



Release Note for Cisco Wide Area Application Services Software Version 4.1.1x

July 17, 2009



Note

The most current Cisco documentation for released products is available on Cisco.com.

Contents

This release note applies to the following software versions for the Cisco Wide Area Application Services (WAAS) software:

- 4.1.1d
- 4.1.1c
- 4.1.1b
- 4.1.1a
- 4.1.1

For information on WAAS features and commands, see the WAAS documentation located at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

This release note contains the following sections:

- [New Features](#)
- [Windows Server on WAAS](#)
- [Upgrading From WAFS to WAAS](#)
- [Upgrading from a Prerelease Version to Version 4.1.1](#)
- [Upgrading from Version 4.0.x to 4.1.1](#)
- [Downgrading from Version 4.1.1 to a Previous Version](#)
- [Cisco WAE and WAVE Appliance Boot Process](#)
- [Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade](#)



Americas Headquarters:

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

- [Operating Considerations](#)
- [Software Version 4.1.1d Resolved and Open Caveats](#)
- [Software Version 4.1.1c Resolved Caveats, Open Caveats, and Command Changes](#)
- [Software Version 4.1.1b Resolved and Open Caveats](#)
- [Software Version 4.1.1a Resolved and Open Caveats](#)
- [Software Version 4.1.1 Resolved Caveats, Open Caveats, and Command Changes](#)
- [WAAS Documentation Set](#)
- [Obtaining Documentation and Submitting a Service Request](#)

New Features

WAAS software version 4.1.1 includes the following major new features and changes:

- Several new transparent application accelerators that optimize and accelerate the following application traffic:
 - CIFS—Accelerates CIFS traffic exchanged with a remote file server. This accelerator replaces the functionality provided by the legacy WAFS feature (which is still available), and greatly simplifies configuration.
 - HTTP—Accelerates HTTP traffic.
 - MAPI—Accelerates Microsoft Outlook Exchange traffic that uses the Messaging Application Programming Interface (MAPI) protocol. Microsoft Outlook 2000–2007 clients are supported.
 - NFS—Accelerates Network File System (NFS) version 3 traffic exchanged with a remote file server.
 - Video—Accelerates Windows Media live video broadcasts that use RTSP. The video accelerator automatically splits one source video stream from the WAN into multiple streams to serve multiple clients on the LAN.
 - Windows Print—Accelerates print traffic between clients and a Windows print server located in the data center.
- Virtualization—Virtual blades allow you to add services running in their own emulated hardware environments to your WAAS system. For example, you could configure a virtual blade in a WAE device to run Windows services such as Print Services, Active Directory Services, DNS, and DHCP services. Virtual blades are supported only on certain models of WAE and WAVE devices.
- Directed Mode—Peer WAEs can exchange traffic using UDP encapsulation to avoid firewall traversal issues.
- WAAS Central Manager GUI enhancements—The WAAS Central Manager GUI has an updated look and feel, reorganized navigation for easier use, a GUI for the troubleshooting tool, and a GUI for defining SNMP traps.
- Monitoring and Reporting—New Monitoring and Reporting drawers in the WAAS Central Manager provide many new functions that allow you to monitor the system operation, define custom reports, and schedule periodic reports for email delivery.
- Read-only access control—Allows you to restrict access to certain GUI pages by making them read-only for a particular user role.

- **Generic GRE Egress Method**—WCCP intercepted connections can use the generic GRE egress method, which encapsulates returned data in GRE frames. The generic GRE egress method is designed specifically to be used in deployments where the router or switch does hardware accelerated processing of GRE packets, such as with the Cisco 7600 series router or the Catalyst 6500 series switch with the Supervisor Engine 32 or 720.
- **Transport enhancements**—Adaptive buffering allows the WAAS software to dynamically vary the size of the send and receive buffers to increase performance and more efficiently use the available network bandwidth. DRE enhancements increase performance.
- **External authority group membership**—You can create user groups if you are using external authentication of users on a TACACS+ or Windows domain server (not a RADIUS server). By creating user group names that match the user groups that you have defined on the external authentication server, WAAS can dynamically assign roles and domains to users based on their membership in a group as defined on the external authentication server.
- **DSCP Marking by Policy**—Application policies can include a DSCP marking attribute to enable different levels of service to be assigned to network traffic.
- **Licensing Manager**—Manages software licenses that are required to enable specific features.
- **Upgrade enhancements**—Allows you to upgrade a WAAS Central Manager before the WAEs that it manages.
- **Setup utility enhancements**—Allows you to get a new WAAS device configured more quickly because more setup steps are automated.
- **Monitoring API**—Allows you to access the monitoring statistics and status information on a WAAS Central Manager through a programmatic interface that uses XML-formatted SOAP requests.
- **New hardware platform support**—Includes support for the following new hardware platforms: WAVE-274, WAVE-474, and WAVE-574.

Windows Server on WAAS

WAAS software version 4.1.1 contains support for the Windows Server on WAAS product, which is Windows Server 2008 Core running in a virtual blade on a supported WAAS device. This product supports running only the following Windows services: Active Directory, Print Services, DHCP, and DNS.

You can purchase a WAAS device with the Windows Server on WAAS installer ISO image already stored on the hard disk of the WAAS device, or you can purchase a field upgrade for supported WAAS devices.

You can also install your own copy of Windows Server on an existing WAAS device that has virtual blade capability and for which you have purchased the virtual blade license. The WAE devices that support virtual blades support Windows Server 2003 R2 with SP2 (32-bit Enterprise Edition) and all 32-bit and 64-bit editions of Windows Server 2008.

Upgrading From WAFS to WAAS

Although WAFS to WAAS migration is supported, a 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 or later to WAAS, you must upgrade to a released WAAS version; you cannot upgrade to a prerelease version of WAAS software.

If you are upgrading from the WAFS 3.0.7-special5 build or from a later WAFS release to WAAS, you must upgrade to a minimum of WAAS 4.0.5 or later; however, to ensure that you obtain all of the latest fixes and features, we recommend that you upgrade to the most current version of WAAS.

Note the following points when upgrading from WAFS to WAAS:

- When you upgrade from WAFS to WAAS, you may lose up to half of the WAFS cache space because the upgrade process uses the WAFS cache eviction process to reclaim the space needed for the DRE cache; the oldest content is removed first.
- The hardware that supports WAFS 3.0 also supports WAAS, with the exception of the NM-CE.
- You need a dedicated WAE to function as the Central Manager in WAAS.
- You must place the WAEs in a separate subnet from the clients, or you must use the GRE return feature.

Upgrading from a Prerelease Version to Version 4.1.1

To upgrade from WAAS prerelease software to version 4.1.1, you must perform the following tasks 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.

Upgrading from Version 4.0.x to 4.1.1

This section contains the following topics:

- [Requirements and Guidelines](#)
- [Ensuring a Successful RAID Pair Rebuild](#)
- [Managing Passwords after an Upgrade](#)

Requirements and Guidelines

When you upgrade from version 4.0.x to version 4.1.1, observe the following guidelines and requirements:

- To take advantage of new features and bug fixes, we recommend that you upgrade your entire deployment to the latest version.
- If you operate a network with devices that have different software versions, the WAAS Central Manager must be the highest version.
- Upgrading to version 4.1.1 is supported only from version 4.0.13 and later. If you want to upgrade WAAS devices running earlier versions, first upgrade them to version 4.0.13, 4.0.17, or 4.0.19, then to 4.1.1.
- Upgrade the WAAS Central Manager devices first, and then upgrade the WAE devices. If you have a standby WAAS Central Manager, upgrade it first, before upgrading the primary WAAS Central Manager. After upgrading, restart any active browser connections to the WAAS Central Manager.

