



Release Note for the Cisco WAAS Mobile, Release 3.5.4

March, 2012



Note

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

Contents

This release note applies to software version 3.5.4 for the Cisco Wide Area Application Services (WAAS) Mobile product.

This release note contains the following sections:

- [WAAS Mobile Product Overview](#)
- [Related Documents](#)
- [Upgrading From or Downgrading to a Previous Version](#)
- [New and Changed Features](#)
- [Operating Considerations](#)
- [Resolved Caveats in Software Version 3.5.4](#)
- [Open Caveats in Software Version 3.5.4](#)
- [Obtaining Documentation and Submitting a Service Request](#)



Americas Headquarters:

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

© 2012 Cisco Systems, Inc. All rights reserved.

WAAS Mobile Product Overview

Cisco Wide Area Application Services (WAAS) Mobile provides significant application acceleration and bandwidth savings to telecommuters, mobile users, and home-office users accessing corporate HTTP applications, e-mail, and file servers.

Cisco WAAS Mobile accelerates a range of applications including most web browsers, email clients, Windows Explorer for file shares, FTP clients, and thin clients like Citrix and Microsoft Remote Desktop Client (RDC). In addition, any generic application using TCP connections to content servers can be added through its process name. This list of accelerated applications is determined by comparing the name of the process running on the end user's machine to a pre-configured list of "Accelerated Processes." TCP connections associated with processes not in this list will be "bypassed."

Related Documents

In addition to this release note, the following documents are also available:

- *Cisco WAAS Mobile Administration Guide*—Everything needed to set up and administer WAAS Mobile Manager.
- *Cisco WAAS Mobile User Guide*—A user guide for the end user. This complements the on-line help system and provides a reference for offline study.

Upgrading From or Downgrading to a Previous Version

This section contains information on how to upgrade from and downgrade to previous software versions.

- [Upgrading from Version 3.5.0, 3.5.1, 3.5.2, or 3.5.3](#)
- [Upgrading from Version 3.4.x or Earlier Versions](#)
- [Upgrading From a Version Prior to 3.3.1342.4](#)
- [Downgrading to an Earlier Version of Software](#)

Upgrading from Version 3.5.0, 3.5.1, 3.5.2, or 3.5.3

Perform the following procedure if you are upgrading to version 3.5.4 from version 3.5.0, 3.5.1, or 3.5.2.

-
- | | |
|---------------|---|
| Step 1 | Prior to upgrading: <ul style="list-style-type: none">• Verify that Automatic Upgrades are enabled on the Configure > Clients > Software page of the Manager.• Backup the system configuration using the Manage > Backup and Restore page of the Manager. |
| Step 2 | Stop all servers. |
| Step 3 | Uninstall the previous version of WAAS Mobile server software and, during the uninstall process, select the option to retain all configuration information. |

Step 4 Uninstall PostgreSQL 9.0 and reboot when prompted.



Note The database will be reinstalled by Version 3.5.4.

Step 5 Delete the C:\postgresql directory.

Step 6 Install the new version of WAAS Mobile Manager on the server machine by double-clicking the ServerSetup.exe file and then rebooting if prompted.

Step 7 Import the database from the backup before starting the servers.

Step 8 Start all servers.

Step 9 Navigate to the **Configure > Apply Settings** page of the Manager and apply settings. The clients will now be automatically upgraded to version 3.5.4.

Upgrading from Version 3.4.x or Earlier Versions

Upgrading from a version earlier than 3.5.0 includes a major upgrade to the WAAS Mobile management infrastructure and introduces enhanced mechanisms and policies for managing clients and servers. As a result of these changes, it will be necessary to reconfigure the WAAS Mobile Manager after upgrading.

Step 1 Prior to upgrading:

- a. Record the current configuration settings.



Note All client and server configurations will be deleted during the upgrade process and will need to be re-entered after Release 3.5.4 is installed. Please be sure to record existing configuration information, including the names of all fielded client distribution profiles. Additionally, export the system configurations by navigating to the Server Configuration tab and selecting the **Import/Export** menu item, and then pressing the **Export** button. The configuration will be exported into an XML file that can be used as a reference if needed.

- b. If you are currently running the WAAS Mobile server on a 32-bit version of the Windows Server Operating System, consider upgrading the Windows Operating System to a 64-bit version for improved scalability and performance.
- c. If you are currently using the IP aliasing feature, perform the following steps before uninstalling 3.5.0:
 - Turn off IP Aliasing.
 - Reboot the server and confirm that no aliased IP addresses exist on the NIC card by typing **ipconfig /all** in the command line.
- d. Uninstall the previous version of WAAS Mobile server software and, during the uninstall process, select the option to remove all configuration information.

Step 2 Install the new version of WAAS Mobile Manager on the server machine by double-clicking the ServerSetup.exe file and then rebooting if prompted.

Step 3 Login to the WAAS Mobile Manager using the following default credentials:

- Username: admin

- Password: default

Step 4 Configure the Manager, Server(s) and Clients, following the guidance in Chapters 5, 6, and 7 of the *Cisco WAAS Mobile Administration Guide* and apply configurations when complete.



