



Release Note for the Cisco WAAS Mobile

April 28, 2009



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

This release note applies to software version 3.4.2 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](#)
- [Deprecated Features](#)
- [Operating Considerations](#)
- [Resolved Caveats in Software Version 3.4.2](#)
- [Open Caveats in Software Version 3.4.2](#)
- [Obtaining Documentation and Submitting a Service Request](#)

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 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 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 associated with processes not in this list will be "bypassed."



Americas Headquarters:

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

© 2009 Cisco Systems, Inc. All rights reserved.

Related Documents

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

- *Cisco WAAS Mobile Administration Guide*—Everything you need to set up and administer 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.
- *Cisco WAAS Mobile Network Design Guide*—Provides network architects with best practices for integrating WAAS Mobile with various distributed network topologies and usage scenarios.
- *Cisco WAAS Mobile Integration Guide*—Provides information required by network administrators 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.

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 3.4.1](#)
- [Upgrading from Version 3.4.0](#)
- [Upgrading from Version 3.3.1342.4](#)
- [Upgrading From a Version Prior to 3.3.1342.4](#)
- [Downgrading to an Earlier Version of Software](#)

Upgrading from Version 3.4.1

This procedure applies to upgrading WAAS Mobile from version 3.4.1.

1. Prior to upgrading:
 - a. Enable Component Upgrades by navigating to Server Configuration > Upgrades and selecting "Enable Component Upgrades."
 - b. Navigate to the Home > Status page and select "Stop Server."
2. Install the new version of WAAS Mobile Manager on the server machine by double-clicking on the "ServerSetup.exe" file. Your current configuration settings will be saved automatically, the 3.4.1 software will be uninstalled, the new version installed, and your previous configuration will be restored during the upgrade process.
3. Navigate to the Home > Status page and select "Start Server". WAAS Mobile clients will be upgraded automatically the next time they connect.



Note

When the upgrade completes, users will be prompted to reboot. Acceleration will be disabled (indicated by the gray task bar icon) until the reboot occurs; at that time, the client will reconnect and begin accelerating, and the icon will turn green.

4. If you are currently using the IP aliasing feature, perform the following steps after installing 3.4.2:
 - a. Turn off IP Aliasing.
 - b. Reboot the server and confirm that no aliased IP addresses exist on the NIC card by typing **ipconfig /all** in the command line.
 - c. Reconfigure IP Aliasing to ensure that the valid sources field is filled in and is the same size as the IP Pool.
5. If processes had been added to the HTTPS accelerated process list prior to an upgrade to 3.4.2, only these custom processes will get HTTPS acceleration after the upgrade. To re-enable HTTPS acceleration for the default processes:
 - a. Navigate to the Client Configuration > Http/Https Settings page.
 - b. Click the 'Apply Changes' button at the bottom of the page.

Upgrading from Version 3.4.0

This procedure applies to upgrading WAAS Mobile from version 3.4.0.

1. Prior to upgrading:
 - a. Enable Component Upgrades by navigating to Server Configuration > Upgrades and selecting "Enable Component Upgrades."
 - b. Navigate to the Home > Status page and select "Stop Server."
2. Install the new version of WAAS Mobile Manager on the server machine by double-clicking on the "ServerSetup.exe" file. Your current configuration settings will be saved automatically, the 3.4.0 software will be uninstalled, the new version installed, and your previous configuration will be restored during the upgrade process.
3. Navigate to the Home > Status page and select "Start Server". WAAS Mobile clients will be upgraded automatically the next time they connect.



Note When the upgrade completes, you will be prompted to reboot. Acceleration will be disabled (indicated by the gray task bar icon) until the reboot occurs. At that time, the client will reconnect and begin accelerating and the icon will turn green.

4. If you have existing client configurations where the proxied process list has been modified, your proxied process list will not be automatically updated to include the default proxied processes that were added in software version 3.4.1. If acceleration of the following processes is desired, you must manually add the existing client distribution's proxied process list:
 - Cisco IP Communicator: communicork9.exe; accel type=4
 - Microsoft Office Communicator: communicator.exe; accel type=4
 - Nortel Unified Communications: SMC.exe; accel type=2
 - Nortel softphone: i2050.exe; accel type=2
 - Microsoft Live Meeting: lm.exe; accel type=4
 - Java Runtime Environment for Oracle: javaw.exe; accel-type=0; auto-reset=yes
 - Chrome browser: chrome.exe; accel type=0
5. If you are currently using the IP aliasing feature, perform the following steps after installing version 3.4.2:

- a. Turn off IP Aliasing.
 - b. Reboot the server and confirm that no aliased IP addresses exist on the NIC card by typing **ipconfig /all** in the command line.
 - c. Reconfigure IP Aliasing to ensure that the valid sources field is filled in and is the same size as the IP Pool.
6. If processes had been added to the HTTPS accelerated process list prior to an upgrade to 3.4.2, only these custom processes will get HTTPS acceleration after the upgrade. To re-enable HTTPS acceleration for the default processes:
- a. Navigate to the Client Configuration > Http/Https Settings page.
 - b. Click the 'Apply Changes' button at the bottom of the page.

