



Cisco WAAS Mobile Administration Guide

Software Version 3.4

July 2008

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-15416-03

Contents

Contents	i
List of Tables	iii
List of Figures	iv
About this Document	vi
Intended Audience	vi
Document Outline.....	vi
Related Documents.....	vi
Chapter 1 Overview	1
Product Overview.....	1
Chapter 2 Hardware and Software System Requirements	2
Software Compatibility	3
Chapter 3 Cisco WAAS Mobile System Installation	6
Pre-Installation System Check.....	6
WAAS Mobile Server Installation.....	7
WAAS Mobile Client Installation	10
Chapter 4 Configuring the Cisco WAAS Mobile Client	14
Client Distributions	14
Diagnostics.....	15
User Interface.....	16
Connection Settings	17
HTTP / HTTPS Settings.....	21
Exclusion Lists	24
Accelerated Networks	25
Proxied Process List.....	26
File Shares	28
Delta Cache Settings	29
Chapter 5 Configuring the Cisco WAAS Mobile Server	31
Licensing	31
Authentication.....	32
Logging.....	37
Server Farm.....	40
Advanced Settings	44
Import/Export.....	54
Chapter 6 Managing WAAS Mobile	55
Status and Server Control.....	56
System Alarms.....	57
Performance Monitoring.....	57
Active Sessions Reports.....	65
Past Sessions Reports.....	68

Log File	70
System Reports	71
Chapter 7 Diagnostics	73
Server-Side Diagnostics.....	73
Client-Side Diagnostics	75
Chapter 8 Troubleshooting	78
Problem Isolation	79
Chapter 9 System Status Reports	92
Generating a System Report from a Client Computer	92
Generating a System Report from the WAAS Mobile Server	93
Chapter 10 List of Acronyms.....	94

List of Tables

Table 1 Server Hardware System Requirements.....	2
Table 2 Client Hardware System Requirements	2
Table 3 Server Software Requirements.....	3
Table 4 Client Software Requirements	3
Table 5 Protocols and Applications Compatible with Cisco WAAS Mobile.....	3
Table 6 WAAS Mobile Server Issues and Isolation.....	79
Table 7 WAAS Mobile Client Issues and Isolation	80
Table 8 WAAS Mobile Client Event Messages.....	82
Table 9 WAAS Mobile Server Event Messages	88

List of Figures

Figure 1 License Information	8
Figure 2 Client Software Distribution Window	10
Figure 3 Client Distribution List.....	10
Figure 4 New Client Distribution File	11
Figure 5 Client File Download.....	12
Figure 6 Client Registration	12
Figure 7 Diagnostics Settings	15
Figure 8 Client User Interface Settings	16
Figure 9 Connection Settings	17
Figure 10 HTTP and HTTPS Settings.....	21
Figure 11 Exclusion Lists Settings	24
Figure 12 Accelerated Networks	25
Figure 13 Proxied Process List	26
Figure 14 File Shares Settings.....	28
Figure 15 Delta Cache Settings	29
Figure 16 Authentication Settings	32
Figure 17 User Management Screen.....	33
Figure 18 RDBMS Authentication Settings	34
Figure 19 Radius Authentication Settings.....	35
Figure 20 Logging Settings.....	37
Figure 21 RDBMS Logging Settings	38
Figure 22 Log Rotation Settings.....	39
Figure 23 Server Farm Settings.....	40
Figure 24 Configure Single Server farm	41
Figure 25 Configure Multiple Server Farms	41
Figure 26 Server Selection and Farm Selection Methods	42
Figure 27 HTTP Prefetching Settings.....	45
Figure 28 Delta Cache Settings	46
Figure 29 Radius Accounting Settings.....	47
Figure 30 Aliasing Settings.....	48
Figure 31 Access Control Settings	49
Figure 32 Upgrade Settings	50
Figure 33 System Reports Settings	52
Figure 34 Import/Export Settings.....	54
Figure 35 Status.....	56
Figure 36 System Alarms.....	57
Figure 37 Traffic Summary – Application Summary	58
Figure 38 Traffic Summary – Compression Summary	58
Figure 39 Application Traffic	59

Figure 40 Session Monitoring	60
Figure 41 HTTP Details Monitoring.....	61
Figure 42 Disk System Monitoring.....	62
Figure 43 Server System Statistics Monitoring	63
Figure 44 Delta Cache Monitoring	64
Figure 45 Active Sessions - Connection Time.....	65
Figure 46 Active Sessions - Traffic Volume	65
Figure 47 Active Sessions - Link Performance.....	66
Figure 48 Active Sessions - Delta Cache Performance	66
Figure 49 Active Sessions - Installation Information	66
Figure 50 Active Sessions - Management.....	67
Figure 51 Past Sessions - Connection Time History.....	68
Figure 52 Past Sessions - Traffic Volume History	68
Figure 53 Past Sessions - Link Performance History	69
Figure 54 Past Sessions - Delta Cache History.....	69
Figure 55 Past Sessions - Client Installation History.....	70
Figure 56 Log File	70
Figure 57 System Reports Monitoring	71
Figure 58 Acceleration Icon in System Tray	75
Figure 59 Client Manager - Connection Monitor Tab.....	76
Figure 60 WAAS Mobile System Tray Icon Menu	92
Figure 61 Client Manager - Support Tab	92
Figure 62 System Report - Additional Information.....	93