Note Recreate the client distributions using the same names that were previously used to ensure that when the WAAS Mobile servers are started, the client software and configurations will be automatically updated.



Note The system configuration that was exported from Release 3.4 cannot be automatically inputted. The configurations must be entered via the GUI.

Step 5 Verify that:

- a. If more than one server is deployed, all servers are managed centrally.
- b. All servers are assigned to a server profile, which defines the configuration policies for those servers
- c. All servers are assigned to a server farm, which associates them with the networks that they will accelerate and provisions load balancing and failover, when appropriate.
- d. All previously existing client distributions have been re-created. The quickest approach is to configure a single client distribution fully and then use the copy feature to generate the other distributions.
- e. All processes that were previously configured on the HTTP and HTTPS accelerated processes list have been configured.
- f. Delta cache size and location is correctly specified.

Step 6 From the **Manage > Servers** page of the WAAS Mobile Manager, verify that all servers are properly addressed and have licenses and then start the servers that are not running.

Step 7 When the server upgrade completes and the servers are restarted, the WAAS Mobile clients on the users' PCs will automatically download the new software and configurations and, at the conclusion of the client software upgrade, the users will be prompted to reboot. Acceleration will be disabled (indicated by the gray icon) until the reboot occurs; at that time, the client will reconnect and begin accelerating, and the icon will turn green.

Upgrading From a Version Prior to 3.3.1342.4

When upgrading from any version of WAAS Mobile prior to version 3.3.1342.4, you must completely uninstall both the client and the server software. See the *Cisco WAAS Mobile Administration Guide* for a detailed description of install and uninstall procedures.

Downgrading to an Earlier Version of Software

To downgrade from version 3.5.4 to an earlier version of 3.5.x software, perform the following steps on the server:

-
- | | |
|---------------|--|
| Step 1 | Before downgrading, on the Upgrades tab of the Configure > Clients > Software page, select Enable Automatic Downgrades . |
| Step 2 | Uninstall version 3.5.4 and then re-install version 3.5.x. |
| Step 3 | Restart the server. |
-

To downgrade to a version prior to 3.5.0, you must completely uninstall both the client software installation and the server installation. See the *Cisco WAAS Mobile Administration Guide* for a detailed description of install and uninstall procedures. After downgrading, configurations will need to be manually re-entered.

New and Changed Features

The Cisco WAAS Mobile Manager now supports the use of FIPS-compliant encryption algorithms on the underlying Windows Server platform for encryption, hashing, and signing.

Operating Considerations

Operating considerations include the following categories:

- [Installation Considerations](#)
- [Interoperability Considerations](#)
- [Acceleration Performance Considerations](#)
- [Management Considerations](#)

Installation Considerations

- Cisco WAAS Mobile Release 3.5.4 minimum hardware guidelines have been revised as follows:
 - Minimum RAM for a small deployment (approximately 100 users) should be at least 6 GB.
 - Windows Server 2008 R2 is recommended.
- ASP.Net must be pre-installed on the Windows Server 2008 R2 Operating System before WAAS Mobile may be installed.
- Cisco WAAS Mobile Manager should not be installed on a Windows Domain Controller.
- When running Cisco WAAS Mobile on a Virtual Machine, shut down the VM before updating its hardware configuration

Interoperability Considerations

- Cisco WAAS Mobile Manager requires that the inetpub directory be configured on the C: drive.
- When interoperating with the CheckPoint IPsec or Microsoft Intelligent Application Gateway (IAG) VPN clients, the network monitoring feature on the client should not be enabled. Note that this feature is disabled by default.
- The WAAS Mobile server may show higher memory utilization with software version 3.5 than in version 3.4. When starting, the WAAS Mobile server will allocate memory for its use based on the amount of RAM available and the amount of contiguous blocks of memory available. A relatively high memory allocation (roughly half the available memory or more) is seen regardless of the number of users for performance reasons. This necessitates a requirement that the WAAS Mobile server or VM be reserved solely for WAAS Mobile to avoid starving any other memory-heavy processes. Depending on the users' delta cache configuration, this may mean that not all the memory being allocated for use by WAAS Mobile is necessarily in active use at any given time. As the number of users increases on the server, more of the allocated memory will be in active use.

Acceleration Performance Considerations

- The Cisco WAAS Mobile client will not function if the user logs in using Microsoft Windows Guest accounts.
- Cisco WAAS Mobile will only accelerate the first user that logs into a computer. For example, if a user is logged-in locally, and another user logs into the same machine via remote terminal services, only the local user's sessions will be accelerated. Also, if Fast User Switching is used, only the sessions associated with the user that logged-in first will be accelerated.
- Transparent CIFS SMB does not support the persistent sessions feature. Connections opened via transparent CIFS SMB will not be maintained when a short network outage occurs.
- To enable protocol optimization of Outlook 2003 and 2007, change the protocol optimization type from Generic Acceleration to Normal Acceleration. Note that when using Outlook 2007 with Exchange 2007, the Meeting Room Request and Resource Availability features are not supported. Also, note that protocol optimization of Outlook 2010 is not supported.
- The WAAS Mobile client should be enabled and running before initiating SMB sessions between Windows 7 and Vista clients and Windows Server 2008 or 2008 R2 file shares in order to achieve optimum acceleration of this traffic.
- In some cases, CIFS SMB traffic between PCs running Windows 7 or Vista PCs and file servers running Windows Server 2008 or 2008 R2 may not receive protocol optimization. Workaround: Configure these PCs for SMB 1.0 compatibility mode by setting the following registry key:
`HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters Smb2 (DWORD) = 0.`
- When optimizing the CIFS protocol when SMB signing is required, users may be prompted to enter credentials the first time they access the file share after WAAS Mobile has been installed or upgraded.