Upgrading from Version 3.3.1342.4

This procedure applies to upgrading WAAS Mobile from version 3.3.1342.4. Note that if you are upgrading multiple server farms, you must manually save and restore the farm configuration data for a 3.3 to 3.4.2 upgrade.

To upgrade from version 3.3.1342:

1. Install the new version of WAAS Mobile Manager on the server machine by double-clicking on the "ServerSetup.exe" file. Your current configuration settings will be saved automatically, the 3.3 software will be uninstalled, the new version installed and your previous configuration will be restored during the upgrade process.
2. Verify delta cache size and location. Before starting the server for the first time, be sure to verify the size and location of the delta cache by navigating to the WAAS Mobile Manager Server Configuration > Delta Cache screen. By default, the delta cache will be placed on the same disk partition as the server. For typical deployments, it is recommended that the cache be placed in its own RAID 5 partition.

By default, WAAS Mobile Manager will attempt to set up a 275 GB delta cache. If there is insufficient space available, WAAS Mobile Manager will attempt to set up a fallback cache of 50 GB. See the *Cisco WAAS Mobile Administration Guide* for information on how to change delta cache size settings. If the minimum disk space is not available, delta caching will not be supported and acceleration performance will be limited to transport optimization and compression.

3. Start the Server. Navigate to the WAAS Mobile Manager > Home > Status page and click the Start Server button.
4. Upgrade the client software by navigating to Client Configuration > Client Distributions and selecting the appropriate client distribution from the drop-down menu. The new client distribution packages are created automatically and links to those distributions are posted on the web page.

Note the following considerations:

- When the WAAS Mobile Manager software is upgraded, all users running a 3.3 version of the WAAS Mobile client will disconnect from the WAAS Mobile server (indicated by the gray task bar icon) and a "version mismatch" message appears in the Client Manager event log to indicate that the software upgrade is required. Because this is a major upgrade that involves a kernel driver update, component upgrades are not supported.
- The link to the ".exe" file may be emailed to your clients so that they may download and install the software upgrade manually.

- For automated upgrades, the ".cab" file contains an .msi for deploying with your enterprise software distribution tool (for example, Microsoft SMS).
- Regardless of which software distribution approach is selected, the installation process will uninstall the Release 3.3 software automatically before installing the Release 3.4.2 software.
- You will be prompted to exit all applications prior to installation.
- When the upgrade completes, you will be prompted to reboot. Acceleration will be disabled (indicated by the gray task bar icon) until the reboot occurs. At that time, the upgrade process will complete and the client will reconnect to the server 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.

Note that once every client machine has been successfully upgraded, you should re-enable component upgrades so that future upgrades to the server will be automatically distributed to the clients.

Downgrading to an Earlier Version of Software

To downgrade from version 3.4.2 to version 3.4.1 (or from version 3.4.2 to version 3.4.0), perform the following steps on the server:

1. Uninstall 3.4.2. Re-install 3.4.1 (or 3.4.0).
2. Select the Distribution from the Client Configuration and Enable Component Downgrades.
3. Restart the server.

To downgrade to a version prior to 3.4.0, 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 may need to be manually re-entered.

New and Changed Features

Software version 3.4.2 includes the following enhancements:

- The VoIP bandwidth preservation feature has been enhanced to better match the bandwidth requirements of the latest generation of Cisco and Nortel softphones, as follows.
If the link bandwidth is:
 - less than 142 kbps, 85% of the bandwidth is reserved for VoIP.
 - between 142 and 800 kbps, 120 kbps is reserved for VoIP.
 - greater than 800 kbps, 20% of the link is reserved for VoIP (or other UDP traffic).
- The IP aliasing feature has been enhanced for better client tracking and interoperability with web filter proxies by providing a persistent mapping of client IP addresses to server-side addresses
- SharePoint over HTTPS is now accelerated by default when HTTPS acceleration is enabled, eliminating manual configuration steps.

- The SNMP MIB has been enhanced to provide clearer reporting of key metrics. Additionally, the OIDs have been modified for improved interoperability with certain network management tools.

Minor enhancements include:

- WAAS Mobile configures the Internet Explorer browser to automatically look for new versions of stored pages. A registry key has been added to allow administrators to optionally disable this setting.
- Farm selection is better supported for users that travel between offices and use LAN connections in each location, as the client will first use latency-based farm selection to make sure that the server previously used is still the best server.