About this Document

Intended Audience

This guide is intended for administrators of the Cisco WAAS Mobile software. Administrators may be responsible for any or all of the following tasks:

- Installing, configuring, and monitoring the WAAS Mobile server
- Creating, distributing, and installing the WAAS Mobile client on end user machines
- Providing support for Cisco WAAS Mobile end users

Document Outline

- *Overview* – briefly describes the overall WAAS Mobile system.
- *Hardware and Software System Requirements* – hardware and software requirements for optimal operation of the WAAS Mobile system.
- *Cisco WAAS Mobile System Installation* - describes installation and upgrade procedures for the WAAS Mobile server and client software.
- *Configuring the Cisco WAAS Mobile Client* – provides instructions for configuring and managing client software distributions.
- *Configuring the Cisco WAAS Mobile Server* – provides instructions for configuring the acceleration server.
- *Managing WAAS Mobile* - provides instructions for operating the acceleration system.
- *Diagnostics* – provides a high level summary of the various types of diagnostic information that are generated.
- *Troubleshooting* – provides guidance on how to troubleshoot and resolve WAAS Mobile client and server issues.
- *System Status Reports* – provides detailed instructions for creating and using system status reports used by support personnel to isolate and diagnose problems.

Related Documents

In addition to this Administration Guide, the following documents are also available:

- *Cisco WAAS Mobile Integration Guide* – Provides information required by network engineers as they consider the deployment of the WAAS Mobile server, covering discussion topics such as firewalls, network topology, authentication and accounting.
- *Cisco WAAS Mobile User Guide* – A guide for the WAAS Mobile 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 Release Notes* – Release-specific information regarding features added, changed, and removed as well as known and resolved issues.

Chapter 1 Overview

Product Overview

Cisco Wide Area Application Services (WAAS) Mobile extends Cisco® WAAS software application acceleration benefits to teleworkers, small and home office workers, and mobile employees who travel outside the branch office. Compared to corporate WAN and branch-office optimization, acceleration of mobile VPN connections over the public Internet brings new technical challenges:

- Quality of the network connection lower than the corporate WAN: Rather than using dedicated branch-to-corporate WAN leased lines, mobile users are using public Internet connections such as DSL, Wi-Fi, satellite, dial-up, cable, and cellular. These connections have lower bandwidth, higher packet loss and latency, and additional challenges such as time-slicing delay in cellular environments;
- Small footprint on PC/laptop: In contrast to branch-office users who can rely on a dedicated branch-office device for application acceleration, mobile users have to share laptop or PC computing resources and the TCP software stack with numerous other PC applications;
- Support cost and manageability concerns: The open environment of a Windows PC, in contrast to the controlled environment of an appliance, has a very different class of stability and interoperability requirements, with a variety of operating systems, browser versions, end point security applications, VPN client software and a wide range of business applications.

To address these challenges, Cisco WAAS Mobile requires the smallest PC footprint and the lowest Total Cost of Ownership (TCO) normally associated with mass-user deployment of PC software, plus it achieves industry-leading performance under the most challenging network connectivity conditions by extending Cisco WAAS acceleration technologies to include the following:

- Advanced data transfer compression: Cisco WAAS Mobile maintains a persistent and bi-directional history of data on both the mobile PC and the Cisco WAAS Mobile server. This history can be used in current and future transfers, across different VPN sessions and during temporary network disconnects, to minimize bandwidth consumption and improve performance.
- Application-specific acceleration for a broad range of applications including:
 - Microsoft Exchange: Microsoft Outlook Messaging API (MAPI)
 - Windows Common Internet File System (CIFS)
 - HTTP, supporting enterprise web-based intranet and Internet applications
 - HTTPS for secured intranet applications without compromising security
- Transport optimization: Cisco WAAS Mobile handles the timing variations found in packet switched wireless networks, the significant bandwidth-latency problems of broadband satellite links, and noisy Wi-Fi and DSL connections. The result is significantly higher link resiliency.

Chapter 2 Hardware and Software System Requirements

This section details hardware and software requirements for proper system performance.

