



# Release Note for Cisco Wide Area Application Services

---

July 9, 2007



**Note**

---

The most current Cisco documentation for released products is also available on [cisco.com](http://cisco.com). The online documents may contain updates and modifications made after the hardcopy documents were released.

---

## Contents

This release note applies to Cisco Wide Area Application Services (WAAS), software versions 4.0.5, 4.0.3, and 4.0.1. For information on WAAS features and commands, refer to WAAS documentation located at [http://www.cisco.com/en/US/products/ps6870/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html).

This release note contains the following sections:

- [WAAS Product Overview](#)
- [Upgrading From WAFS to WAAS](#)
- [Upgrading from a Prerelease Version to Version 4.0.x](#)
- [WAAS Upgrade Requirements](#)
- [New Features](#)
- [WAAS Documentation Set](#)
- [Operating Considerations](#)
- [Software Version 4.0.5 Resolved Caveat](#)
- [Software Version 4.0.3 Open and Resolved Caveats](#)
- [Software Version 4.0.1 Open Caveats](#)
- [Documentation and Support Information](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

# WAAS Product Overview

The WAAS system consists of a set of devices called wide area application engines (WAEs) that work together to optimize TCP traffic over your network. When client and server applications attempt to communicate with each other, the network intercepts and redirects this traffic to the WAEs so they can act on behalf of the client application and the destination server. The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized.

You use the WAAS Central Manager GUI to centrally configure and monitor the WAEs and application policies in your network. You can also use the WAAS Central Manager GUI to create new application policies so that the WAAS system can optimize custom applications and less common applications.

Cisco WAAS helps enterprises meet the following objectives:

- Provide branch office employees with LAN-like access to information and applications across a geographically distributed network.
- Migrate application and file servers from branch offices into centrally managed data centers.
- Minimize unnecessary WAN bandwidth consumption through the use of advanced compression algorithms.
- Provide print services to branch office users. WAAS allows you to configure a WAE as a print server so you do not need to deploy a dedicated system to fulfill print requests.
- Improve application performance over the WAN by addressing the following common issues:
  - Low data rates (constrained bandwidth)
  - Slow delivery of frames (high network latency)
  - Higher rates of packet loss (low reliability)

## Upgrading From WAFS to WAAS

While WAFS to WAAS migration is supported, rollback from WAAS to WAFS is not supported. For information regarding a WAFS-to-WAAS migration, contact your Cisco Sales Engineer.

If you are upgrading from WAFS 3.0.7 to WAAS, you must upgrade only to a release version of WAAS 4.0.x; you cannot upgrade to a prerelease version of 4.0.x.

If you are upgrading from WAFS 3.0.7-special5 to WAAS, you must upgrade to WAAS 4.0.3 or later; you cannot upgrade to WAAS 4.0.1.

## Upgrading from a Prerelease Version to Version 4.0.x

When upgrading from WAAS prerelease software to version 4.0.x, perform one of the following steps to ensure a successful upgrade:

- Restore the factory default settings by using the **restore factory-default** command.
- Perform a fresh install from the rescue CD.

# WAAS Upgrade Requirements

Before you upgrade your WAE, you must run a script (the WAAS disk check tool) that checks the file system for errors that can result from a RAID synchronization failure. (For more information about RAID synchronization, see the “About RAID Synchronization and File System Errors” section on page 4.)

You can obtain the WAAS disk check tool from the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/waas40>



## Note

When you run the WAAS disk check tool, you will be logged out of the device. The device automatically reboots after it has completed checking the file system. Because this operation results in a reboot, we recommend that you perform this operation after normal business hours.

Copy the script to your WAE device by using the **copy ftp install** command.

```
WAE# copy ftp install <ftp-server> <remote_file_dir> disk_check.sh
```

Run the script from the CLI, as shown in the following example:

```
WAE# script execute disk_check.sh
This script will check if there is any file system issue on the attached disks
Activating the script will result in:
Stopping all services. This will log you out.
Perform file system check for few minutes.
and record the result in the following files:
/local1/disk_status.txt - result summary
/local1/disk_check_log.txt - detailed log
System reboot
If the system doesn't reboot in 10 minutes, please re-login and check the result files.
Continue?[yes/no] yes
Please disk_status.txt after reboot for result summary
umount: /state: device is busy
umount: /local1/PAM_unix[26162]: ### pam_unix: pam_sm_close_session (su) session closed
for user root
waitpid returns error: No child processes
No child alive.
```

After the device reboots and you log in, locate and open the following two files to view the file system status:

- **disk\_status.txt**—Lists each file system and shows if it is “OK,” or if it contains an error that requires attention.
- **disk\_check\_log.txt**—Contains a detailed log for each file system checked.

