billing as described in the *Cisco BBSM 5.2 User Guide* using `<merchantID>` as the credit card billing Merchant ID.

Load Balancing Note

With the release of BBSM 5.2, load balancing is no longer supported on this platform.

IP Spoofing Note

As of BBSM 5.2 SP2, a new feature has been added that detects IP spoofing, which occurs when a second MAC address, such as a laptop, tries to use the same IP address. Consequently, the second MAC address is prevented from accessing the system.

Because the IP address spoofing feature blocks a DHCP client if its IP address is already associated with an existing active session, some DHCP clients cannot connect although they have IP addresses assigned through DHCP. The affected clients cannot ping BBSM's internal NIC address. They receive "The Page Cannot Be Displayed" error message on their browsers.

This problem can occur in these situations:

1. A link status switch type is used when a hub device is connected to a switch port.
2. A hibernating client is connected to a switch that is configured as a link status switch.
3. A long packet inactivity period is used.
4. A combination of long packet inactivity and port hopping is used.

In all of these cases, BBSM maintains a session although a client is no longer in the network or is not requesting to renew the IP address. Since the DHCP server is not aware of the existing session in BBSM, it assigns the IP address to another client when the default lease time expires. When this occurs, the IP address spoofing logic in BBSM blocks packets from the IP address because packets are from a different IP and MAC combination.

IP Spoofing Workaround for Switches

For situations 1 and 2 above, the workaround is to either remove the hub or other device from the port or to change the activity detection method, which is set through WEBconfig. Otherwise, the switch type of the affected devices must be changed to the packet inactivity switch type, and the packet inactivity period must be configured to be less than 15 minutes. See the "[Port Hopping Note](#)" section on page 8. Follow these steps:

-
- Step 1** Go to the Network Elements - Switches web page in WEBconfig, and use the ">" button to navigate to the switch that needs modification.
 - Step 2** Click the **Switch Type** drop-down arrow, and change the selected switch type to the correct packet type. For example, if you are using the Cisco Catalyst 2940, you would choose Cisco Catalyst 2940 Packet. As soon as this change is made, the Packet Inactivity Period field is enabled.



Note If you need to use a long packet inactivity period or port hopping, you must increase the DHCP lease time. The minimum DHCP lease time is calculated by using the appropriate formula: $[(PIP \text{ or } PHD + 15 \text{ minutes}) * 2]$ or $[(PIP + PHD + 15 \text{ minutes}) * 2]$, where PIP equals *Packet Inactivity Period* and PHD equals *Port Hop Delay*. For example, if PIP equals 30 minutes and PHD equals 10 minutes, then the minimum DHCP lease time must be changed to 110 minutes $[(30 + 10 + 15) * 2]$. To configure the DHCP lease time, see the "[Increasing the DHCP Lease Time](#)" section on page 11.

- Step 3** From the Packet Inactivity Period field, enter a value of time, in seconds, that is 15 minutes or less.
- Step 4** To save the changes, click **Save**.
- Step 5** Repeat for every switch needing this modification.
- Only Cisco switches support Packet Inactivity switch types. If you are using other switch types, they are considered legacy devices and are not supported by TAC.
-

If you are using a Daily Access Policy (24 hours) and a switch that cannot support the packet inactivity detection type, another alternative is to change the DHCP lease time to 24 hours. This will guarantee that the IP address will not be given to other users within that period.

IP Spoofing Workaround for Access Points

For situations 3 and 4 above, the workaround is to reduce the packet inactivity period or the combined packet inactivity periods and port hop delay to be less than 15 minutes. See the [“Port Hopping Note” section on page 8](#). To do so, follow these steps:

- Step 1** Go to the Network Elements - Access Point web page in WEBconfig, and use the “>” button to navigate to the access point that needs modification.
- Step 2** Under Access Point Type, change the selected access point type to the correct packet type. For example, if you are using the Cisco Aironet 1100 AP, you would choose Cisco Aironet 1100 Packet.



Note If you need to use a long packet inactivity period or port hopping, you must increase the DHCP lease time, which is calculated by using this formula: $[(PIP \text{ or } PHD + 15 \text{ minutes}) * 2]$ where PIP equals *Packet Inactivity Period* and PHD equals *Port Hop Delay*. For example, if the PIP equals 30 minutes, then the minimum DHCP lease time would be 90 minutes $[(30 + 15) * 2]$. To configure the DHCP lease time, continue to the following section.

- Step 3** From the Packet Inactivity Period field, enter a value of time, in seconds, that is 15 minutes or less.
- Step 4** To save the changes, click **Save**.
- Step 5** Repeat for every access point needing this modification.
- Only Cisco access points support Packet Inactivity switch types. If you are using other access point types, they are considered legacy devices and are not supported by TAC.
-

Increasing the DHCP Lease Time

Follow these steps to increase the DHCP lease time:

- Step 1** From the BBSM desktop, choose **Start > Programs > Administrative Tools > DHCP**. The DHCP window appears.
- Step 2** Right-click the **Scope** folder and choose **Properties**. The Scope BBSM53 Properties window appears.