Table 1 Server Hardware System Requirements

	Minimum	Recommended	
	Small Server	Mid-Size Server	High Capacity Server
CPU	Dual Core 1.8-GHz	Dual QuadCore 1.6 GHz	Dual QuadCore 2.6 GHz
System Memory (RAM)	2 GB	8 GB	16 GB
Hard Drive	80-GB 7.2K RPM	4 x 146-GB 15K RPM	4 x 300-GB 15K RPM
Max cache size (gigabyte)	50 GB	318 GB	748 GB
RAID?	no	RAID 1 & RAID-5	RAID 1 & RAID-5
Interface	Dual 1-GBE NIC card	Dual 1-GBE NIC card	Dual 1-GBE NIC card
Capacity (max concurrent users)	50	2,000	8,000
Capacity (max active users)	12	500	2,000

When multiple disks are employed, the following configuration is recommended:

- Partition 1: 30 GB RAID-1 mirror for Operating System and WAAS Mobile
- Partition 2: remaining disk space: RAID-5 for cache

Table 2 Client Hardware System Requirements

	Minimum	Recommended
CPU	750 MHz	1.5 GHz
System Memory (RAM)	512 MB	512 MB
Disk Space Available for Cache	80 MB	1 GB

Table 3 Server Software Requirements

Operating Systems supported:

- Windows Server 2003, Standard Edition (optionally with SP1)
- Windows Server 2003 R2, Standard Edition (optionally with SP2)
- Windows Server 2003 x64, Standard Edition
- Windows Server 2003 R2 x64, Standard Edition (optionally with SP2)

Internet Information Server (IIS) version 6 or higher.
ASP.NET v2.0 Framework

Table 4 Client Software Requirements

Minimum	Recommended
Windows 2000	Windows XP SP2 or later

Software Compatibility

Cisco WAAS Mobile has been tested and is compatible with the following applications, for the versions listed. Older versions of the programs listed below, as well as other software packages not listed, may also be compatible.

Protocol and Application Compatibility

This table contains the list of enterprise software applications that Cisco WAAS Mobile accelerates, including web browsers, email clients and other web-enabled applications.

Table 5 Protocols and Applications Compatible with Cisco WAAS Mobile

Protocol	Application ¹	Versions
HTTP	Microsoft Internet Explorer	7.0, 6.0, 5.5, 5.0
	Netscape	
	Netscape Communicator	4.75, 4.05
	Opera	
	Mozilla	
	FireFox	
	MSN Explorer	8
	Windows Explorer	
HTTPS	Microsoft Internet Explorer	7.0, 6.0, 5.5, 5.0
FTP	Microsoft Internet Explorer	7.0, 6.0, 5.5, 5.0
	Netscape	

Protocol	Application¹	Versions
	Netscape Communicator 4.75	4.75, 4.05
	Opera	
	Mozilla	
	FireFox	
	MSN Explorer	8
	Windows Explorer	
	WS-FTP PRO	
SMTP/POP3 (email)	Microsoft Outlook	2007, 2003, 2002, 2000
	Eudora	
	Netscape Communicator	
	Email-enabled MS Office Apps	
	Outlook Express	6.0, 5.0
CIFS SMB	Windows Explorer and other applications that use the CIFS protocol. Signed and unsigned SMB supported.	
MAPI	Microsoft Outlook 2007 Online, Cached mode, Encryption not in use	
	Microsoft Outlook 2003 Online, Cached mode	
	Microsoft Outlook 2002 Online, Offline	
	Microsoft Outlook 2000 Online, Offline	
IMAP4 (email)	Microsoft Outlook	All Versions
	Outlook Express	All Versions
Lotus Notes (email)	Lotus Notes	
Microsoft Office	Microsoft Office 2007	
	Microsoft Office 2003	
	Microsoft Office XP	
Misc. Applications	Citrix/RDP (compression and encryption disabled)	
	Microsoft Remote Desktop (Terminal Services)	
	Misc test utilities (wget, urlclnt, curl)	

¹ Applications that do not appear on this list can be added by the enterprise administrator. However, only the applications listed have been certified for use with Cisco WAAS Mobile.

Antivirus/Security Software Interoperability

- McAfee Virus Scan Enterprise Version 8.0
- McAfee Internet Security Suite 2007
- Norton Internet Security 2006
- Norton 360 Version 1.0
- Norton Anti Virus 2007
- CA Antivirus 2007
- Trend Micro PC-Cillin 2005
- Microsoft Windows Firewall
- Panda Antivirus 2008
- Kaspersky Internet Security 7.0
- AVG Anti-Virus Versions: 7.0, 7.5
- Bit Defender 2008

VPN Software Interoperability

- A broad range of IPsec VPNs, including
 - Cisco VPN Client Versions: 4, 5
 - Nortel Contivity VPN Client Versions: 5, 6
 - Checkpoint Versions: R55, R60
- SSL VPNs
 - Cisco SVC, Thin Client, and Clientless WebVPN
 - Juniper Network Connect, Secure Application Manager, and Clientless Core Web Access
 - Nortel Net Direct, Enhanced Clientless, and Clientless Web Access
 - F5 FirePass Network Access

Software Incompatibilities

The software programs below are not interoperable with the Cisco WAAS Mobile client and are therefore not supported.