If no repair is needed, then each file system will be listed as “OK,” as shown in the following example:

```
WAE# type disk_status.txt
Thu Feb 1 00:40:01 UTC 2007
device /dev/md1 (/swstore) is OK
device /dev/md0 (/sw) is OK
device /dev/md2 (/state) is OK
device /dev/md6 (/local/local1/spool) is OK
device /dev/md5 (/local/local1) is OK
device /dev/md4 (/disk00-04) is OK
```

If any file system contains errors, the **disk\_status.txt** file instructs you to repair it.

## About RAID Synchronization and File System Errors

You must ensure that all RAID pairs are done rebuilding before you reboot your WAE device. If you reboot while the device is rebuilding, you risk corrupting the file system.

RAID pairs will rebuild on the next reboot after you enable WAFS core or edge services, use the **restore factory-default** command, replace or add a hard disk drive, delete disk partitions, or reinstall WAAS from the booted recovery CD-ROM.

To view the status of the drives and check if the RAID pairs are in “NORMAL OPERATION” or in “REBUILDING” status, use the **show disk details EXEC** command. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process can take several hours.

If you do not wait for the RAID pairs to complete the rebuild process before you reboot the device, you may see the following symptoms indicating a problem:

- The device is offline in the Central Manager GUI.
- CMS can not be loaded.
- Error messages say that the file system is “read-only.”
- The syslog contains errors such as “Aborting journal on device md2,” “Journal commit I/O error,” “Journal has aborted,” and “ext3\_readdir: bad entry in directory.”
- Other unusual behaviors related to disk operations or the inability to perform them.

If you encounter any of these symptoms, run the WAAS disk check tool to locate the problem. (For information about obtaining and using this tool, see the [“WAAS Upgrade Requirements” section on page 3.](#))

## New Features

WAAS software version 4.0.3 includes the following new features and changes:

- Support for WAAS network modules that are installed in Cisco integrated services routers.
- Support for user account domains. An account domain defines which devices or device groups that a user can manage.
- The Device Home window now reports the amount of memory installed in a device that is running software version 4.0.3 or later.
- There is a new CLI global configuration command named **[no] adapter epm enable**. The default state of the EPM (EndPoint Mapper) service is enabled after upgrading to WAAS software version 4.0.3. The default is disabled on a new WAE or after restoring factory defaults.

Use the **[no]** form of the command to disable the EPM service. Use this command without the **[no]** option to enable the EPM service. If the running configuration does not show this command, it indicates that the EPM service is enabled. If the EPM service is disabled, then the running configuration will show that.

This command corresponds to a new Enable EPM Adapter check box in the WAAS Central Manager GUI. This setting is available in the Acceleration > General Settings window, after you have chosen a device or device group to edit.

# WAAS Documentation Set

In addition to this document, the WAAS documentation set includes the following publications:

- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Using the Print Utilities to Troubleshoot and Fix Samba Driver Installation Problems*

## Operating Considerations

This section includes operating considerations that apply to software versions 4.0.1, 4.0.3, and 4.0.5:

- [Using Full-Duplex Connections](#)
- [WAAS Print Driver Support and Interoperability](#)
- [WAAS Print Services CUPS Log Files](#)
- [Ensuring Subnets are Reachable using Static or Dynamic Routing Protocols](#)
- [Configuring a WAE for Maximum Performance on High Bandwidth Delay Product \(BDP\) Links](#)
- [Disabling the Automatic Machine Account Password Changes for the Edge WAE](#)

## Using Full-Duplex Connections

We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

## WAAS Print Driver Support and Interoperability

WAAS WAE incorporates a Print Server based on the integration of open source Samba and CUPS technology. During the testing process, it has been determined that certain Print Drivers with complex features, such as sophisticated paper handling, may not be Point-and-Print compatible with WAAS. Most notably, Fiery Drivers incorporated into some Printer Manufacturer solutions are not compatible with Samba. Other Multi Function Printers (MFP) may also have limited functionality when working with Samba and are not supported by WAAS.

