



Release Note for the Cisco WAAS Mobile

April 25, 2008



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

Contents

This release note applies to the maintenance release software version 3.3.1342.4 for the Cisco Wide Area Application Services (WAAS) Mobile product.

This release note contains the following sections:

- [Introduction](#)
- [WAAS Mobile Product Overview](#)
- [Upgrading from Version 3.3.1321.3](#)
- [Upgrading from a Version Prior to 3.3.1321.3](#)
- [Related Documents](#)
- [New and Changed Features](#)
- [Operating Considerations](#)
- [Open Caveats in Software Version 3.3.1342.4](#)
- [Resolved Caveats in Software Version 3.3.1342.4](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)



Introduction

This document contains the release notes for Cisco WAAS Mobile version 3.3.1342.4. This is a maintenance release to the Cisco WAAS Mobile for evaluation and usage. Instructions for use of this product are detailed in the following documents:

- *Cisco WAAS Mobile Integration Guide*
- *Cisco WAAS Mobile System Administration Guide*
- *Cisco WAAS Mobile Software User Guide*

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.

By default, Cisco WAAS Mobile proxies 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 via 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 not in this list will be "bypassed".

Upgrading from Version 3.3.1321.3

This procedure applies to upgrading WAAS Mobile from version 3.3.1321.3 to version 3.3.1342.4.

1. Uninstall the WAAS Mobile Manager and WAAS Mobile Server from the server machine.
2. Install the new version of your WAAS Mobile Manager and WAAS Mobile Server (in that order) on the server machine.
3. Open the WAAS Mobile Manager by entering the URL "http://<IP of the server>/waasmobile" in a browser.
4. In the Cisco WAAS Mobile Manager Server Configuration, enable component upgrades.
5. Navigate to the Status page by clicking the Home link in the upper left of the screen, and start the server by clicking the Start Server button.

Upgrading from a Version Prior to 3.3.1321.3

This procedure applies to any pre-release or release version of WAAS Mobile prior to version 3.3.1321.3. For version prior to build 1321, it is necessary to completely uninstall both the client software installation and the server installation. See the WAAS Mobile Admin Guide for a detailed description of install and uninstall procedures.

1. In the old software, disable upgrades.
 - a. In the WAAS Mobile Manager, navigate to Server Configuration and click the Upgrades menu item.
 - b. If the Enable Component Upgrades checkbox is checked, uncheck it and click the Submit button.
2. Uninstall the WAAS Mobile Manager and WAAS Mobile Server from the server machine.
3. Install the new version of your WAAS Mobile Manager and WAAS Mobile Server (in that order) on the server machine.
4. Open the WAAS Mobile Manager by entering the URL "http://<IP of the server>/waasmobile" in a browser.
5. Navigate to the Status page by clicking the Home link in the upper left of the screen, and start the server by clicking the Start Server button.
6. Navigate to the Client Configuration and click the Manage Distributions link.
7. Click on a client distribution to select it, and click the Download Distribution button. Save the clientdistribution.cab file when prompted.
8. Extract the contents of the clientdistribution.cab file to a local directory and distribute them to the intended client machines in whatever way is most convenient.
9. On every client machine that the new version will be on, you must uninstall the old WAAS Mobile client and install the new distribution by running the clientsetup.exe (from a folder that contains all the other files that were in clientdistribution.cab).

Any prior version of WAAS Mobile client that tries to connect to the upgraded server will get a "Version Mismatch" error in their Connection Monitor and will be unable to connect to the new server. This is the desirable result of having turned off the automatic upgrade feature in

Step 1b above, and is useful as it lets the user and admin know that the client machine's old WAAS Mobile client needs to be uninstalled.

Note that once every client machine has been successfully upgraded, it is worth re-enabling component upgrades so that future upgrades to the server will be passed on to the clients.

Related Documents

In addition to this Release Note, the following documents are also available:

Cisco WAAS Mobile Integration Guide - Provides information required by network engineers as they consider the deployment of the Cisco WAAS Mobile Server. It provides detailed discussion of aspects of deployment such as firewalls, network topology, authentication and accounting.

- *Cisco WAAS Mobile Administration Guide*— Everything needed to set up and administer Cisco WAAS Mobile.
- *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.

New and Changed Features

Release 3.3.1342.4 includes the following changes:

- Performance when using certain anti-virus programs has been improved by modifying file extensions so as to avoid repeated scanning during operation.
- Cisco WAAS Mobile Manager now provides improved control over client configuration settings. Previously, if a user changed settings locally, these changes overrode any future attempts by an administrator at the central management server to reset these settings. With Release 3.3.1342.4, the local user may change settings, but if an administrator at the central management server subsequently modifies these settings, the administrator's settings will over-write the local user's settings.
- Ability to import and export configuration settings is added to Cisco WAAS Mobile Manager.
- IP Routability Scheme is now turned off by default.
- Process Acceleration List is added to HTTPS Settings page in Cisco WAAS Mobile Manager.
- Cisco WAAS Mobile no longer supports client IP Preservation.