Management Considerations

- The WAAS Mobile Manager statistics for client sessions may not match client-side statistics, as the WAAS Mobile Manager is updated less frequently than the WAAS Mobile client.

- WAAS Mobile Manager may incorrectly report a failure to start when, in fact, WAAS Mobile did start. When this occurs, the Windows Service Control Manager displays a message that states “At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details.” When the Event Viewer's system log is viewed, it will indicate the following error message “The WAAS Mobile Manager service hung on starting.” These messages should be ignored.
- Some pages of the Manager GUI may not render well with Internet Explorer 6.0 or 7.0. Workaround: Upgrade to Internet Explorer 8 or later or use the Firefox browser.
- When using SNMP to manage WAAS Mobile servers, the dll must be manually registered as follows:
 - a. Open the Windows command prompt.
 - b. Type “cd c:\Program Files\Cisco Systems\WAASMobileServer”.
 - c. Type “rundll32.exe AccelSnmpXa.dll, DllRegisterServer”.
 - d. Reboot.
- When the WAAS Mobile Manager is configured to send email alerts notifying an administrator that a system report has been generated, the system report for only one of the worker servers associated with the event is listed in the email. The other system reports are posted on the Manage > System Reports page of the WAAS Mobile Manager.
- If PCs are cloned, connected clients may not displayed on the Manage > Clients page. Workaround: Use client registration to ensure that unique client names are used.
- If the WAAS Mobile Manager password is updated while a worker server is offline, the worker server will not authenticate with the WAAS Mobile Manager when it is brought back online and hence, will not manage that server. Workaround: Manually update the password on the worker server by changing it's management authority to be locally managed and then entering the new password. Once the updated password has been entered, reconfigure the worker server to be managed by the WAAS Mobile Manager.
- Refresh button does not work on some WAAS Mobile Manager pages. Workaround: Manually refresh the page.
- In some cases, after a license expires and a new license is entered, the WAAS Mobile Manager fails to automatically restart. Workaround: Restart the ControllerService after applying the new license key.

Resolved Caveats in Software Version 3.5.4

The following caveats have been resolved in software version 3.5.4.

Management Caveats

- **CSCty51776**—Fixed issue where number of TCP connections occasionally showed a very high value. Note that the old PostgreSQL database must be uninstalled and then reinstalled as part of this upgrade in order for this fix to be applied.
- **CSCty62039**—Database log rotation has been fixed.
- **CSCtx21686**—Protection against low memory condition added which restarts services if available memory drops below 256 MB for more than 30 minutes.
- **CSCtw87728**—Display of Cyrillic character computer names in the Cisco WAAS Mobile Manager interface is now supported.

- **CSCtt96239**—Localization issue that resulted in high CPU usage has been fixed.
- **CSCtx65887**—The traffic timeline table is now populated correctly. Note that the old PostgreSQL database must be uninstalled and then reinstalled as part of this upgrade in order for this fix to be applied.

Acceleration Caveats

- **CSCty62073**—Issue with downloading files from non-standard file servers resolved by handling varying word count lengths in the protocol message.
- **CSCts42486**—CIFS SMB protocol optimization configuration defaults modified to eliminate potential edge case where file would not open.
- **CSCtt20099**—The VoIP preservation bandwidth allocation feature was broken in Release 3.5.3 and this has been fixed.
- **CSCty62112**—The issue that was caused when accelerating HTTPS with generic optimization for secure sites for which certificates are already in trusted stores on client and server, has been resolved.
- **CSCtw99103**—HTTPS acceleration when virtual domains are used is now properly supported.

Open Caveats in Software Version 3.5.4

The following caveats are open in software version 3.5.4.

Management caveats

- **CSCth06923**—DBCS characters, such as those used for Japanese characters, are not supported by WAAS Mobile, resulting in the following issues:
 - Client system report transmission fails if Windows Login name contains DBCS.
 - Japanese text is garbled in the description field of a System Report.
 - Client log entries in the Event Log show nothing if c_working.log contains DBCS characters in path name.
 - If DBCS characters are entered, the field value cleared without notification and the value isn't used.
 - OK and Cancel buttons disappear from “Editing Server Profile” dialog if DBCS characters are entered in the Profile field.
 - DBCS text sent in a message to a user is garbled.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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.

© 2012 Cisco Systems, Inc. All rights reserved.