To determine if a Print Driver is compatible with WAAS, perform the Add Driver processes with a WAE using the Add Printer Wizard. Compare all the client Print features available after creating a print queue and compare it to a similar installation on a Microsoft Windows Print Server. If there are obvious feature inconsistencies, it is indicative of a Print Driver that cannot be used with WAAS Print Server for Point-and-Print. As a workaround, an installation on each client desktop from a CD or other source will be required.

When using the WAAS print services in a Windows XP Pro/Windows 2003 Server environment, you must register the WAE with Active Directory for the automatic printer driver download feature to operate correctly. This is due to a default computer policy for domain members that does not allow the host to download drivers from an unregistered device. A user will see a message similar to the following when encountering this issue: “A policy is in effect on your computer which prevents you from connecting to this print queue. Please contact your system administrator.”

The WAAS print solution does not offer authentication. Any user may access and send print jobs to the WAAS print server. Also, WAAS supports 32-bit drivers.

## WAAS Print Services CUPS Log Files

Common Unix Printing System (CUPS) log files are rotated when the log file reaches the maximum size of 1 MB.

## Ensuring Subnets are Reachable using Static or Dynamic Routing Protocols

The Cisco WAAS provides transparent optimizations, which preserves source and destination IP addresses and TCP header information. Because of this, the Cisco WAE device must be deployed on separate subnets than those existing on the LAN, both on the server side and on the client side. These standalone subnets, and the Cisco WAE devices attached to them, must be reachable from the Central Manager and other WAE devices. Ensure that these subnets are reachable using static or dynamic routing protocols. If the subnets are not reachable, critical WAE functions may be impaired, including file protocol optimizations, WAE management, central management, and management authentication.

## Configuring a WAE for Maximum Performance on High Bandwidth Delay Product (BDP) Links

Cisco WAAS can be deployed in different network environments, involving multiple link characteristics (bandwidth, latency, packet loss, etc.). All systems are optimized by default to accommodate networks with maximum Bandwidth Delay Product (BDP) up to the values listed below:

- WAE-511/512: DefaultBDP = 32KB
- WAE-611/612: DefaultBDP = 512KB
- WAE-7326: DefaultBDP = 2048KB

In cases where higher bandwidth is available or higher latencies are involved, replace BDP with 2048KB. Use the following example to configure BDP from the WAAS CLI:

```
#config t
(config)#tfo tcp optimized-receive-buffer BDP
(config)#tfo tcp optimized-send-buffer BDP
(config)#exit
#write
```

To configure BDP from the WAAS Central Manager GUI:

1. Go to Devices > Devices or Device > Groups.
2. Click the Edit icon next to the device for which you want to configure BDP.
3. From the Contents pane, select Acceleration > Acceleration TCP Settings.
4. In the Receive Buffer Size > Optimized Side field, apply the BDP value as calculated above.
5. In the Send Buffer Size > Optimized Side field, apply the BDP value as calculated above.
6. Click Submit. Changes will be applied within a configuration distribution cycle (default 5 min).

## Disabling the Automatic Machine Account Password Changes for the Edge WAE

In a WAAS network where a Windows domain controller is configured for authentication and Disconnected Mode is enabled on an edge WAE, the domain controller authenticates content requests in the event of a WAN failure. By default, Windows domain controllers enforce automatic machine account password changes as part of the authentication process. The machine account password for the edge WAE is automatically negotiated and changed between the edge WAE and the domain controller every seven days. However, if the authentication service is down, this process may not occur, and the machine account password for the edge WAE may expire.

To prevent this situation, we recommend that you disable automatic machine account password changes for the edge WAE. The procedure that follows describes how to disable automatic machine account password changes for Windows XP and Windows Server 2003 using Group Policy Editor. Refer to Microsoft's Help and Support page for details on how to disable automatic machine account password changes for other Windows operating systems.

To disable the automatic machine account password changes for the edge WAE using Group Policy Editor:

1. On the domain controller, click Start, then select Run.
2. Type **Gpedit** at the prompt, then click OK.
3. Expand the Local Computer Policy, Windows Settings, Security Settings, Local Policies, Security Settings, Local Policies, Security Options.
4. Configure the following setting: Domain Member: Disable machine account password changes (DisablePasswordChange).

## Software Version 4.0.5 Resolved Caveat

The following caveat was resolved in software version 4.0.5:

- **CSCse36646**—The WAE file system might be corrupted when RAID is used.