- Before upgrading a WAAS Central Manager to version 4.1.1, make a database backup by using the **cms database backup** EXEC command. This command creates a backup file in /local1/. In case of any problem during the upgrade, you can restore the database backup that you made before upgrading by using the **cms database restore** *backup-file* EXEC command, where *backup-file* is the one created by the backup command.
- If you upgrade a WAAS Central Manager to 4.1.1 using the **Jobs > Software Update** page from a 4.0.x WAAS Central Manager, enter 4.1.1.0.1 in the Software Version field.
- After upgrading application accelerator WAEs, verify that the proper licenses are installed by using the **show license** EXEC command. The Transport license is enabled by default. If WAFS was enabled on the device before the upgrade, then the Enterprise license should be enabled. Configure any additional licenses (Video and Virtual-Blade) as needed by using the **license add** EXEC command. For more information on licenses, see the “[Managing Software Licenses](#)” section on page 9-3 in the *Cisco Wide Area Application Services Configuration Guide*.
- After upgrading application accelerator WAEs, verify that the proper application accelerators, policies, and classifiers are configured. For more information on configuring accelerators, policies, and classifiers, see [Chapter 12, “Configuring Application Acceleration”](#) in the *Cisco Wide Area Application Services Configuration Guide*.
- WAAS version 4.1.1 supports strong passwords. When you upgrade from version 4.0.17 or an earlier version, which does not support strong passwords, the previous weaker passwords will be retained. For details, see the “[Managing Passwords after an Upgrade](#)” section on page 6.
- If you are upgrading a WAAS Central Manager from version 4.0.19 and have the secure store enabled, you will need to reopen the secure store after the device reloads (and after any reload). Use the **cms secure-store open** EXEC command. For more information on using the secure store, see the “[Configuring Secure Store Settings](#)” section on page 9-10 in the *Cisco Wide Area Application Services Configuration Guide*.
- If you are upgrading a WAE-511 or WAE-611, ensure that the BIOS disk mode is set to Native.
- When upgrading a WAE to version 4.1.1, the name of the default traffic policy for NFS traffic remains NFS-non-wafs in the WAAS Central Manager and on the WAE device, instead of being changed to the new name, NFS. This has no effect on NFS traffic acceleration, which continues to operate as configured.
- If you are upgrading from version 4.0.x to version 4.1.1, the way a wildcard mask is interpreted has changed. Wildcard masks can be specified for a traffic classifier match condition or an ACL rule. In version 4.0.x, a wildcard mask of 255.255.255.255 would (incorrectly) match no IP addresses, but in version 4.1.1, this wildcard mask matches any IP address, as expected.

Ensuring a Successful RAID Pair Rebuild

RAID pairs will rebuild on the next reboot after you 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.



Caution

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.

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** command in EXEC mode. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process may 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 that could indicate a problem:

- The device is offline in the Central Manager GUI.
- CMS cannot 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,” or “ext3_readdir: bad entry in directory.”
- Other unusual behaviors occur that are related to disk operations or the inability to perform them.

If you encounter any of these symptoms, reboot the WAE device and wait until the RAID rebuild finishes normally.

Managing Passwords after an Upgrade

WAAS software version 4.1.1 includes a strong password feature for improved security. Versions of the WAAS software previous to 4.0.19 do not have a strong password capability.



Note

The following considerations apply to WAAS software version 4.1.1 with the strong password policy enabled. Strong passwords are disabled by default.

When you upgrade from version 4.0.17 or earlier to version 4.1.1, note the following password considerations:

- Existing passwords from the older version will continue to work in version 4.1.1.
- Existing passwords will expire after 90 days. Subsequent new passwords must conform to strong password requirements.
- Strong passwords must meet the following requirements:
 - The password must be at least 11 characters long.
 - The password can include both uppercase and lowercase letters (A–Z and a–z), numbers (0–9), and special characters including ~`!@#\$%^&*()_+=[\]{};:;</>.
 - The password cannot contain all the same characters (for example, 99999).
 - The password cannot contain consecutive characters (for example, 12345).
 - The password cannot be the same as the username.

Downgrading from Version 4.1.1 to a Previous Version

Note the following guidelines for downgrading:

- Downgrade is supported only to versions 4.0.19, 4.0.17, or 4.0.13.
- When downgrading WAAS devices, first downgrade application accelerator WAEs, then the standby WAAS Central Manager (if you have one), and lastly the primary WAAS Central Manager.
- If you enable features such as secure storage and strong passwords in version 4.1.1, you must disable them before you downgrade WAAS to a previous version that does not support them.
- Locked-out user accounts will be reset upon downgrade.

- All preposition directives configured in CIFS accelerator mode must be removed before downgrading to a version prior to 4.1.1. (In versions 4.1.1c and 4.1.1d, unassign CIFS devices from the preposition before downgrading to retain the preposition directives.) You also must configure legacy mode file services by enabling a core server and configuring a WAFS core cluster, enabling an edge server, and registering file servers with the Central Manager.
- All dynamic shares configured in CIFS accelerator mode must be switched to legacy mode before downgrading to a version prior to 4.1.1, if you want to keep the dynamic shares. To switch a dynamic share to legacy mode, follow these steps:
 1. Edit the dynamic share in the **Configure > File > Dynamic Shares** window and choose a file server in the drop-down list. (File servers must be previously registered in the **Configure > File > File Servers** window.)
 2. Click **Submit**.

To downgrade the WAAS Central Manager (not required for WAE devices) to version 4.0.19, 4.0.17, or 4.0.13, follow these steps:

-
- Step 1** (Optional) Disable secure storage mode if it is enabled by using the **cms secure-store clear** global configuration command. This step is needed only if you are downgrading to a version earlier than 4.0.19.
- ```
(config)# cms secure-store clear
```
- Step 2** Disable the management service by using the **no cms enable** global configuration command.
- ```
(config)# no cms enable
```
- Step 3** From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command. Move the backup file to a separate device.
- ```
CentralManager# cms database backup
```
- Step 4** (Optional) If you are downgrading from a fresh install of version 4.1.1 (from the factory or from an installation performed with the WAAS recovery CD), back up the downgrade scripts to an FTP server as follows:
- a. Enable FTP on the WAAS Central Manager by using the **inetd enable ftp** global configuration command.
  - b. Copy each downgrade script to the FTP server by using the **copy disk** EXEC command as follows:
 

```
CentralManager# copy disk ftp ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_19
downgrade/WAAS_Downgrade4_1_1_to_4_0_19
CentralManager# copy disk ftp ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_17
downgrade/WAAS_Downgrade4_1_1_to_4_0_17
CentralManager# copy disk ftp ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_13
downgrade/WAAS_Downgrade4_1_1_to_4_0_13
```
- Step 5** Install the downgrade WAAS software image by using the **copy ftp install** EXEC command.
- Step 6** Reload the device.
- The database needs to be downgraded before the Central Manager can use it and the CMS process can start. To optionally verify this status, use the **show cms info** EXEC command. It should respond with a message saying that a database downgrade is required.
- Step 7** (Optional) If you performed Step 4, then restore the downgrade script files from the FTP server where you backed them up to the /downgrade directory on the WAAS Central Manager by using the **copy ftp** EXEC command as follows:
- ```
CentralManager# copy ftp disk ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_19
downgrade/WAAS_Downgrade4_1_1_to_4_0_19
```

```
CentralManager# copy ftp disk ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_17
downgrade/WAAS_Downgrade4_1_1_to_4_0_17
CentralManager# copy ftp disk ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_13
downgrade/WAAS_Downgrade4_1_1_to_4_0_13
```

Step 8 Downgrade the database by using the appropriate **cms database downgrade script EXEC** command.

```
CentralManager# cms database downgrade script downgrade/WAAS_Downgrade4_1_1_to_4_0_19
```

There are separate scripts depending on what version you are downgrading to:

- WAAS_Downgrade4_1_1_to_4_0_13
- WAAS_Downgrade4_1_1_to_4_0_17
- WAAS_Downgrade4_1_1_to_4_0_19

Step 9 Enable the CMS service by using the **cms enable** global configuration command.

```
config
(config)# cms enable
```

Downgrading the database may trigger full updates for registered devices. In the Central Manager GUI, ensure that all previously operational devices come online.