Note If the Properties option is not visible, wait a few seconds, and right-click the **Scope** folder again.

-
- Step 3** In the Lease duration for DHCP clients area, enter the correct number of hours and minutes, and click **OK**.
- Step 4** Close the DHCP window.
-

WEBpatch Note

After you install BBSM 5.2 SP2, a complete patch log is not generated for BBSM 5.2 SP2 in the WEBpatch - Patch Log web page. The log has only one entry, *CPatchUtil::InstallPatch started*, which indicates that the service pack was successfully installed.

Page Set Note

This service pack applies fixes that directly affect BBSM 5.2 page sets. When you apply this service pack, new page set files are installed in the `c:\atcom\ekgnkm` directory. The new page sets do not overwrite your existing page sets, and they are easy to identify because `_52SP2` has been added to the filename. (See the “[New Page Set Files](#)” section below.)



Caution

This service pack does not automatically apply the fixes associated with the BBSM 5.2 page sets. To incorporate these fixes, you must replace your existing page set files with the new page set files. (See “[Replacing Page Sets](#)” in the next section.) If you are using custom page sets, you must add your custom changes to the new page set files.

Replacing Page Sets

Follow these steps to replace your existing page set file with a new page set file:

-
- Step 1** From the `c:\atcom\ekgnkm` directory, rename (or move) your existing page set files.
- Step 2** Locate the new page set file, and delete `_52SP2` from the page set filename.
-

New Page Set Files

This service pack installs these new page set files in the `c:\atcom\ekgnkm` directory:

- `BiDirectional_Checkout_52SP2.asp`
- `BiDirectional_CheckoutStatus_52SP2.asp`
- `BiDirectional_DailyHotelPost_52SP2.asp`
- `BiDirectional_DailyHotelStart_52SP2.asp`
- `BiDirectional_HotelError_52SP2.asp`
- `DailyHotelStart_52SP2.asp`
- `DailyICSClearPackage_52SP2.asp`
- `DailyICSClearPost_52SP2.asp`

- DailyICSPackage_52SP2.asp
- DailyICSPost_52SP2.asp
- disconnect_52SP2.asp
- MDSubStart_52SP2.asp
- MDSubSubscribe_52SP2.asp
- MegaClearPost_52SP2.asp
- MegaPost_52SP2.asp
- RADIUSClearStart_52SP2.asp
- RADIUSStart_52SP2.asp
- RADIUSUBandClearStart_52SP2.asp
- RADIUSUBandStart_52SP2.asp
- SimpleDailyHotelStart_52SP2.asp
- startCheckout01_52SP2.gif
- startCheckout02_52SP2.gif
- SubscriptionHomeStart_52SP2.asp
- SubscriptionHotelStart_52SP2.asp
- SubscriptionHotelSubscribe_52SP2.asp
- SubscriptionICSSStart_52SP2.asp
- SubscriptionICSSubscribe_52SP2.asp
- SubscriptionStart_52SP2.asp

Page Set Caveats

These caveats are associated with BBSM 5.2 page sets and are discussed in detail below:

- CSCdy52064
- CSCdy86714
- CSCdz02609
- CSCdz05331
- CSCdz87386
- CSCea02036
- CSCea41536



Caution

If you do not use the new page sets that this service pack installs in the c:\atcom\ekgnkm directory, these caveats remain unresolved, and the new page set fixes are not applied. For additional information, refer to the [“Resolved Caveats”](#) section below.

Resolved Caveats

This section describes the caveats that are resolved with BBSM 5.2 SP2.

- CSCdy06922
When the regional settings of the BBSM server are set to anything except English (United States), the access codes calendar days are no longer transposed, and they are processed correctly.
- CSCdy52064
For clarity, the Checkout button in the BiDirectional_DailyHotelStart.asp file has been changed to *View Folio and Checkout*. This affects the BiDirectional_DailyHotel page set.
- CSCdy77129
New Cisco Catalyst 2950 LRE switch type options have been added to the BBSM 5.2 server. These switches can be accessed from the Cisco Switch Type drop-down menu, which is located on the Switches web page in WEBconfig.
- CSCdy86714
Clients can now use blank passwords on the RADIUSstart.asp, RADIUSClearStart.asp, RADIUSUBandStart.asp, and RADIUSUBandClearStart.asp files. This change affects the RADIUS, RADIUSClear, RADIUSUBand, and RADIUSUBandClear page sets.
- CSCdz02609
When a client clicks the disconnect button while using the RadiusUband or RadiusUbandClear page set, the generated charge summary statement now shows the correct figures.
- CSCdz05331
When using Internet Explorer, Macintosh clients can now connect after they initially log on from the start page. This affects all page sets.
- CSCdz17812
The atnat.sys is more restrictive and no longer has a hole that allows http GET requests to pass through the system.
- CSCdz25560
The full functionality of the BBSM switch clustering feature is now restored. If a client connects to BBSM from a cluster member switch, BBSM detects the client on the correct port.
- CSCdz87386
When you map rooms using the Bi-Directional page set (configured for TCP/IP and two-way PMS), the *Accounting Request Failed* error message no longer appears. This affects the BiDirectional_DailyHotel page set.
- CSCdz87448
When you change PMS configurations in WEBconfig, the Athdmn service no longer hangs.
- CSCdz88767
The entire class attribute value is now sent in the accounting-request packet from the RADIUS server.
- CSCea02036
The default call type specified in the MegaPost.asp and MegaClearPost.asp files has been changed from *Default* to *Internet Session*. This change affects the Mega and MegaClear page sets.