## Software Version 4.0.3 Open and Resolved Caveats

The following sections list the open and resolved caveats for software version 4.0.3:

- [Software Version 4.0.3 Open Caveats](#)
- [Software Version 4.0.3 Resolved Caveats](#)

### Software Version 4.0.3 Open Caveats

The following caveats apply to software version 4.0.3:

- **CSCsd89635**—Certain server-side applications do not function correctly due to the presence of auto-discovery TCP options. Workaround: None.
- **CSCse36646**—A WAE-612 may have file system corruption under rare circumstances. When the problem occurs, the WAE may go into a state where the corrupted disk partition is being remounted as read only with the message “Remounting filesystem read-only” in the syslog. The following syslog errors occur:

```
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-2-900000: EXT3-fs error (device md2):
ext3_new_block: Allocating block in system zone - block = 1507328
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-3-900000: Aborting journal on device
md2.
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-3-900000: ext3_reserve_inode_write:
aborting transaction: Journal has aborted in __ext3_journal_get_write_access<2>EXT3-fs
error (device md2) in ext3_reserve_inode_write: Journal has aborted
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-2-900000: ext3_abort called.
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-2-900000: EXT3-fs error (device md2):
ext3_journal_start_sb: Detected aborted journal
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-2-900000: Remounting filesystem
read-only
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-2-900000: EXT3-fs error (device md2)
in ext3_ordered_commit_write: Journal has aborted
May 26 05:34:56 sats-waas-612-e1 kernel: %CE-SYS-4-900000:
__journal_remove_journal_head: freeing b_committed_data
```

Workaround: Delete both disks of the affected partition, reload the device, and reinstall the image.

- **CSCse62556**—When trying to access the ~snapshot folder on a Netapp file server using the “.snapshot” name, the folder is inaccessible using WAFS. Workaround: Use ~snapshot instead of .snapshot to access the backup copies. Or configure snapshot folders to be visible in CIFS (they will still be hidden in Windows Explorer) using **cifs.show\_snapshot on** in the Netapp configuration and then access the visible folder.
- **CSCsg04648**—On the NME-WAE device, the kernel enters KDB just after a reboot from a rescue image with a trace back from ad\_synccache. Workaround: If the problem occurs, reboot from KDB and the next boot will succeed. To prevent this problem from occurring, after the rescue image states that it is rebooting, go to the shell in the router and enter the command **service-module integrated-service-module slot/0 reset**. Then the card will reboot as normal.

- **CSCsg11506**—EPM (EndPoint Mapper) breaks connections if it does not intercept both traffic directions, so EPM-based applications are unavailable in asymmetric routing scenarios. This occurs when a WAE has visibility to only one side of a TCP connection. Because of router configuration or network topology, the return traffic bypasses the WAE. For example, this would occur if WCCP redirection is configured on some router interfaces but not all. When using WCCP redirection in a router with two WAN and one LAN interface must have interception configured on all three WAN and LAN interfaces. If one WAN interface is omitted, EPM traffic from that interface will not be handled properly. Workaround: Ensure that both WCCP service groups 61 and 62 are on the same interface, which is the WAN interface that connects to another WAE-accelerated site. Alternatively, configure WCCP redirection in on all relevant interfaces.
- **CSCsg14550**—Service 89 does not perform WCCP bypass return for CIFS servers that are not in the WAFS acct list. This may occur when the WAE device is not on its own interface/subnet separate from the clients or servers, or if it is on its own interface/subnet, the interface to the redirecting router or switch is not configured properly to support the WCCP L2 return of packets. Workaround: Change the network to accommodate L2 packet return. Migrating from WAFS 3.0 to WAAS 4.0 requires network changes because WAAS does L2 return and WAFS does WCCP GRE return for CIFS servers that are not being optimized.
- **CSCsg22705**—On successive upgrades and downgrades, multiple role entities are created with the same name. Workaround: Delete all role entities named all-waes-dgs.
- **CSCsg24304**—Under some circumstances, flow protection may stop working and active connections may hang or be reset when new WAEs are added to the WCCP cache farm. This problem is seen when an FTP Get request is made to request a large file from a server in the data center and the request is served through one of the WAEs in the WCCP cache farm. At the same time, a new WAE is added to the existing WCCP cache farm and causes the recalculated hash/mask assignment to redirect the FTP request to the new WAE. Workaround: Add or remove WAEs from the WCCP cache farm only when the traffic through the WAEs is light or nonexistent.
- **CSCsg25863**—When you try to create a new classifier, the Central Manager may give you the message “Could not add new Application Classifier, Application classifier name already exists.” Workaround: Reinitialize the policy engine configuration using one of the following CLI commands: **policy-engine config remove-all** or **policy-engine config restore-predefined**.
- **CSCsg39177**—The windows authentication method is not properly enabled from the Central Manager Windows domain page after restoring factory-defaults. Workaround: Unregister the WAE from the domain controller (after seeing the problem) using the CLI command **windows-domain diagnostics net "ads leave"**. Then reregister the WAE from the Central Manager.
- **CSCsg46821**—There is an internal error when WCCP is disabled while the WAE is optimizing connections and traffic is flowing through the device. Because WCCP is being disabled, the connections through the WAE are going to be dropped anyways, and there is no additional impact from this problem. The error is indicated by the following messages in the console and syslog:
 

```
"Badness in pe_add_fltr_pkt_statistics at
/users1/waas_4.0.3-b1/bfc/linux/kernel-2.6.x/cisco/policy_engine_core.c:5593"
```