- Microsoft ISA Server Firewall Client
- Avira AntiVir AntiVirus
- Citrix Metframe Secure
- Trend Micro Internet Security 2007
- Embassy Trust Suites (see note below)

NOTE : Uninstalling the LSP component of Embassy Trust Suites resolves this issue. See: <http://www.wavesys.com/support/Documents/PBA/PBA-008.asp>.

Chapter 3 Cisco WAAS Mobile System Installation

This chapter describes the procedures an administrator will need to use in order to install the Cisco WAAS Mobile software.

This chapter contains the following sections:

- Pre-Installation System Check
- WAAS Mobile Server Installation
- WAAS Mobile Client Installation

Pre-Installation System Check

1. Verify that the computer on which you intend to install the server software meets the system requirements listed in Chapter 2.
2. Do not run other applications, including the client software, on the WAAS Mobile server machine. If anti-virus software is installed on the server, it must be configured to allow outgoing ports that the WAAS Mobile server may use (e.g., SMTP port 25).
3. Verify network routability from the client computers that will run the WAAS Mobile client to the WAAS Mobile server.
4. Verify network routability from the WAAS Mobile server to the content and application servers that will be accelerated.
5. Verify that any firewalls between the WAAS Mobile server and computers running the WAAS Mobile client are configured to allow TCP and UDP access over port 1182.
6. If WAAS Mobile is being installed on a 32-bit Windows OS and the server is configured with 4 GB or more RAM, configure server memory management to allocate additional memory to the user process. To do this, modify the "boot.ini" file to allocate 3 GB of RAM for user space for the WAAS Mobile server, by adding the /3GB option to the appropriate line, as follows:
`multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise" /fastdetect /3GB`

IMPORTANT: When deploying with a Windows 32-bit OS, memory management must be properly configured to achieve desired server performance.

7. Read the **Release Notes**.

WAAS Mobile Server Installation

Initial Installation of the WAAS Mobile Server Software

To perform the procedures in this section, you must be logged into the server computer as a user with administrator privileges.

Install the WAAS Mobile server as follows:

1. Verify that IIS is running.

NOTE: WAAS Mobile sets IIS to use NTLM authentication only and installs on IIS port 80.

2. Download software from link provided by Cisco.
3. Install server software by clicking on the ServerSetup.exe file.
4. When installation completes, a browser window will open and display the WAAS Mobile Manager **Home** page. If this page does not open automatically or if you receive an error, verify that IIS permissions are set correctly.

NOTE: It may take some time to load the page for the first time.

5. Before proceeding with the installation, read the **Release Notes** thoroughly.
6. Obtain a license key by sending the Network Adapter Address of one of the NIC cards installed on the server machine to your Cisco sales representative.

IMPORTANT: If your server is running on a virtual machine, and change to the Media Access Control (MAC) address may cause your license key to fail.

License keys are affiliated with MAC addresses, so a new key will be required to re-host the WAAS Mobile server. Please contact your Cisco sales representative to obtain new keys prior to re-hosting your application.

7. Enter the license key by clicking on the WAAS Mobile Manager **Server Configuration > Licensing** page, and entering the license number sent in the license.dat attachment and click **Submit**.

License Information

License Key: 2F3A397CDDAD81255654B01C8450F8B23D01E9898

Network Adapter Address: 0019D14E3733

Maximum Number of Active Users: 100

License Expiration Date: 11/14/2008 (366 days remaining)

Server Type: N/A

Customer Type: Full Enterprise

Submit

Figure 1 License Information

NOTE: Only licenses that are issued for evaluation and test purposes have an expiration date. Production licenses do not expire.

8. Verify Delta Cache size and location by navigating to the WAAS Mobile Manager **Server Configuration > Advanced Settings > Delta Cache** screen.

IMPORTANT: Before starting the server for the first time, verify the size and location of the delta cache.

- By default, delta cache is placed on the same disk partition as the server. For typical deployments, it is recommended that cache be placed in its own RAID 5 partition.
- By default, WAAS Mobile will attempt to configure a 275 GB cache. If there is insufficient space available, a fallback cache of 50 GB will be attempted. A minimum of 50 GB of delta cache disk space is required

IMPORTANT: If the minimum disk space is not available, then delta caching will not be supported and acceleration performance will be limited to transport optimization and compression.