- CSCea09282
When you run the Switch Discovery Wizard, the *SwitchDiscovery.exe - Entry Point Not Found - The procedure entry point IcmpCreateFile could not be located in the dynamic link library iphlpapi.dll.* error message no longer appears.
- CSCea41536
When a client is using the Daily access policy with the ICS Credit Card accounting policy, the session is now automatically disconnected at the session boundary, and the client is forced to re-authenticate. This change affects the DailyICS and DailyICSClear page sets.
- CSCea46801
When you add a Cisco Catalyst 4507 switch in WEBconfig, a port configuration can now be generated.
- CSCea49167
When using WEBconfig or Switch Discovery Wizard, you can now generate a port configuration for the Cisco Catalyst 6509 switch (with Supervisor I) and the Cisco Catalyst 4006 switch (with Supervisor II).
- CSCea54363
When you click the Restore Router Configuration button from the Bandwidth Reservation - External Router web page in WEBconfig, BBSM now restores the static policy map to the external router.
- CSCea58252
When clients are not in the Found state and they access the Post ASP page, BBSM no longer posts a phantom entry in Port_State_Radius table, which allows clients to connect.
- CSCea76386
If VLAN 1 is configured as a default management VLAN on the Cisco Aironet 1100 Series Access Point, clients can now connect, and a port configuration is generated.
- CSCeb10039
Atnat has been further modified with additional safeguards to prevent security holes that result from malformed GET requests.
- CSCeb20161
The sysObjectID for the Cisco Aironet 1230 Access Point has been added to the registry, and the Switch Discovery Wizard no longer discovers the 1230 access point as an unknown switch type.
- CSCeb37180
If the Yahoo Messenger client has either the proxy or client firewall settings enabled, Yahoo Messenger client can no longer send and receive messages without authenticating to BBSM.
- CSCeb56260
If the port hop delay is set for a longer period than a client's session timeout in a RADIUS prepaid case, the client's port hopping no longer stays in progress indefinitely.
- CSCeb58473
When a Macintosh iBook client connects to the BBSM network through a Cisco Aironet 1200 Series Access Point or through an Ethernet cable to a switch on the BBSM network, the BBSM server no longer reboots.
- CSCeb65884
When Atnat receives an invalid Address Resolution Protocol (ARP), it no longer reboots the BBSM server.

- CSCec23171
Clients can now connect to BBSM after making configuration changes to Cisco Aironet 1100 and 1200 Series (using Cisco IOS software) Access Points. These access points no longer stop working after configuration changes are made.
- CSCec42080
The Packet Inactivity timer now expires when a client is physically disconnected.
- CSCec49455
BBSM 5.2 SP2 no longer overwrites existing custom page sets.
- CSCed74734
When the Switch Discovery Wizard is used to configure Cisco Aironet access points, and you specify a non-default management VLAN ID for access points, the wizard incorrectly appends @<management VLAN ID> to the access point's SNMP password on BBSM. Consequently, clients cannot connect because Cisco access points do not support indexed passwords.

The workaround is to rediscover Cisco access points with the Switch Discovery Wizard without editing the BBSM VLAN ID field (by leaving the BBSM VLAN ID as 1), or to use WEBconfig to edit and remove @<VLAN ID> from the access point's SNMP password on BBSM.

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.

Related Documentation

The following documents provide information about BBSM:

- *Cisco BBSM 5.2 User Guide* (order number DOC-7814689=)
- *Cisco BBSM 5.2 and BBSD Software Installation Guide* (order number DOC-7812741=)
- *Cisco BBSM 5.2 Quick Start Guide* (order number DOC-7814813=)
- *Release Notes for the Cisco BBSM 5.2* (available on Cisco.com)

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/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/index.shtml>

- 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 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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. Go to this URL to visit the company store:

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *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 online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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>

- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.