 Workaround: None required.
- **CSCsg50460**—The CMS status becomes offline and restarts when you select a printer driver to be downloaded and then deselect the driver while it is being downloaded by device. Workaround: Wait until the printer driver download is finished by the device before deselecting the driver in the Central Manager.
- **CSCsg55474**—A Central Manager running version 4.0.1 is able to configure a NME-WAE-302 device with 512 MB RAM as a WAFS edge and core device, and the memory is insufficient to support WAFS operation. Workaround: Do not configure a NME-WAE-302 device with 512 MB RAM as a WAFS edge or core device.

- **CSCsg55609**—The Central Manager restore operation does not restore the print services configuration, which disables the print service that had been enabled when the backup was created. Workaround: After the restore operation, enable and configure the print service on the device (assign print drivers).
- **CSCsg59943**—A java core dump is sometimes created on a WAE when it first registers with the Central Manager. The root cause is unknown. Workaround: None required. The management agent will restart automatically.
- **CSCsg60239**—CMS import fails during upgrade process from WAFS to WAAS. Workaround: Manually apply changes where needed and then restart the management service.

## Software Version 4.0.3 Resolved Caveats

The following caveats were resolved in software version 4.0.3:

- **CSCsd53423**—WCCP field is Not Applicable on the IP ACL Page in the Central Manager.
- **CSCsd81901**—Windows-domain users fail to be authenticated. Authentication will not work properly if you enable windows-domain authentication using a CLI command prior to registering the device with the Domain Controller.
- **CSCse23864**—Cannot complete a software upgrade while in Disconnected mode.
- **CSCse51806**—When the WAE is busy or starting up and internal access to print status information is unavailable, a non-critical Java exception is logged in the CMS error log (errorlog/cms\_log.current).
- **CSCse63098**—When there are a large number of optimized connections, additional internal memory cannot be allocated to perform LZ compression in the DRE compression module. This may result in lower than possible compression and throughput.
- **CSCse70800**—The Central Manager Export icon freezes the GUI when the file is saved.
- **CSCse76023**—The system error ‘System Had Trouble Processing Last Request’ is received after exceeding 256 Acceleration Applications for a WAE.
- **CSCse99631**—When you restore the database on a CM, nearly all CLI commands for which there are equivalent GUI pages that you configured for the CM devices may retain their default settings.
- **CSCsf02435**—If you perform a software upgrade of an edge WAE while the edge WAE is disconnected from the core WAE, the edge does not function in Disconnected mode until after it is reconnected to the core WAE.
- **CSCsf02491**—The Central Manager Authentication Status Window reports Not OK for “wbinfo -D” and “wbinfo - sequence”.
- **CSCsf02616**—When navigating from the Central Manager GUI Page ‘System > AAA > User > Create or Modify’ directly to the ‘System > AAA > Password’ without previously clicking Submit or Cancel on the User Form, a Central Manager GUI error message is displayed.
- **CSCsf04135**—The HTTP Status 404 is displayed in the Central Manager when navigating from the View detail report button of ‘System-Wide Application Traffic Mix for last month’ or ‘System-Wide Reduction(%)’ to other screens.
- **CSCsf09130**—The Time Zone configuration is not reflected in the CLI. Summer Time configured with absolute dates fails when the configured start date is today, but with the start time in the past or when the start date is in the past.