Cisco WAE and WAVE Appliance Boot Process

To monitor the boot process on Cisco WAE and WAVE appliances, connect to the serial console port on the appliance as directed in the *Hardware Installation Guide*.

Cisco WAE and WAVE appliances have video connectors that should not be used in normal operation. The video output is for troubleshooting purposes only during BIOS boot and stops displaying output as soon as the serial port becomes active.

Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade

Under rare circumstances, the RAID controller firmware used in the WAE-674, WAE-7341, and WAE-7371 appliances can cause the disk storage subsystem to go offline and the affected devices to stop optimizing connections. The symptoms are as follows:

- Syslog output contains several instances of the following message:
“WAAS-SYS-3-900000: sd 0:0:0:0: rejecting I/O to offline device.”
- A sysreport and running-config cannot be generated and copied to /local/local1.

Both of the above symptoms are an indication of the file system becoming read-only during traffic flow.

- An increasing number of pending connections appear in the output of the **show statistics tfo** command, indicating that new connections cannot be optimized. You can use this command to proactively check the functionality of the system.

The solution is to upgrade to the 5.2-0 (15427) RAID Controller Firmware, which can be found on cisco.com at the [Cisco Wide Area Application Engine \(WAE\) Utilities Software Downloads \(registered customers only\)](#) page. The firmware binary image is named L4_15427_FIRMWARE.bin.

Instructions on how to apply the firmware update are posted on cisco.com together with the firmware and are named L4_15427_FIRMWARE.pdf.

Operating Considerations

This section includes operating considerations that apply to software versions 4.1.1, 4.1.1a, 4.1.1b, 4.1.1c, and 4.1.1d:

- [Interoperability](#)
- [Device Group Default Settings](#)
- [Using Autoregistration with Port-Channel Interfaces](#)
- [WAFS Support of FAT32 File Servers](#)
- [Virtual Blade NIC Emulation](#)
- [Setting the Primary Interface When Using CIFS Accelerator](#)

Interoperability

This section discusses operating considerations when operating a WAAS network that mixes version 4.1.1 or higher devices with devices running earlier software versions.

- WAAS versions 4.1.1 and higher do not support running in a mixed version WAAS network where any WAAS device is running a software version lower than 4.0.13. If you have any WAAS devices running version 4.0.11 or earlier, you must first upgrade them to version 4.0.13 (or a later 4.0.x version), before you install version 4.1.1. You should first upgrade any WAEs to version 4.0.13 (or a later 4.0.x version) and then upgrade any WAAS Central Managers to version 4.0.13 (or a later 4.0.x version).
- In a mixed version WAAS network with version 4.1.1 or higher, the WAAS Central Manager must be running the highest version of the WAAS software.
- When a WAAS Central Manager is upgraded to version 4.1.1 or higher from 4.0.19, and the WAAS network contains a WAE that is running version 4.0.19 with the strong password policy is enabled, and when a WAE full database update is triggered on the WAE, user accounts may erroneously be shown in the Failed Creation on Devices list in the Central Manager Account Management window. Such accounts are not actually failed, and users can still log into these accounts. Ignore the failed status.
- When a WAAS Central Manager is upgraded to version 4.1.1 or higher and it is managing a 4.0.x device with legacy mode WAFS enabled that is not upgraded, the device may appear to have both legacy mode WAFS and the transparent CIFS accelerator enabled, because the Central Manager enables it by default. Disable the transparent CIFS accelerator if you want to continue to use legacy mode for WAFS.
- In a mixed version WAAS network, if your Central Manager is running WAAS versions 4.1.1c and 4.1.1d and your WAE devices are running version 4.1.1, 4.1.1a, or 4.1.1b, the sitemap does not work for preposition and dynamic shares directives in CIFS legacy mode. To avoid this issue, upgrade the WAE devices to 4.1.1c or 4.1.1d.

Device Group Default Settings

When you create a new device group in WAAS version 4.1.1 or higher, the **Configure > Acceleration > DSCP Marking** page is automatically configured for the group, with the default DSCP marking value of copy.

Using Autoregistration with Port-Channel Interfaces

Do not enable the **auto-register** global configuration command when both interfaces are configured as port-channel interfaces.

WAFS Support of FAT32 File Servers

The WAFS feature does not support file servers that use the FAT32 file system. You can use the policy engine rules to exclude from CIFS optimization any file servers that use the FAT32 file system.

Virtual Blade NIC Emulation

When you configure the virtual blade network interface card emulation in WAAS version 4.1.1c or 4.1.1d, you can select **E1000** (an Intel E1000 NIC emulator) in addition to the **rtl8139** and **virtio** emulators.

Setting the Primary Interface When Using CIFS Accelerator

In WAAS software version 4.1.1c and 4.1.1d, you may receive an alarm when you start the CIFS accelerator if the WAE device primary interface is not configured, or if it is misconfigured. To avoid the alarm, or to reset an existing alarm, wait 5 minutes after configuring the WAE primary interface to allow the configuration change to propagate through the system before enabling the CIFS accelerator. If you attempt to start the CIFS accelerator while it is already running, the CIFS accelerator will automatically restart.

Software Version 4.1.1d Resolved and Open Caveats

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.1.1d:

- [Software Version 4.1.1d Resolved Caveats, page 11](#)
- [Software Version 4.1.1d Open Caveats, page 11](#)

It is recommended that you upgrade to 4.1.1d only if you are currently using 4.1.1a/b/c and are affected by a caveat that has been resolved in 4.1.1d.

Software Version 4.1.1d Resolved Caveats

The following caveats were resolved in software version 4.1.1d:

- **CSCsu98623**—Under rare conditions, when a client accesses certain file types, like MS Access, optimization by the CIFS application accelerator may result in increased CPU or memory utilization. The client may experience degraded response or communication failure.
- **CSCsv01873**—Outlook clients may observe slow access or errors while accessing .pst files stored on a remote share.
- **CSCsv21165**—When a WAE establishes communication with a new peer WAE for the first time, one of the client connections may continue to persist on the WAE even after the client has closed the connection. This happens under very rare conditions.
- **CSCsv42901**—Database synchronization between a Primary Central Manager and a Standby Central Manager can result in the Primary Central Manager becoming unresponsive. This may happen if the Primary Central Manager is managing more than 50 WAEs, has more than 3 months of statistics data, and the Standby Central Manager (following a reload) requests a full database update. This does not happen if Primary and Standby Central Managers are already in sync and there is no Standby reload. This has no impact on traffic acceleration by WAEs and does not impact user experience.
- **CSCsv69306**—Under certain conditions, HTTP clients whose connections are being optimized by HTTP accelerator can experience slow response.
- **CSCsv77430**—On rare occasions, MAPI clients such as Microsoft Outlook need to retry connections that are being optimized by the MAPI application accelerator.
- **CSCsw28181**—Under heavy load conditions, a CIFS application accelerator restart alarm is seen on the WAE.
- **CSCsw66121**—When WAAS optimizes Quickbook traffic using the CIFS application accelerator, the user may not see the Quickbook login prompt.
- **CSCsw82410**—Connections optimized by the CIFS application accelerator, when closed abruptly by the clients, may generate excessive log messages.
- **CSCsw82908**—Certain TCP clients that advertise a zero receive window size may experience communication errors.
- **CSCsx15003**—Under stress conditions, a CIFS application accelerator restart alarm is seen. Clients may observe slow response during this period.
- **CSCsx34812**—Under rare conditions, CIFS application accelerator Keep Alive failure alarms are seen. Clients may observe slow response during this period.
- **CSCsx50930**—Under rare conditions, a WAE initiated internal connection can impact the optimization of a client-to-server user connection. Clients may experience slow response or communication failure.
- **CSCsx73347**—Under rare conditions, CIFS application accelerator Keep Alive failure alarms are seen. Clients may observe slow response during this period.