9. If the WAAS Mobile server software is being installed on a drive other than C: (i.e., the parent inetpub directory is not on C:), then, after installation, change the IIS directory property "Local Path:" to the drive letter on which it was installed.
10. Start the Server. Navigate to the WAAS Mobile Manager **Home > Status** page and click the **Start Server** button.

Uninstalling the WAAS Mobile Server Software

To uninstall the WAAS Mobile server software:

1. From the Control Panel, select **Add/Remove Programs**.
2. Select Cisco WAAS Mobile Server from the list, and click the **Remove** button.
3. The server software will be removed from the system.

Upgrading the WAAS Mobile Server Software

To upgrade the WAAS Mobile server software:

1. Stop the WAAS Mobile server by navigating to the WAAS Mobile Manager **Home > Status** page and clicking the **Stop Server** button
2. Install the new software version; the previous version will be automatically uninstalled and your current configuration will be automatically saved and reloaded.
3. Proceed to upgrade the WAAS Mobile client software.

WAAS Mobile Client Installation

Initial Installation of the WAAS Mobile Client Software

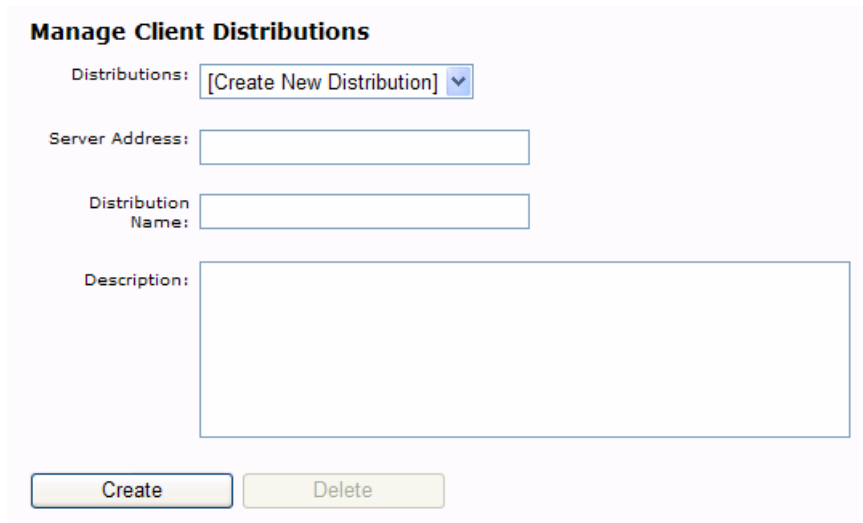
Before the WAAS Mobile client can be installed, a client distribution must be created. The required steps are:

- Create
- Configure
- Distribute
- Install

NOTE: For best operation, do not install the client software on the WAAS Mobile server machine.

Creating a Client Distribution

1. Go to the **Client Configuration** section of WAAS Mobile Manager.
2. Click **Client Distributions** in left column.



Manage Client Distributions

Distributions: [Create New Distribution] ▼

Server Address:

Distribution Name:

Description:

Create Delete

Figure 2 Client Software Distribution Window

3. From the pull-down menu in the **Distributions** field, select "Create New Distribution."

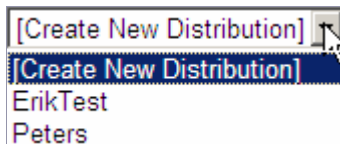


Figure 3 Client Distribution List

4. Enter the IP or DNS host name of the server in the **Server Address** field.

5. Enter a name and description for the distribution and click **Create**; after the distribution has been created, new links will appear, as shown at the bottom of Figure 4.

Manage Client Distributions

Distributions:

Server Address:

Distribution Name:

Description:

Use the links below to download the selected distribution. The .exe will install the software

http://10.13.1.42/ClientDistributions/SampleClientDistribution_1405.cab

http://10.13.1.42/ClientDistributions/SampleClientDistribution_1405.exe

Figure 4 New Client Distribution File

Configuring a Client Distribution

Prior to distributing the client distribution file, the administrator may wish to modify the default configuration for specific user populations, applications, or networks, as discussed in Chapter 4. If the administrator distributes the client software before it is configured, and later configures it, the client will automatically update upon startup. For many installations, the default settings provide the appropriate configuration, and additional configuration may not be necessary.

Distributing a Client Distribution

1. Navigate to the WAAS Mobile Manager **Client Configuration > Client Distributions** page.
2. Select the desired client distribution from the **Distributions** drop-down menu.
3. Click on the “.cab” or “.exe” link at the bottom of the screen and save the distribution file.
 - The “.cab” file can be extracted to distribute client software to users with standard software distribution programs.
 - A link to the “.exe” file can be emailed to users for self-install.

Installing the Client Software

To install the client software “.exe” file:

1. Login to the client PC with administrator or power user privileges.
2. Begin the client install by clicking on the “.exe” file, then clicking **Run**.