- **CSCsf17513**—Print spooling fails when a Windows print client spools to a WAAS print server across an optimized connection (which may occur if the client is in a data center and the print server is in a branch office).
- **CSCsf21056**—If you issue the **restore factory-default preserve basic-config** command prior to upgrading the software, the original software will not be maintained on the WAE. Therefore, performing a rollback to the earlier version will fail.

## Software Version 4.0.1 Open Caveats

The following open caveats apply to software version 4.0.1:

- **CSCsc71589**—Home shares of other users are shown on Disconnected mode. This bug applies to NetApp and Windows Servers, but does not apply to EMC file servers. In NetApp, you (as administrator) can create a home directory for a user on a remote server with a matching name. When a user logs on to a server, he will see a share named after his user name. This share is actually a link to a directory that is defined for each user, usually under <server>\home\user. The default permission to all user home directories is 'Everyone'. When you switch to Disconnected mode, you see all of the other users' shares as well as your own share. This can be considered as a security breach under at least the following two scenarios:
  - If you deny List Permissions to the 'home' directory (which contains all the user's home directories). In this case, in native mode you cannot enter this directory and see its contents. But in DM you will see all the contents under the root share.
  - If you define the 'home' directory as hidden (using \$) in native mode, you will not see it. In DM, you will still see all its contents under the root. In both cases, if the default 'everyone' permission given to home dirs was not changed, then in DM you can access files that cannot be accessed in connected mode.

Workaround: Change permissions to home directories from 'everyone' to a specific user only so that another user can only see the share, but not access it.

- **CSCsd53423**—WCCP field Not Applicable on IP ACL Page in the Central Manager. The IP ACL Feature Usage page for the Central Manager device in the CM GUI has an option for 'WCCP'. Because content requests are not handled by the CM, WCCP is not supported on the CM, and this option is not valid for the CM device mode. If you configure this option, you will see a CLI failure error message on the system messages page and the page will correctly reflect 'do not set' in one polling period. The error message is always present on the page, though it is not relevant to the CM. Workaround: None required. The setting will be cleared from the CM GUI in one polling period.
- **CSCsd81901**—Windows-domain users fail to be authenticated. Authentication will not work properly if you enable windows-domain authentication using a CLI command prior to registering the device with the Domain Controller. Workaround: Register the device with the Domain Controller before you enable windows-domain authentication.
- **CSCse18421**—A NetBIOS client cannot connect to a file server in transparent mode (on port 139 only) by using the file server's NetBIOS name if the NetBIOS name is different than the DNS name of that server, and the file server is registered in the Central Manager using only its DNS name. This can happen on file servers that are configured with NetBIOS names or aliases and DNS names or aliases that are different. Workaround: Use the **Services > File > File Servers** window to register the file server in the Central Manager with its NetBIOS name instead of its DNS name or ensure that all of the file server's NetBIOS and DNS names and aliases are registered in the Central Manager.
- **CSCse23864**—Cannot complete a software upgrade while in Disconnected mode. Workaround: Perform a software upgrade while connected to the Central Manager and Core WAE, but not while in Disconnected mode.

- **CSCse30014**—DRE compression ratio is lower than expected in first hot pass after issuing the **clear dre cache** command. After issuing the **clear dre cache** command, the first one Mbyte of data passed between a WAE Core and WAE Edge is not optimized. Workaround: When performing WAAS testing of throughput and compression ratios, in addition to issuing the **clear dre cache** command, transfer one Mbyte of un-related data for the first connection between the peers.
- **CSCse51806**—When the WAE is busy or starting up and internal access to print status information is unavailable, the following non-critical Java exception is logged in the CMS error log (errorlog/cms\_log.current):

```
08/14/2006 04:33:56.995(Local) [W] ce(DataFeedPoll): java.io.IOException:
dsc/nativeGetIntItem: Failed for item=/cfg/print-services/enable sysdb_errno=63: ja
va.io.IOException: dsc/nativeGetIntItem: Failed for item=/cfg/print-services/enable
sysdb_errno=63
```

Workaround: None required. The error code indicates that the device is too busy to respond with print server status. The manager service automatically retries to retrieve the print status information required.