Software Version 4.1.1d Open Caveats

The open caveats for software version 4.1.1d are the same as those for software version 4.1.1c, with the exception of CSCsu98623 and CSCsv01873, which are resolved for 4.1.1d. For details, see the [“Software Version 4.1.1c Open Caveats” section on page 14](#).

Software Version 4.1.1c Resolved Caveats, Open Caveats, and Command Changes

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.1.1c:

- [Software Version 4.1.1c Resolved Caveats, page 12](#)
- [Software Version 4.1.1c Open Caveats, page 14](#)
- [Software Version 4.1.1c Command Changes, page 15](#)

Software Version 4.1.1c Resolved Caveats

The following caveats were resolved in software version 4.1.1c:

- **CSCso90969**—When AAA accounting is enabled for TACACS, disk encryption cannot be enabled on a WAAS device.
- **CSCsq99215**—The Admin user login times out when the Kerberos LDAP fails to register the WAE device to the Windows Active Directory.
- **CSCsr21342**—In rare circumstances, the WAAS Central Manager or a WAE device displays an alarm that a parser_server core file has been generated.
- **CSCsr89299**—A routing loop might occur between the WAE device and the router when the egress method is set to negotiated return. In this situation TCP RST packets are looped between the WAE device and the router.
- **CSCsr96298**—When one or more virtual blades are running on a WAE device and the kernel debugger (KDB) is enabled, the KDB commands kdump and reboot do not operate.
- **CSCsu07763**—When a WAE device is configured with IP on the inline interface, the route entry for the default gateway may be lost.
- **CSCsu07891**—The monthly weekdays pattern for the preposition schedule does not work. For example, preposition should run on the third Thursday of every month.
- **CSCsu23043**—The device GUI does not show CIFS accelerator mode even though the device is in CIFS accelerator mode. This situation occurs when switching the device from legacy to CIFS accelerator mode using the CLI.
- **CSCsu24201**—When you unassign a device or device group from a preposition in CIFS accelerator mode, the unassigned devices reappear as assigned after a few minutes (5 minutes by default). This situation occurs when you are modifying an existing CIFS accelerator mode preposition directive in the Central Manager GUI.
- **CSCsu25035**—When the secure store is initialized and open on a Central Manager or Core WAE device, the sitemap does not work for preposition and dynamic shares directives. This situation occurs when the preposition and dynamic shares are defined from the Central Manager in CIFS legacy mode.
- **CSCsu38832**—When an IP address is configured on the inline group, and the default gateway is removed, the inline port flaps (repeatedly switches between the shut and noshut states).
- **CSCsu40632**—When you try to distribute print drivers from the Central Manager, the download of the print driver files fails.
- **CSCsu45339**—When WAAS attempts to optimize MAPI traffic, the MAPI application accelerator generates core files. This situation occurs when the MAPI traffic is RPC Type 9 data.

- **CSCsu49878**—On the Central Manager GUI, HTTP statistics are displayed as very large values in milliseconds (ms).
- **CSCsu53046**—A WAAS print service printer is stopped/paused, and must be restarted from the WAAS Print Services Administration GUI. This situation can occur when one of the following happens:
 - The WAAS printer is configured using an lpd URI, and the printer is in an error condition for more than 5 minutes while a print job is “processing” in the WAAS printer queue.
 - The WAAS printer is configured using a socket URI, and communication to the printer is disrupted while a job is being spooled from the WAE device to the network attached printer.
- **CSCsu55188**—When you retrieve voice messages over your WAAS network, the CIFS application accelerator stops operating. This situation occurs when the log level is set to debug/detail and a connection is established.
- **CSCsu61597**—When WCCP is enabled on a WAAS core farm and one WAE device has WCCP disabled, the client is unable to connect to the WAE device for print services.
- **CSCsu62182**—When you attempt to restore a WAE devices configuration from a backup using the WAAS GUI, the configuration is not restored.
- **CSCsu66717**—When you view Generic AO statistics using the **show statistics accelerators EXEC** command, a huge value is displayed for active connections value.
- **CSCsu67322**—When operating with IP traffic on the inline interface port for many hours, the WAE-674 enters kernel debug mode.
- **CSCsu67330**—When you reload a WAE device that has one or more virtual blades running, the virtual blade configuration is changed. This situation occurs if you do not stop the virtual blade before you reload the WAE device.
- **CSCsu68909**—On rare occasions, during initialization of the CIFS accelerator when WAFS is disabled, the CIFS accelerator might unexpectedly restart and create a core dump.
- **CSCsu69661**—When you create user names using the Central Manager GUI, WAAS does not allow you to use special characters including the dot, dash, underscore, or back slash (. - _ \).
- **CSCsu71939**—When you use the **show statistics cifs requests EXEC** CLI command in Legacy mode, the command does not work and an error message is returned.
- **CSCsu72185**—When the HTTP application accelerator is active and you attempt to transfer a file that is larger than 2 GB, the connection is reset and error messages are generated.
- **CSCsu74163**—When you schedule a preposition task to occur on a monthly weekday (for example, on the third Wednesday of every month), the task is removed from the WAE device and listed as “not scheduled”.
- **CSCsu78054**—The WAAS HTTP accelerator response times increase significantly on the WAE-574.
- **CSCsu81961**—When you schedule preposition tasks for monthly daily or monthly weekday and then click Refresh, you cannot log into the WAE device GUI.
- **CSCsu83521**—When you view the system traffic summary report, on some occasions WAAS may display double the actual amount of traffic for each WAE device.
- **CSCsu90033**—When the secure store feature is initialized and open on a WAE device, the site map does not work for preposition and dynamic share directives from the Central Manager. This situation occurs when CIFS Legacy mode is active.
- **CSCsu94360**—When WAAS is running, you receive an acastor_watchdog alarm every five minutes. This situation occurs when you have configured a custom time zone.

- **CSCsv01806**—When you switch from CIFS accelerator mode to Legacy mode, disk encryption is disabled. This situation occurs when prepositioning is active in CIFS accelerator mode.
- **CSCsv10158**—When there is no optimized traffic, there is a discrepancy between the statistics shown on the Central Manager GUI and the statistics included in the exported CSV data.
- **CSCsv20907**—When you downgrade from WAAS version 4.1.x to 4.0.x, on some occasions the WAE device may go offline.
- **CSCsv31679**—A major alarm is incorrectly triggered on Outlook client connections using encryption. There is no impact on the system.
- **CSCsv44349**—The WAAS MAPI accelerator local and remote response statistics are wrong after stress testing.
- **CSCsv46053**—When the WAE device is operating in certain conditions, no connection is established between the Outlook 2007 client and the Exchange 2000 server.
- **CSCsv48186**—When the MAPI accelerator is disabled, the monitoring chart displays invalid data.

Software Version 4.1.1c Open Caveats

The following open caveats apply to software version 4.1.1c:

- **CSCsr64136**—WAFS preposition and read-ahead statistics are not displayed properly on the Central Manager. The prepositioning and read-ahead data is counted as optimized traffic, and the compression is shown as zero. Workaround: None.
- **CSCsu90205**—When you configure a customized time zone for a WAE device, the CIFS application accelerator line graphs all display zero. Workaround: Configure a standard time zone on the WAE device.
- **CSCsu98623**—Under rare conditions, when a client accesses certain file types, like MS Access, optimization by the CIFS application accelerator may result in increased CPU or memory utilization. The client may experience degraded response or communication failure. Workaround: The issue may be fixed temporarily by disabling and then enabling CIFS A0. It does not require a device reboot. To fix the issue permanently, disable and then enable CIFS A0 and remove any values from the NoOplockAccessPatternsDatabase and NoOplockAccessPatternsLocks fields in Edge WAE Expert Mode > CifsAO > RxCIFS configuration.
- **CSCsu99458**—The CLI **show tech-support EXEC** command displays the incorrect status for the WAE device interfaces. The WAE interfaces are displayed as shutdown when they are running. Workaround: None.
- **CSCsv18782**—WCCP CLI commands fail to get applied. The CLI is unable to acquire a configuration lock for WCCP. This situation typically occurs when you issue a ctrl-C. Workaround: None.
- **CSCsv01873**—Outlook clients may observe slow access or errors while accessing .pst files stored on a remote share. Workaround: None.
- **CSCsv23957**—When operating the WAE device on the data center side, in extremely rare circumstances and under high stress, the CIFS application accelerator may stop operating and display an “OutOfMemory on Core” error message. Workaround: Restart the CIFS application accelerator if it does not restart automatically.
- **CSCsv24575**—When you run a certain type of preposition task on a WAE device, the status is displayed as zero bytes and “in progress”. This situation occurs on a WAE device running the CIFS application accelerator and Legacy mode not configured. Workaround: None.