Deprecated Features

The following features have been deprecated in software version 3.4.2:

- GUI to manage user authentication (list-based and RADIUS) and RADIUS accounting.
- Farm selection based on client IP address. Latency-based farm selection will continue to be supported and will be used to select the best server farm.
- RDBMS logging. Logging will employ log files only, however the RDBMS logging option will no longer be longer supported.
- Many-to-one IP aliasing. Only one-to-one IP aliasing will be supported.
- Prioritized server selection method for selecting a server within a farm. Randomized server selection with persistent affiliation will continue to be supported.

Operating Considerations

Operating considerations include the following categories:

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

Interoperability Considerations

- Cisco WAAS Mobile Manager should not be installed on a Windows Domain Controller.
- Cisco WAAS Mobile Manager requires that the inetpub directory be configured on the C: drive.
- Cisco WAAS Mobile is incompatible with the APC InfraStruXure Manager client. Workaround: Uninstall the APC InfraStruXure Manager client.
- 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 on all OSs. Workaround: Uninstall Microsoft Firewall Client.
- Installing Trend Micro Internet Security 2007 after installing Cisco WAAS Mobile causes Cisco WAAS Mobile to cease accelerating CIFS SMB 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 statistics increment on the client and will not experience acceleration.

- When interoperating with the CheckPoint IPsec VPN client, the network monitoring feature on the client should not be enabled. Note that this feature is disabled by default.

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.
- The WAAS Mobile Manager should be configured in a production mode (that is, configured as a subordinate CA to the enterprise CA) when accelerating the following:
 - HTTPS from browsers other than Internet Explorer
 - Encrypted Oracle Forms traffic
- When persistent sessions are employed, a DNS name must be used to refer to the WAAS Mobile Manager server.
- 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.
- When using Outlook 2007 with Exchange 2007, the Meeting Room Request feature is not supported. Workaround: Disable Outlook 12 protocol optimization for those users who require this feature.

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.
- Once delta cache encryption has been enabled on the client or server, it cannot be disabled using WAAS Mobile Manager.

Resolved Caveats in Software Version 3.4.2

The following caveats have been resolved in software version 3.4.2:

Performance caveats

CSCsx95687—DFS shares are now properly accelerated, fixing an issue that was introduced in Release 3.4.1.

CSCsy72260—CIFS optimization now properly accelerates applications that use short file names to represent long file names (for example, WIN32_~1.exe to represent WIN32_muchlongername.exe).

CSCsy72246—Active FTP is now properly accelerated, fixing an issue that was introduced in software version 3.4.1.

Management caveats

- **CSCsw69944**—SNMP traps now correctly reports the OIDs.
- **CSCsy72279**—The localization issue associated with activating the 5-user, 30-day trial license has been resolved.

Installation caveat

- **CSCsy72294**—After installing a server upgrade, the installation script will no longer occasionally prompt the user to uninstall the software after successfully completing installation.

Open Caveats in Software Version 3.4.2

The following caveats are open in software version 3.4.2:

Management caveats

- **CSCso53417**—WAAS Mobile Manager in Debug and URL-only logging modes does not function properly.
- **CSCsr54075**—The WAAS Mobile Manager log viewer timeline filter does not function properly.
- **CSCsr54087**—The WAAS Mobile Manager control to restore default settings on the Client Configuration > File Shares page does not function properly.
- **CSCsu60386**—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.

Performance caveats

- **CSCsr56236**—Application protocol optimization is not supported for MAPI 2000 and earlier. Workaround: When accelerating email traffic from an Exchange 2000 or earlier server, set the acceleration mode for all Outlook versions to 'generic' on the Client Configuration > Proxied Process list screen. Similarly, when accelerating email traffic to clients running Outlook version 9 or earlier, set the Outlook version 9 acceleration mode to 'generic'. These settings ensure that MAPI transport optimization and data reduction/compression techniques are applied.
- **CSCsw69978**—Acceleration of signed SMB traffic between Vista clients and Windows Server 2008 is not supported. Workaround: Disable SMB signing on the file server.
- **CSCsv78422**—CIFS optimization is supported for SMB over TCP or NetBIOS over TCP, but not both simultaneously.

Authentication caveats

- **CSCsr54134**—When logged into a computer via domain credentials and attempting to map a drive with a different set of credentials, users are prompted for credentials multiple times.
- **CSCsm78019**—Cisco WAAS Mobile causes extra prompts for credentials when users access 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.
- **CSCsy72308**—In some deployments, Vista clients may occasionally be prompted for credentials by the domain controller. Workaround: Verify that the domain controller has been excluded from being accelerated.
- **CSCso53463**—Users cannot join a domain while Cisco WAAS Mobile client is running. Workaround: Users should exit the Cisco WAAS Mobile client before trying to join the domain.

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store 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. (0903R)

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.