- **CSCse62278**—Using Windows Add Printer Wizard with Print Driver's for NT4 Operating System fails. If you add a Print Driver intended for NT4 compatibility to the Central Manager Print Repository, it may fail if the driver contains a 0 byte file (example 0 byte .DAT file). Workaround: Perform the following steps after the failure message in Add Printer Wizard appear:
  1. Log on to the CM CLI.
  2. Type 'cd spool/samba/printers/W32X86' .
  3. Type 'ls' .
  4. Remove the SKIP dirs by entering 'rmdir <SKIP>' .
  5. Go back to the Windows client.
  6. Click on the Finish button on the APW.
  7. When prompted for the drivers for NT4, browse to the directory that contains the ML500.inf and click on 'Open'.
  8. Click 'OK'.
  9. Click 'Yes' on the digital signature warning. The driver should be successfully downloaded.
- **CSCse63098**—When there are a large number of optimized connections, additional internal memory cannot be allocated to perform LZ compression in the DRE compression module. This may result in lower than possible compression and throughput. The following syslog message indicates memory allocation failure for LZ encode buffers:

```
LZ buffer error: Failed to allocate LZ encode buffer (size %d) for conn-id=%d (%d are
replaced with numbers)
```

Workaround: This error message can be ignored because basic DRE compression is still being performed. Reducing the number of connections or using a WAE with a higher capacity will reduce the frequency of this problem.

- **CSCse64582**—CIFS (WAFS) disconnected read mode does not work after reloading an edge WAE. The client receives an 'Internal Error' message and the filer is not available in Disconnected mode. Workaround: Use one of the following workarounds:
  - After reloading the edge WAE, execute the **windows-domain diagnostics wbinfo "-t"** command. The CIFS (WAFS) Disconnected Read Mode should start working.

- Go to the Central Manager WAE GUI > Configuration > Windows Authentication page and click on the ‘Show Authentication Status’ button. After checking the authentication status from the GUI (which should report the status to be OK), Disconnected mode starts working.
- Issue the **service restart winbindd** command.
- **CSCse70800**—The Central Manager Export icon freezes the GUI when the file is saved. With certain versions of Internet Explorer, performing CSV export and selecting the Save option rather than selecting the Open option may freeze the GUI. Workaround: When prompted to Save or Open the file, select Open, and then Save the file.
- **CSCse76023**—The system error ‘System Had Trouble Processing Last Request’ is received after exceeding 256 Acceleration Applications for a WAE. After removing factory default Applications, and then creating a maximum of 256 Applications, you cannot restore factory defaults. This occurs because it would exceed the 256-Application limit. Workaround: To minimize the potential for exceeding internal limits:
  1. Do not exceed the 256 limit.
  2. If the device has many applications, minimize the number of Device Groups in which it is configured.
  3. If an error occurs, remove the applications and retry.
- **CSCse80058**—WAE 611 devices temporarily report a status of offline after a major configuration change. If you have a large number of devices registered to a CM and you perform a major operation that affects all devices (for example, upgrading all devices simultaneously), it may take more than 2 polling periods (2\*5 minutes or 10 minutes, by default) for all devices to synchronize their configuration with the CM. During this time, the CM GUI will show some devices as offline until all the devices have been synchronized. While offline, the devices are able to serve requests, though they may not have the latest configuration changes made on the CM. Workaround: None required. The devices eventually synchronize with the CM, but it may take 10 minutes or longer. Consider running a higher-performance model as the CM if you perform such operations regularly.
- **CSCse83854**—When using the Central Manager to assign some or all WAE to a Device Group, certain WAEs cannot be assigned to a Device Group. If a WAE is already configured with 256 applications, adding it to a Device Group with application definitions will result in exceeding the 256 limit. Workaround: Do not assign a WAE that already has 256 applications to a Device Group, or eliminate some of the applications on the device.
- **CSCse87762**—WAE 612 devices temporarily report a status of offline after a major configuration change. If you have a large number of devices registered to a CM and you perform a major operation that affects all devices (for example, upgrading all devices simultaneously), it may take more than 2 polling periods (2\*5 minutes or 10 minutes, by default) for all devices to synchronize their configuration with the CM. During this time, the CM GUI will show some devices as offline until all the devices have been synchronized. While offline, the devices are able to serve requests, though they may not have the latest configuration changes made on the CM. Workaround: None required. The devices eventually synchronize with the CM, but it may take 10 minutes or longer. Consider running a higher-performance model as the CM if you perform such operations regularly.
- **CSCse99631**—When you restore the database on a CM, nearly all CLI commands for which there are equivalent GUI pages that you configured for the CM devices may retain their default settings. Workaround: Navigate to the related Central Manager configuration page and perform a Save to force the correct settings rather than the defaults settings.
- **CSCsf02435**—If you perform a software upgrade of an edge WAE while the edge WAE is disconnected from the core WAE, the edge does not function in Disconnected mode until after it is reconnected to the core WAE. Workaround: Do not perform a software upgrade if the WAE Edge is disconnected from the WAE Core. If the problem occurs, reconnect the edge to the core.