- **CSCsv27907**—When you schedule a preposition task to occur, it does not execute. This situation occurs on a WAE device running the CIFS application accelerator and Legacy mode not configured. Workaround: None.
- **CSCsv33344**—Clients from unoptimized sites are randomly unable to connect to servers. This situation occurs with multiple WCCP routers and WAEs in a farm. The WCCP flow tables are mismatched for WCCP service 61 & 62. Workaround: Reconfigure the WCCP farm by removing and re-adding the affected WAE from the farm to rectify the WCCP flow tables.
- **CSCsv40008**—Under heavy traffic conditions, kernel debug messages may appear on the console. There is no impact on performance. Workaround: Reduce the logging console priority from debug to warning or less.
- **CSCsv50453**—CIFS auto-discovery cannot perform a direct latency check. This situation occurs when the WAE device is low on virtual memory. Workaround: Use GUI expert mode or the CLI expert command to set the CifsAutoDiscovery EnableDirectLatencyCheck attribute to “false”.
- **CSCsv51243**—A NullPointerException is displayed on the Scheduled Reports table and the scheduled report may fail. This situation can occur when you delete a scheduled report. Workaround: Schedule the report on the Manage Reports page, but do not delete it until after the scheduled report has been run.
- **CSCsv54772**—After an upgrade to WAAS version 4.1.1, the WAE device appears to lose policy mappings and is no longer receiving policies from a device group. This situation occurs when policies were created under WAAS version 4.0.x that were configured with the Action “Passthrough” and an Accelerate configured to something other than “Do Not Set”. Workaround: Use the Central Manager GUI to edit the policies that have Action “Passthrough” so that they have Accelerate configured for “Do Not Set”.
- **CSCsv55714**—When you restart the CIFS accelerator, under extreme conditions a Java core file is generated and an alarm is displayed. Workaround: None; the CIFS accelerator restarts automatically.

The additional open caveats for software version 4.1.1c are the same as those for software version 4.1.1, with the exception of CSCsu07891, CSCsu23043, CSCsu24201, and CSCsu25035, which are resolved for 4.1.1c. For details, see the [“Software Version 4.1.1 Open Caveats” section on page 19](#).

Software Version 4.1.1c Command Changes

This section lists the modified CLI commands in WAAS software version 4.1.1c.

[Table 1](#) lists existing commands that have been modified in WAAS software version 4.1.1c.

Table 1 *CLI Commands Modified in Version 4.1.1c*

Mode	Command and Syntax
EXEC	<p>show stats auto-discovery</p> <p>A new field has been added to the output of this command: “Packets dropped state already exists” displays the number of packets dropped because state was already detected.</p>
	<p>show wccp gre</p> <p>A new field has been added to the output of this command: “Spoofed packets dropped” displays the number of packets that were dropped because there was no socket on which to receive the packet. This typically happens on reception of packets for an optimized connection after it has been terminated by the client/server with a reset.</p>
Preposition configuration ¹	<p>schedule monthly { week-day dayname daynumber time time { day day [day]... } } time time }</p> <p>The variable <i>weeknumber</i> is replaced by <i>daynumber</i>. This variable selects the occurrence during the month of the specified week-day, for example first, second, and so on.</p> <p>The following example schedules a preposition task to start on the second Monday of every month at 9:00 AM:</p> <pre>(config-preposition)# schedule monthly week-day monday 2 time 09:00</pre>

1. Preposition configuration commands are used to create and modify preposition directives that are used with the transparent CIFS accelerator.

Software Version 4.1.1b Resolved and Open Caveats

The following sections contain the open and resolved caveats in software version 4.1.1b:

- [Software Version 4.1.1b Resolved Caveats, page 16](#)
- [Software Version 4.1.1b Open Caveats, page 17](#)

Software Version 4.1.1b Resolved Caveats

The following caveats were resolved in software version 4.1.1b:

- **CSCsu53188**—This corner case is seen on a data center WAE. The HTTP application accelerator generates a core file while parsing a server response. This situation resets existing connections at the TCP level and triggers a core dump alarm. Most web-based applications are designed to recover from a TCP reset without any impact on application availability. However, affected connections may appear slow to the end-user under such conditions. The HTTP application accelerator restarts automatically to accelerate new connections.
- **CSCsu64601**—In the Central Manager GUI, the system message ArrayOutOfBounds Exception is displayed on the acceleration reports page for all application accelerators. This exception does not affect reports on bandwidth optimization and comparing original/optimized bytes data, based on layer 4 optimization. This situation may occur when more than 10 WAE devices are registered with the Central Manager.
- **CSCsu65835**—The port mapper (port 135) freezes when non-port mapper traffic is connected to the port and the EPM application accelerator is enabled. EPM server port 135 is used by certain applications to exchange dynamically generated end-ports for data transfer. Non-EPM-service traffic for server port 135 can be affected, which leads to application unavailability. Not all

applications that use non-EPM service on port 135 are affected. Most typical enterprise applications such as the Outlook client and Exchange server (e-mail) that use the EPM service are not affected. However, other applications such as Mobile-server retrieving voicemail from the Exchange server, can be affected by this caveat.

- **CSCsu71120**—When many pass-through connections are established and closed and new connections are opened at regular intervals, the Central Manager reports traffic data incorrectly. The original/optimized/pass-through traffic values are reported in the Central Manager as huge numbers, even though there is little traffic flowing across the network.
- **CSCsu82757**—When you upgrade a WAE-512 from WAAS release 4.0.13 or later to WAAS release 4.1.1 or 4.1.1a, the upgrade fails and the device does not boot. This rare situation occurs on certain WAE devices that are equipped with a specific version of compact flash. This caveat may potentially affect a small number of WAE-612 and WAE-7326 units but has not been observed yet.

Software Version 4.1.1b Open Caveats

The open caveats for software version 4.1.1b are the same as those for software version 4.1.1. For details, see the [“Software Version 4.1.1 Open Caveats” section on page 19](#).

Software Version 4.1.1a Resolved and Open Caveats

The following sections contain the resolved and open caveats in software version 4.1.1a:

- [Software Version 4.1.1a Resolved Caveats, page 17](#)
- [Software Version 4.1.1a Open Caveats, page 17](#)

Software Version 4.1.1a Resolved Caveats

The following caveats were resolved in software version 4.1.1a:

- **CSCsu12325**—Service `cms_cdm` is unable to start on the Central Manager after upgrading to WAAS 4.1.1. This situation occurred on a Central Manager running a WAAS version below 4.0.13 that is upgraded to a version between 4.0.13 and 4.0.19, and then subsequently upgraded to WAAS 4.1.1.
- **CSCsu29527**—Device dropped to `kdb`. Seen under certain conditions when connection reuse is in effect with the HTTP accelerator.
- **CSCsu45339**—Core files generated when certain mobile and voice communication servers interact with an Exchange server. Typical Outlook client-Exchange server interactions are not affected.