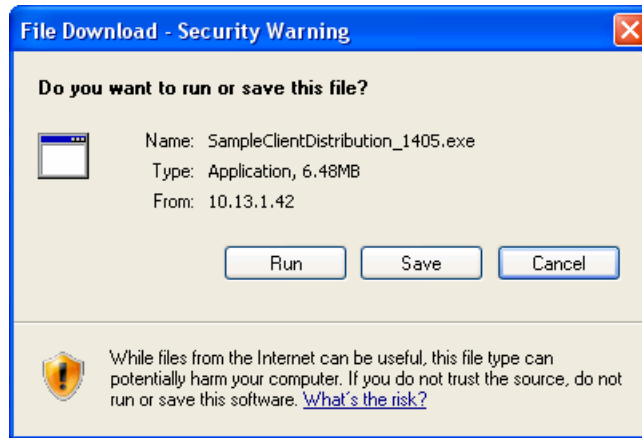


Figure 5 Client File Download

3. Follow the instructions in the Installation Wizard to continue the installation and accept the license agreement. When the installation is complete, click **Finish**.
4. You will be asked to restart the computer. Click **Yes**.
5. Upon restart, a software registration screen may appear. Registration information is transmitted only to the WAAS Mobile server to assist the administrator with managing the deployment, and is not transmitted externally. The administrator has the option to disable this registration (via the **Server Configuration > Authentication** screen), but without it, troubleshooting user issues may be more difficult.

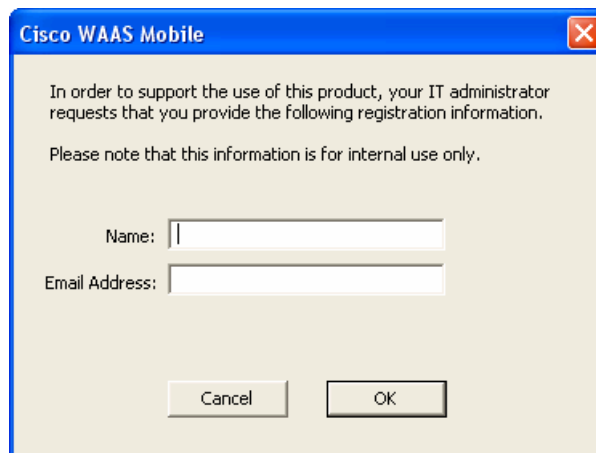


Figure 6 Client Registration

- 5.1. After registering, the client software will automatically start up and connect to the WAAS Mobile server.

Upgrading WAAS Mobile Client Software

There are three mechanisms for upgrading the WAAS Mobile client software:

- Component upgrades
- Manual installation using the self-installation program (.exe)
- Deployment with system management software (.cab)

Component Upgrades

The component upgrade feature enables WAAS Mobile clients to be automatically upgraded once the server has been upgraded. When the WAAS Mobile client connects to the server, it will detect that a new software version is available and automatically download and install it. To use this deployment mechanism:

- Navigate to the WAAS Mobile Manager **Server Configuration > Advanced Settings > Upgrades** page, check the **Enable Component Upgrades** box, and then click **Submit**.

NOTE: Component upgrades are not supported for all software upgrades. In particular, if the upgrade includes a driver upgrade, the component upgrade mechanism may not be used. Refer to the appropriate **Release Notes** for each software version for information about component upgrade support.

Manual Installation using the Self-Installation Program

WAAS Mobile client software may also be upgraded using a self-installation program (.exe) file. Upon installation, the previous client software version will be uninstalled automatically and the new version will be installed. To use this deployment mechanism:

- Users must have power user or administrative privileges.
- A link to the “.exe” program must be provided to the users. Navigate to the WAAS Mobile Manager **Client Configuration > Client Distributions** page and select the desired distribution from the drop-down menu. A link to the “.exe” will be displayed and this link may be cut and pasted into an email.
- Users should follow the procedure defined in “*Installing the Client Software*” above.

Deployment with System Management Software

The WAAS Mobile client may also be upgraded using standard enterprise software distribution and management programs such as Microsoft SMS. To use this deployment mechanism:

- Retrieve the “.cab” file for each client distribution. Navigate to the WAAS Mobile Manager **Client Configuration > Client Distributions** page and select the desired distribution from the drop-down menu. A link to the “.cab” file will be displayed. This “.cab” file contains the “.msi” and associated files.
- Follow standard procedures for your software distribution software program.

Chapter 4 Configuring the Cisco WAAS Mobile Client

To create and configure client distributions, go to the WAAS Mobile Manager **Client Configuration** section.

NOTE: You will not be able to navigate to the other pages in Client Configuration until a distribution has been created.