- **CSCsf02491**—The Central Manager Authentication Status Window reports Not OK for “wbinfo –D” and “wbinfo – sequence”. If NTLM authentication is being used and WINS has not been configured, the Authentication Status Window shows these errors. However, registration is successful. It is the status “wbinfo” that is incorrect. Workaround: Configure WINS to eliminate the errors.
- **CSCsf02616**—When navigating from the Central Manager GUI Page ‘System > AAA > User > Create or Modify’ directly to the ‘System > AAA > Password’ without previously clicking Submit or Cancel on the User Form, the following Central Manager GUI error message is displayed:

"Sorry, but because the CLI user for this account was not created from CM GUI, you cannot change your password from the CM GUI" may appear.

Workaround: Click on any page in the GUI and return to ‘System > AAA > Password’.

- **CSCsf04135**—The HTTP Status 404 is displayed in the Central Manager when navigating from the View detail report button of ‘System-Wide Application Traffic Mix for last month’ or ‘System-Wide Reduction(%)’ to other screens. Workaround: Click on the browser refresh button.
- **CSCsf09025**—The WAE Print Server is not available in an Active Directory Search. If the WAE NetBIOS name and DNS name are different, then publishing and searching using the Active Directory does not function. Workaround: It is a best practice to keep the WAE DNS and NetBIOS name the same, which is the default.
- **CSCsf09130**—The Time Zone configuration is not reflected in the CLI. Summer Time configured with absolute dates fails when the configured start date is today, but with the start time in the past or when the start date is in the past. Workaround: Use the **recurring** option to create a recurring summertime setting instead of a fixed date summertime.
- **CSCsf10382**—The CM reports the error message ‘Incorrect number of columns’ when trying to import file servers using the import tool even though the number of columns entered is correct. This condition is seen when there are two or more clusters to be assigned to some of the filers and no clusters to be assigned to some of the filers. Workaround: Instead of leaving the unused columns empty, use space characters.

This is an example of a correct configuration:

```
Name, Type, UsingTCP, UsingUDP, AllowDisconnected, Cluster, Cluster
filer1, CIFS, FALSE, FALSE, TRUE, ,
```

This is an example of an incorrect configuration:

```
Name, Type, UsingTCP, UsingUDP, AllowDisconnected, Cluster, Cluster
odi-23k-srv1, CIFS, FALSE, FALSE, TRUE, ,
```

- **CSCsf17513**—Print spooling fails when a Windows print client spools to a WAAS print server across an optimized connection (which may occur if the client is in a data center and the print server is in a branch office). Workaround: Define a traffic policy of Pass-Through for the source and destination pair.
- **CSCsf21056**—If you issue the **restore factory-default preserve basic-config** command prior to upgrading the software, the original software will not be maintained on the WAE. Therefore, performing a rollback to the earlier version will fail. Workaround: If you need to revert to an earlier version of software, you must use the software upgrade procedure.
- **CSCsf22341**—The Central Manager (CM) alarm is not always cleared after a corrective action is taken. If a CM alarm is present and the action is taken to clear the alarm, the alarm may not be cleared in the CM. Workaround: Perform the action again to clear the alarm.

# Documentation and Support Information

This section contains the following topics:

- [Obtaining Documentation](#)
- [Documentation Feedback](#)
- [Cisco Product Security Overview](#)
- [Product Alerts and Field Notices](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

### Cisco.com

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

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

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](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

## Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

## Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

## 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — [security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — [psirt@cisco.com](mailto:psirt@cisco.com)

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

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



**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

## Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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 at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation 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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

**Tip**

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

## 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 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 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)—An existing 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 operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:  
<http://www.cisco.com/offer/subscribe>
- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:  
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, 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>
- *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>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:  
<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>
- 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>

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)

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.

© 2006, 2007 Cisco Systems, Inc. All rights reserved.