Software Version 4.1.1a Open Caveats

The open caveats for software version 4.1.1a are the same as those for software version 4.1.1. For details, see the [“Software Version 4.1.1 Open Caveats” section on page 19](#).

Software Version 4.1.1 Resolved Caveats, Open Caveats, and Command Changes

The following sections contain the resolved caveats, open caveats, and command changes in software version 4.1.1:

- [Software Version 4.1.1 Resolved Caveats, page 18](#)
- [Software Version 4.1.1 Open Caveats, page 19](#)
- [Software Version 4.1.1 Command Changes, page 23](#)

Software Version 4.1.1 Resolved Caveats

The following caveats were resolved in software version 4.1.1:

- **CSCsi66278**—When you access a fileshare on the DFS root of a NetApp filer, you see the following error message: `NT_STATUS_NO_SUCH_FILE`.
- **CSCsk36732**—The log message “RE Cache error: sub hash table is full” appears in the syslog and CPU spikes also occur.
- **CSCso03782**—When ACLs are applied to the Gigabit Ethernet interface, they are also applied to the inline interfaces.
- **CSCso47539**—When you enter the **show alarms** CLI command, WAAS indicates that the node health manager was restarted and that the WAE should be restarted. However, there is no indication in the syslog that the node health manager was restarted. The following message is displayed:

```
NOTE: The Node Health Manager was restarted and Alarm information
      may be inconsistent; however all other Device functionality
      should be unaffected.
      This device should be reloaded at the earliest convenience.
```

- **CSCsq24325**—If you press Enter when prompted for the secure store password, a Java error message is displayed. This situation occurs either while a Central Manager with secure store enabled is booting, or when you open the secure store using the **cms secure-store open** CLI command.
- **CSCsq24705**—When a Central Manager with the secure store enabled is booting, if you enter an invalid pass-phrase twice and then the valid pass-phrase on the third time, the Central Manager displays the following message: “Attempt to enter pass-phrase failed, continue device boot without opening secure-store?(y/n):”
- **CSCsq33268**—When the secure store is open on a standby Central Manager and you attempt to execute the **cms secure-store open** CLI command, you are prompted to enter the secure store password even though the secure store is already open.
- **CSCsq43732**—The network analysis tool Tethereal stops functioning while attempting to capture a packet from the WAE device. This situation does not affect WAAS system operation.
- **CSCsq50614**—When the secure store is enabled and you use the **Change CMS Secure Store** function to generate a new encryption key for the WAE devices in a device group, the Force Device Group icon is displayed on the Central Manager GUI.
- **CSCsq87537**—When you manually shut down an inline interface, the “The interface InlinePort 1/1/wan is in bypass mode” alarm is displayed and cannot be disabled.

Software Version 4.1.1 Open Caveats

The following open caveats apply to software version 4.1.1:

- **CSCsl43335**—Vista client cannot upload print drivers. In legacy mode, native Vista printing does not work as expected. Workaround: Use an alternate WAAS printing solution, such as the Windows Print accelerator, when using Vista.
- **CSCsm34473**—After using the **debug authentication user** CLI command, the **undebbug authentication user** CLI command fails. Workaround: None.
- **CSCsq82978**—Policy configuration application failure messages and other error messages appear in the CMS logs. This situation occurs when you use the **policy-engine config restore predefined** CLI command to apply a policy configuration, and the Central Manager GUI also applies a configuration to WAE device at the same time. Workaround: Reapply the desired configuration from only one source (either the CLI or the Central Manager GUI).
- **CSCsr41091**—The pie-chart graph is not visible on screen after the Central Manager GUI dashboard is resized (minimized, maximized, or restored). Workaround: Save the chart settings on the report and then refresh the dashboard page.
- **CSCsr62574**—Unable to remove an interface port channel configuration using the **no int port channel 1** CLI command. Workaround: Deregister the WAE from the Central Manager before making any change to the primary interface, and then reregister the WAE.
- **CSCsr67792**—When a legacy mode preposition fails with errors, the number of copied files displayed in the Central Manager GUI is more than 0 but all the other counters show 0. Workaround: None.
- **CSCsr72573**—A WAE port channel cannot be reached from the LAN. This situation occurs after a shutdown of the physical interface followed by an unshutdown of the interface, when that physical interface is a member of the port channel. Workaround: Shut down the interface, remove it from the port channel using the **no channel-group 1** CLI command. Next, instead of doing a no shut command, add the interface back to the port channel using the **channel-group 1** CLI command.
- **CSCsr80504**—After you upgrade WAAS from software version 4.0.19 to 4.1.1 using a rolling upgrade procedure, the TCP page goes into override mode when you configure the Device Group TCP parameters. Workaround: Force the Device Group settings again on the devices. The Device Group does not go back into override mode.
- **CSCsr83205**—Unable to change network interface settings from Gig 2/0 to 1/0 on an NME-502 WAE using the Central Manager Network Interfaces settings page. Workaround: Use the CLI to change the primary interface from Gig 2/0 to 1/0.
- **CSCsr85123**—When load-balance is set to “dst-ip—” the second link is not shown for “sh cdp nei” at the WAE. Workaround: None.
- **CSCsr86100**—When a standby group is assigned as the primary interface, the CMS is unable to start after a reload. Workaround: Do not use a standby group as the primary interface. Or, restart CMS services on the affected device after reload.
- **CSCsr86658**—The hostname of the Central Manager cannot be changed through the Activation Page. Workaround: Use the CLI to change the hostname. However, the change is not reflected in the Central Manager GUI until you reload the Central Manager.
- **CSCsr88853**—A WAE device with a primary interface set to a dummy IP address can be registered to the Central Manager. Workaround: Configure a valid IP address for the primary interface on the WAE device before registering it to the Central Manager.
- **CSCsr90637**—The port channel link G2/0 is under utilized (not load balanced) when load balancing is configured with the dst-ip option. Workaround: Use load balancing with round robin.

- **CSCsr91207**—When changing a WAE to a different device group on the Assign Device Group page, the policy definitions page shows the configuration from a previous device group. Workaround: Refresh the policy definitions page to see the applicable configurations.
- **CSCsr93154**—When the primary interface of a WAE is changed after registering it to the Central Manager, a full database update occurs for every polling period (default period is 300 seconds). Workaround: Deregister and the reregister the WAE to the Central Manager.
- **CSCsr93241**—Under certain error conditions, HTTP accelerator is disabled after every datafeed poll (default period is 300 seconds), even if the HTTP accelerator is configured as enabled. Workaround: Deregister the WAE and reregister it to the Central Manager.
- **CSCsr93523**—When the primary Central Manager fails and the standby Central Manager comes online, if secure store operations are performed on the Central Manager the following situations may occur:
 - The connected WAE devices go offline.
 - The Force Device Group icon is displayed on the device Group pages.
 - If the Force Device Group icon is clicked on the Disk Encryption page in the GUI, the encryption key is changed for the WAEs even though disk encryption was already enabled.