Several configuration settings pages are reviewed in this section, including:

- *Diagnostics*. Configure diagnostic features for the client.
- *User Interface*. Configure the client interface preferences.
- *Connection Settings*. Configure high speed bypass, persistent connections, traffic encryption, and bandwidth limits for users.
- *HTTP/HTTPS Settings*. Configure HTTPS acceleration and select HTTP and HTTPS ports that will be accelerated. Also, configure certain compressed file types to bypass acceleration.
- *Exclusion Lists*. Configure clients to ignore traffic to certain ports or traffic that is destined to certain IP addresses or hosts.
- *Accelerated Networks*. Configure either a white list of subnets to be accelerated or a black list of subnets to be bypassed.
- *Proxied Process List*. Configure applications to be accelerated.
- *File Shares*. Configure SMB CIFS acceleration.
- *Delta Cache Settings*. Configure clients' delta caches.

Client Distributions

This screen allows administrators to add, delete, and change properties for client distribution files. Refer to Figure 4 in Chapter 3 for screen shot.

Distributions	The pull-down contains the list of currently-defined client distributions, as well as a selection for creating a new distribution.
Server Address	The address of the server associated with the distribution.
Distribution Name	The name assigned to the distribution by the administrator.
Description	The description assigned to the distribution by the administrator.

Diagnostics

Diagnostics Distribution: SampleClientDistribution

Enable Large Client System Reports

Enable Network Monitoring

Change System Report Destination

System Report URL:
Enter "default" for System Reports to be sent to this server

Figure 7 Diagnostics Settings

Enable Large Client System Reports	Use this feature to create a system report that captures a longer time period of events than is captured by default. By default, large system reports are disabled as this will use more memory on the end user's machine.
Enable Network Monitoring	Checking this box enables network monitoring. By default network monitoring is disabled. The network monitoring feature should be enabled prior to generating a system report. See Chapter 9 for more information on system reports.
Change System Report Destination	Checking this box posts system reports to destinations other than the default location, which is %ALLUSERSPROFILE%\Application Data\Cisco\WAASMobile\Inbox on the WAAS Mobile server to which the administrator is connected.

User Interface

User Interface Settings Distribution: SampleClientDistribution

Use Simplified User Interface (tray icon with Exit option only)

Use UTC time in Connection Monitor

Enable Advanced Tab

Disable User Generated System Reports

Apply Changes Restore Defaults

Figure 8 Client User Interface Settings

Use Simplified User Interface	If this box is checked, the client user interface is simplified to just a tray icon with an Exit option. The Client Manager is not displayed and the user may not generate system reports.
Use UTC time in Connection Monitor	Displays UTC (Universal Time, Coordinated) time in the Connection Monitor. By default, GMT (Greenwich Mean Time) is displayed.
Enable Advanced Tab	Enables the Advanced tab in the Client Manager, which provides the user with the ability to control select configuration settings. By default, the Advanced tab is not displayed.
Disable User Generated System Reports	Disables the user from generating system reports. By default, system report generation is enabled. Disabling system reports removes this option from the icon menu and from the Support tab of the Client Manager.

Connection Settings

Connection Settings Distribution: SampleClientDistribution

Enable Latency-Based Bypass

Threshold (msec):

Enable High Speed Bypass

Download Bandwidth Threshold (kbps, Max: 972.8)

Upload Bandwidth Threshold (kbps, Max: 972.8)

Round Trip Time Threshold (ms)

Determine connection speed every time Cisco WAAS Mobile connects

Enable Persistent Connections

Disable Traffic Encryption

Enable Bandwidth Limits

Maximum Bandwidth: (in kbps)

Figure 9 Connection Settings

Please review the *Cisco WAAS Mobile Network Design Guide* for guidance on how to configure WAAS Mobile clients given various WAAS Mobile server deployment topologies.

Enable Latency-Based Bypass

Latency-Based Bypass is used to accelerate individual TCP connections if the latency of the network between the client machine and the destination content server exceeds the threshold value. Use this setting for mobile workers that access a combination of local and remote servers. By default, latency-based bypass is disabled.

NOTE: The client will still connect to the WAAS Mobile server when this feature is enabled. Once WAAS Mobile has performed a latency check to a specific content server, it will either bypass or accelerate that connection for the remainder of the session.

Enable High Speed Bypass	High Speed Bypass disables acceleration when a high speed connection to the WAAS Mobile server is detected. Use this setting for workers that are not always located where WAAS Mobile Manager is installed. By default, high-speed bypass is disabled. If checked, high-speed connections as determined by threshold settings discussed below will take effect.
--------------------------	--

NOTE: When High Speed Bypass is enabled, the WAAS Mobile client will not connect to the WAAS Mobile server when a high speed connection is detected.