Operating Considerations

- Cisco WAAS Mobile is incompatible with Microsoft Firewall Client (MFC) for ISA Server. This incompatibility is caused by a LSP conflict and applies to all versions of MFC and on all operating systems. Workaround: Uninstall Microsoft Firewall Client.
- Cisco WAAS Mobile client fails to connect to the WAAS Mobile Server when logged in to the server using Microsoft Windows Guest accounts.
- Installing Trend Micro Internet Security 2007 after installing Cisco WAAS Mobile causes Cisco WAAS Mobile to cease accelerating connections. Trend Micro Security 2007 intercepts data before it gets to the client, so the data bypasses the client. (The client is not in bypass mode, it is just not receiving data from the client process.) When this occurs, the user will not see the connection stats increment on the client and will not experience acceleration.
- HTTPS high performance acceleration only works with Internet Explorer and applications that leverage the Windows Crypto API.
- Disabling Accelerated Folders through client config update requires a Cisco WAAS Mobile client restart to take effect.
- Accelerate folders are being depreciated. Use transparent CIFS/SMB instead.

Open Caveats in Software Version 3.3.1342.4

The following caveats are open in software version 3.3.1342.4.

- **CSCsm77932**—You may receive the error "Failed to package distribution. Could not set address properly on installer" when creating a client distribution in Cisco WAAS Mobile Manager. This error can occur if Cisco WAAS Mobile Manager/.NET Runtime is installed on a Windows machine that is a Domain Controller. Some manual configuration of ASP.NET and Windows is required to avoid this error. See this URL for more info: <http://support.microsoft.com/kb/315158>. Workaround: Do not install Cisco WAAS Mobile on a Windows Domain Controller.
- **CSCsm77950**—Cisco WAAS Mobile Manager installation via AutoRun requires a second click of the Cisco WAAS Mobile Manager button after prerequisites are installed.
- **CSCsm77973**—IP Exclusion List feature does not apply to transparent SMB acceleration.
- **CSCsm77988**—Cannot download client distribution .cab file from Cisco WAAS Mobile Manager using IE7 on some Windows 2003 machines.
- **CSCsm78019**—Cisco WAAS Mobile causes extra prompts for credentials when a user accesses a file server by IP address, or when the CIFS client cannot use Kerberos authentication with the file server. Workaround: Use host names instead of IP addresses
- **CSCsm78042**—Transparent CIFS requires special configuration when Windows file servers are not using the default settings, namely CIFS file servers that serve both SMB hosted directly over TCP/IP (port 445) and NetBIOS over TCP/IP (port 139).
- **CSCso53919**—A user may see the "Insufficient data to graph" message when refreshing the Traffic Summary page when greater than 2GB of data was uploaded and/or downloaded within a particular session.
- **CSCso53401**—WinPcap version 3.1 provided as a part of Cisco WAAS Mobile Server installation cannot be installed on 64bit platforms. See this URL for more info: <http://www.winpcap.org/misc/faq.htm>
- **CSCso53410**—After importing system settings in the Import/Export Cisco WAAS Mobile Manager page, it might appear that certain changes haven't taken effect. Workaround: close and restart the browser.
- **CSCso53417**—No logs generated in Debug and URL only logging modes.
- **CSCso53427**—Transparent SMB does not support the persistent sessions feature. Connections opened via transparent SMB will not be maintained when a short network outage occurs.
- **CSCso53451**—Very quickly scrolling down a large Accelerated Folders directory that contains thousands of files and folders freezes the explorer window.
- **CSCso53463**—Vista and XP users cannot join domain while Cisco WAAS Mobile client is running. Workaround: Exit the Cisco WAAS Mobile client before trying to join the domain.

Resolved Caveats in Software Version 3.3.1342.4

The following caveats were resolved in software version 3.3.1342.4.

- **CSCsm77569**—Intermittent issues have been resolved when saving .doc files to an EMC Celerra Server when using Cisco WAAS Mobile on Windows XP.
- **CSCsm77618**—Cisco WAAS Mobile client running on a Windows Vista machine blocks access to Windows 2008 File Servers.
- **CSCsm78000**—Cisco WAAS Mobile incompatible with F-Secure Anti-Virus have been resolved.
- **CSCso48047**—Leases table have been corrected to show proper UK time date stamp format of DD-MM-YYYY.
- **CSCso48071**—Cisco WAAS Mobile Server has been corrected to avoid sending erroneous UDP pings to the client after the user exits the client.
- **CSCso48086**—Operational problems with passive FTP with SecureFX have been resolved.
- **CSCso48095**—ITP poor performance problems caused by improper bandwidth reading when switching from low to high bandwidth network have been resolved.
- **CSCso48108**—Cisco WAAS Mobile Manager Application Traffic page no longer displays an invalid image.
- **CSCso48116**—F5 SSL VPN now connects on first attempt when Cisco WAAS Mobile client is installed on the machine.
- **CSCso48127**—WAAS Mobile Manager Status has been updated to ensure display of all error events.
- **CSCso48132**—A typo in the Tooltip mouse-over text on WAAS Mobile Manager Server Configuration page text has been corrected to display 'Submit.'
- **CSCso48143**—When the 'View All' time option is selected on the WAAS Mobile Manager Application Traffic screen, the erroneous error message no longer appears and the graph displays properly.
- **CSCso48173**—Occasional extra authentication prompts during file share access have been corrected.
- **CSCso48187**—Connecting to FTP servers that do not support passive FTP mode no longer causes an FTP client crash or WAAS Mobile client crash.
- **CSCso48192**—The WAAS Mobile Manager Raw Bytes Received statistic no longer reports negative values.
- **CSCso48203**—The Firefox browser no longer produces error messages running with WAAS Mobile if SSL proxy is setup for port 80.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, 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. (0804R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