Workaround: If secure store operations are not required, you can continue to use the system normally. The following workarounds are necessary only if secure store operations on the WAEs are required:

- Set the primary Central Manager role back to the original Central Manager as before the failover. Wait for one data feed poll cycle (default cycle is 300 seconds) for the WAEs to come back online.
 - Reconfigure the IP address of the current Central Manager primary interface to the match the IP address of the primary interface of the original primary Central Manager before the failover. Wait for one data feed poll cycle for the WAEs to come back online.
 - Reconfigure the Central Manager IP address on the WAEs to point to the current Central Manager IP address. Restart the CMS process on the WAEs. Wait for one data feed poll cycle for the WAEs to come back online.
- **CSCsr95716**—Scheduled reports PDF attachments data is not readable on the x-axis for the last-day time frame. Workaround: View the scheduled report page on Central Manager instead of the PDF attachment.
 - **CSCsr99662**—A Monitoring API query for retrieveDataReadStats in a Device Group context returns incorrect values for the MIN and MAX attributes. Workaround: Call retrieveDataReadStats for each WAE in the device group and derive the value for the MIN and MAX attributes for the Device Group by observing the values returned for each WAE.
 - **CSCsu01688**—Unable to ping the default gateway with a port channel and a virtual blade configured. Workaround: None.
 - **CSCsu02423**—The accumulated read ahead data Size statistics in the MAPI accelerator always displays 0 even though read ahead is working. Workaround: None.
 - **CSCsu04237**—After you open secure store from the Device Group window, the Force Device Group icon is displayed on the Device Group secure store page. Workaround: Ignore the Force Device Group icon. This condition does not affect use of the secure store functionality. All further secure store operations will be completed.
 - **CSCsu07775**—In the Central Manager GUI, the Monitoring API for Native TFO does not work at the Device Group level. The “retrieveTrafficStats” and “retrieveAppTrafficStats” APIs retrieve statistics for only one device and do not return the consolidated statistics for all the devices assigned

to the Device Group. Workaround: Invoke the API at the Device level for each WAE in the Device Group and derived the statistics for the Device Group by summing up individual attributes of each WAE.

- **CSCsu07891**—The monthly weekdays pattern for the preposition schedule for does not work. For example, preposition should run on the third Thursday of every month. Workaround: Use the closest configuration you can. For example, use the Weekly pattern set to run every Thursday, or the Monthly Date pattern set to run on the third of every month.
- **CSCsu07976**—The Monitoring API NFSretrieveResponseStats do not work at the Device Group level. Workaround: Retrieve the statistics at the Device level for each WAE in the Device Group and derive the Device Group WAE statistics manually.
- **CSCsu08094**—After downgrading from WAAS software version 4.1.1 to version 4.0.19, most of the Device Group pages have the Force Device Group icon. Workaround: Click the Force Group Setting icon from the Device Group home page.
- **CSCsu09508**—The Central Manager does not show the correct data on the unaccelerated Video weekly chart. Workaround: Wait for a minimum of three days for the weekly/monthly chart and three hours for a daily chart to get plotted.
- **CSCsu09750**—The Monitoring API “retrieveAppTrafficStats” fails to retrieve the application name when “All traffic” and “other traffic” are used. The other statistics retrieved by the API are correct and match with the CSV file. Workaround: Replace the application name for the retrieved statistics structure with the application name specified as input parameter to the API query.
- **CSCsu10451**—After upgrading a Central Manager alone to WAAS version 4.1.1, the following alarm is displayed on a version 4.0.x WAE-NME Edge device: “Roles changed on the device. Reload the device.” Workaround: You can either ignore the alarm or reload the device to get rid of the alarm.
- **CSCsu12199**—After downgrading, the primary interface configuration is removed and the WAE device shows an offline state in the Central Manager GUI. This situation occurs when the Inline Group interface is configured as the primary interface. Workaround: Use the CLI to set the primary-interface Inline Group slot number and group number to the previous primary interface settings.
- **CSCsu12216**—Disk encryption is re-initialized and the WAE device content cache is cleared after a reboot. This situation occurs when you enable disk encryption on a WAE using the CLI, and the device reboots before the change is detected by the Central Manager. Workaround: Enable disk encryption only from the Central Manager GUI. If you do enable disk encryption using the WAE CLI, wait for a complete data feed polling cycle (default period is 300 seconds) to occur before reloading the device.
- **CSCsu12325**—Service cms_cdm is unable to start on the Central Manager after upgrading to WAAS 4.1.1. This situation occurred on a Central Manager running a WAAS version below 4.0.13 that is upgraded to a version between 4.0.13 and 4.0.19, and then subsequently upgraded to WAAS 4.1.1. Workaround: If this has already occurred, contact Cisco TAC for a script to restore the Central Manager services. To prevent this situation, follow these steps before upgrading:
 - a. Create a Central Manager database backup before upgrading to version 4.1.1 by using the **cms database backup EXEC** command. This command creates a backup file in /local1/.
 - b. Upgrade the Central Manager to version 4.1.1 and reload the Central Manager.
 - c. If this issue is observed after reload, execute the following command:
cms database restore backup-file
 where *backup-file* is the one created in step a.
- **CSCsu12410**—Schedule Report changes made using the Edit button do not occur. This situation occurs when you try to apply the changes to a canned report. Workaround: Create a new report from the Manage Reports page. Select the charts to add, change the settings as required, and schedule it.

- **CSCsu18411**—The disk serial number for a WAE-674, WAE-7341, or WAE-7371 is not displayed when executing the **sh disk details** CLI command. Workaround: None.
- **CSCsu18439**—CIFS connectivity is lost after downgrading from WAAS version 4.1.1 to version 4.0.13. This situation occurs if there are prepositions in CIFS accelerator mode that were assigned to the downgraded devices before the downgrade. Workaround: Remove the prepositions before the downgrade.
- **CSCsu21596**—CIFS accelerator configuration changes are not shown properly on the device GUI. This situation occurs when the WAE device has Edge services enabled and, after it is assigned to a device group that has the CIFS accelerator enabled, the device group settings are forced to the device. The WAE device switches to CIFS accelerator, but the device GUI does not reflect the change. Workaround: Disable Edge services on the WAE device before forcing the device group settings with CIFS accelerator mode configured to the device.
- **CSCsu23043**—The device GUI does not show CIFS accelerator mode even though the device is in CIFS accelerator mode. This situation occurs when switching the device from legacy to CIFS accelerator mode using the CLI. Workaround: Switch the device from legacy mode to CIFS accelerator mode from the Central Manager GUI.
- **CSCsu24201**—When you unassign a device or device group from a preposition in CIFS accelerator mode, the unassigned devices reappear as assigned after a few minutes (5 minutes by default). This situation occurs when you are modifying an existing CIFS accelerator mode preposition directive in the Central Manager GUI. Workaround: Delete the preposition completely from the Central Manager, then recreate and assign the remaining devices.
- **CSCsu24488**—When a virtual blade is configured to use a Gigabit Ethernet interface, the interface cannot be unshut after it has been shut down. Workaround: Before unshutting an interface, remove the IP address from its configuration. Reassign the IP after you successfully bring up the interface.
- **CSCsu24579**—When you downgrade from WAAS software version 4.1.1 to 4.0.19, 4.0.17, or 4.0.13, the CMS database downgrade script is not available. This occurs when 4.1.1 was installed by any of the following methods:
 - On a fresh device, after restoring factory-defaults, or after deleting disk-partitions, or
 - Using a rescue CD

Workaround: Before installing WAAS software version 4.0.19, 4.0.17, or 4.0.13, back up the relevant downgrade script. Restore and use the script after the installation.

The following steps describe the script backup procedure (4.0.19 is used as an example below):

- a. Enable ftp on Central Manager using the **inetd enable ftp** CLI command.
- b. Copy downgrade script for 4.0.19.14 to an FTP server using the **copy disk ftp ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_19 downgrade/WAAS_Downgrade4_1_1_to_4_0_19** command.
- c. After installing 4.0.19, 4.0.17, or 4.0.13 reload the Central Manager.
- d. After the Central Manager is up, log in to the Central Manager and restore the backup downgrade script from step 2 using the **copy ftp disk ftp_server_ip remote_dir WAAS_Downgrade4_1_1_to_4_0_19 downgrade/WAAS_Downgrade4_1_1_to_4_0_19** command.
- e. Run the downgrade script using the **cms database downgrade script downgrade/WAAS_Downgrade4_1_1_to_4_0_19** command.
- f. Enter config mode and enable cms using the **cms enable** command.

- **CSCsu25035**—When the secure store is initialized and open on a Central Manager or Core WAE device, the sitemap does not work for preposition and dynamic shares directives. This situation occurs when the preposition and dynamic shares are defined from the Central Manager in CIFS legacy mode. Workaround: Do one of the following:
 - Clear the secure store feature on the Central Manager or Core device by using the **cms secure-store clear** CLI command. The site map will work.
 - Manually assign shares defined on the file server.

Software Version 4.1.1 Command Changes

This section lists the new, modified, and removed commands in WAAS software version 4.1.1.

[Table 2](#) lists the new commands and options that have been added in WAAS software version 4.1.1.

Table 2 CLI Commands Added in Version 4.1.1

Mode	Command and Syntax
EXEC	license add <i>license-name</i>
	show accelerator
	show directed-mode
	show kdump
	show license
	show statistics accelerator
	show statistics aoim
	show statistics application [<i>app_name</i> savings <i>app_name</i>]
	show statistics connection
	show statistics datamover
	show statistics directed-mode
	show statistics dre detail
	show statistics generic-gre
	show statistics tfo connection
	show statistics windows-print requests
	show tfo tcp
show virtual-blade [<i>virtual-blade-number</i>]	

Table 2 CLI Commands Added in Version 4.1.1 (continued)

Mode	Command and Syntax
Global configuration	accelerator cifs { [double-byte-unicode] enable dynamic-share <i>share</i> clear cache cache server-rename <i>oldname newname</i> exception { coredump debug no-coredump } }
	accelerator cifs preposition [remove] <i>directive_id</i>
	accelerator epm { enable exception { coredump debug no-coredump } }
	accelerator http { enable exception { coredump debug no-coredump } }
	accelerator mapi { enable read-opt write-opt exception { coredump debug no-coredump } }
	accelerator nfs { enable exception { coredump debug no-coredump } }
	accelerator video { enable unaccelerated-traffic type all action drop max-initial-setup-delay <i>seconds</i> windows-media { client idle-timeout <i>seconds</i> log-forwarding enable } exception { coredump debug no-coredump } }
	accelerator windows-print enable
	directed-mode enable [port <i>udp-port</i>]
	kernel kdump enable
	policy-engine application set-dscp <i>dscp-marking</i>
	tfo tcp adaptive-buffer-sizing { enable receive-buffer-max <i>size</i> send-buffer-max <i>size</i> }
	virtual-blade { <i>virtual-blade-number</i> enable }
	Preposition configuration ¹
dscp <i>value</i>	
duration <i>minutes</i>	
enable	
ignore-hidden-dir	
max-cache <i>percentage</i>	
max-file-size <i>size_in_kb</i>	
min-file-size <i>size_in_kb</i>	
name <i>name</i>	
pattern { equals starts-with ends-with contains } <i>text</i>	
recursive	
root <i>path</i>	
scan-type { full since last since <i>period units</i> }	
schedule { now daily <i>time</i> date <i>date time</i> weekly { <i>dayname</i> [<i>dayname</i>]... } time <i>time</i> monthly { week-day <i>dayname weeknumber</i> time <i>time</i> { day <i>day</i> [<i>day</i>]... } } time <i>time</i> }	
server <i>name</i>	

Table 2 CLI Commands Added in Version 4.1.1 (continued)

Mode	Command and Syntax
Virtual Blade Configuration ²	autostart
	boot { cd-image { cd-rom disk <i>location</i> } fd-image disk <i>location</i> from { cd-rom disk }}
	description <i>description-text</i>
	device { cpu { qemu64 qemu32 } nic { rt18139 E1000 virtio } disk { IDE virtio }}
	disk <i>space-allocation</i>
	interface <i>vb-interface</i> bridge { GigabitEthernet <i>port</i> PortChannel <i>channel</i> }
	memory <i>memory-allocation</i>

1. Preposition configuration commands are used to create and modify preposition directives that are used with the transparent CIFS accelerator.
2. Virtual blade configuration commands are used to configure virtual blades on platforms that support virtual blades.

Table 3 lists existing commands that have been modified in WAAS version 4.1.1.

Table 3 CLI Commands Modified in Version 4.1.1

Mode	Command and Syntax	Description
EXEC	clear	Added options for licenses, transaction logs, DRE cache, and statistics for accelerators, directed mode, generic GRE, and other items.
	cms deregister force	Forces the removal of the WAE node registration.
	copy cdrom wow-recovery <i>filename</i>	Copies Windows Server on WAAS installation image files from the CD/DVD drive to the staging area on the virtual blade.
	copy ftp wow-recovery { <i>hostname</i> <i>ip-address</i> } <i>dir filename</i>	Copies Windows Server on WAAS installation image files from an FTP server to the staging area on the virtual blade.
	copy tech-support ftp { <i>hostname</i> <i>ip-address</i> }	Copies configuration information to an FTP server.
	debug	Added options for accelerators, auto-discovery, directed mode, DRE nack, generic GRE, inline, statistics, transaction logs, and other items.
	reload [force in <i>m</i> cancel]	Includes option to reload in <i>m</i> minutes or cancel a scheduled reload.
	setup	Enhanced to support quicker setup with more automatic configuration.
	show cms secure-store	Displays the status of the CMS secure store.
	show statistics tfo connection	Displays aggregated TFO connection statistics.
	show transaction-logging	Supports both TFO flow and video accelerator transaction logging.
	transaction-log force { archive export } { flow accelerator video windows-media }	Supports both TFO flow and video accelerator transaction logging.
undebg	Added options for accelerators, auto-discovery, directed mode, DRE nack, generic GRE, inline, statistics, transaction logs, and other items.	

Table 3 *CLI Commands Modified in Version 4.1.1 (continued)*

Mode	Command and Syntax	Description
Global configuration	egress-method { ip-forwarding negotiated-return generic-gre } intercept-method wccp	Supports the generic GRE egress method.
	policy-engine application map adaptor EPM	Added application accelerator options and DSCP marking option.
	policy-engine application map adaptor WAFS transport	Added application accelerator options and DSCP marking option.
	policy-engine application map basic	Added application accelerator options and DSCP marking option.
	policy-engine application map other optimize DRE	Added DSCP marking option.
	policy-engine application map other optimize full	Added DSCP marking option.
	policy-engine application name	Added DSCP marking option.
	port-channel load-balance { dst-ip round-robin }	Removed dst-mac option.
	tcp	Removed memory-limit options.
	transaction-logs	Added video stream transaction logging option.

Table 4 lists commands that have been removed in WAAS version 4.1.1.

Table 4 *CLI Commands Removed in Version 4.1.1*

Mode	Command
EXEC	clear statistics dre connection
	clear statistics dre nack
	clear statistics tfo blacklist
	show key-manager
	show statistics dre connection
	show statistics key-manager
	show tfo bufpool
	show tfo connection
	show tfo status

Table 5 lists commands whose names have changed in WAAS version 4.1.1.

Table 5 *CLI Commands with Changed Names in Version 4.1.1*

Mode	Old Command Name	New Command Name
EXEC	clear statistics dre peer	clear statistics peer dre
	clear statistics tfo auto-discovery	clear statistics auto-discovery
	clear statistics tfo filtering	clear statistics filtering
	clear statistics tfo synq	clear statistics synq
	show statistics dre peer	show statistics peer dre
	show statistics dre config	show dre
	show statistics dre connection	show statistics connection optimized dre
	show statistics tfo pass-through	show statistics pass through
	show statistics tfo peer	show statistics peer
	show tfo accelerators	show accelerator <i>acceleratorName</i> detail
	show tfo auto-discovery	show statistics auto-discovery
	show tfo auto-discovery blacklist entries	show auto-discovery blacklist
	show tfo auto-discovery list	show auto-discovery list
	show tfo connection	show statistics connection optimized tfo
	show tfo connection summary	show statistics connection all
	show tfo egress-methods	show statistics connections egress-methods
	show tfo filtering	show statistics filtering
	show tfo filtering list	show filtering list
	show tfo synq	show statistics synq
show tfo synq list	show synq list	
Global configuration	tfo auto-discovery	auto-discovery

WAAS Documentation Set

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

- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *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 Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *Installing the Cisco WAE Inline Network Adapter*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.