Threshold Settings	The three threshold values are: <ul style="list-style-type: none">▪ Download Bandwidth Threshold▪ Upload Bandwidth Threshold▪ Round-Trip Time (RTT) Threshold If both the download bandwidth threshold and upload bandwidth threshold are exceeded, and the latency is below the RTT threshold, then the connection will be classified as high-speed.
--------------------	---

Determine connection speed every time Cisco WAAS Mobile connects	If checked, WAAS Mobile will perform a test of the network (bandwidth and round trip time) every time it establishes a new session with the server -- typically this is every time a new Windows network connection becomes active. If unchecked, the previously measured network characteristics (stored in the registry) will be used to determine whether or not a connection should be considered "high-speed."
--	---

NOTE: It is recommended that this checkbox remain unchecked unless WAAS Mobile is being deployed on a machine using a network interface or modem that dynamically switches between very high-speed (LAN-like speeds) and high-latency or narrowband connections.

Enable Persistent Connections

Persistent connections are disabled by default, and should be enabled for highly mobile workers. Persistent Connections insulates the end-user from problems with RF coverage in wireless networks as well as from problems in poor quality dial-up access. It allows the acceleration system to support advanced wireless network features such as automated Wi-Fi/cellular switchover or hand-offs when roaming through different cellular networks.

When persistent connections are enabled and communications are disrupted, the WAAS Mobile client will maintain an active session with the application process on the client. Similarly, the WAAS Mobile server will maintain an active session with the application server, keeping the TCP connections alive. Note that the persistent connections feature is not currently supported for SMB CIFS traffic.

In some deployments, clients may not have the same IP when they reconnect or when they roam to a different network. The WAAS Mobile server will recognize the client even if the IP presented to the server has changed. In addition, for deployments of multiple acceleration servers, the WAAS Mobile client-side load balancing feature can be used to ensure that the client will reconnect successfully.

Many web browsers, email clients, and application servers will terminate a session if they detect an inactive connection. During the time that the client-proxy link is unusable, WAAS Mobile keeps the TCP connections to the client and server applications open for a predetermined period of time. It also sends application layer messages for HTTP and email that prevent shutdown of the application session before service is restored. Other applications will time-out according to their tolerated interval of inactivity.

With Persistent Connections, the server always assumes that the most recent session from a client is still active. The server closes a session when one of 3 events occurs:

- The server receives a restart message from the client.
- A request for a new session is received from a client who has an existing session.
- A session remains inactive for an interval longer than a threshold defined in the registry (currently set to 1 hour).

The client closes a session when one of 3 events occurs:

- The client receives a restart message from the server.
 - A session remains inactive for an interval longer than a threshold defined in the registry (currently set to 1 hour).
 - When a network connection is present but the client has not received any data from the server after a pre-defined time period (20 minutes, by default).
-

Disable Traffic Encryption

Traffic encryption is enabled by default. Users who are accessing the network via SSL or IPsec VPN clients may not require the additional layer of encryption provided by WAAS Mobile, so this feature should be disabled for those users.

NOTE: If HTTPS acceleration has been enabled, it is recommended that link encryption be enabled to ensure that the traffic is encrypted at all points between the client and the application server.

Enable Bandwidth Limits

By default, WAAS Mobile does not impose a bandwidth limit on the client. In some multi-user, small office cases, it may be desirable to limit the amount of bandwidth that any single user can use.

HTTP / HTTPS Settings

HTTPS Settings Distribution:

Enable HTTPS Acceleration

Accelerate All HTTPS Sites

Accelerate Host Inclusion List Only

Disable Vista/IE7 Certificate Revocation List

Host Inclusion List

Host Name:

IP Address:

Process Acceleration List

Process Name:

iexplore.exe
explorer.exe

HTTPS Port Inclusion List

Example: 443,444

HTTP Settings

HTTP Port Inclusion List

Example: 80,8080,8081

Bypass Settings

Enable HTTP Bypass

Bypass Audio and Video Files with these extensions:

Bypass Miscellaneous Files with these extensions:

Figure 10 HTTP and HTTPS Settings

Enable HTTPS Acceleration

By default, HTTPS traffic is not accelerated. When HTTPS acceleration is enabled, acceleration is provided for web traffic that uses Microsoft Internet Explorer or that uses the Microsoft API. Browsers such as FireFox can also be supported, but require a workaround to install the WAAS Mobile server as the trusted store. When enabling HTTPS acceleration, it is recommended that HTTPS delta caching also be enabled. To enable HTTPS delta caching, navigate to the **Client Configuration > Delta Cache Settings** screen.

NOTE: When HTTPS acceleration is enabled, **Traffic Encryption** should be enabled on the **Client Configuration > Connection Settings** screen.

Accelerate All HTTPS Sites

All HTTPS traffic will be accelerated if this radio button is selected.

Accelerate Host Inclusion List Only

HTTPS acceleration can be restricted to accelerate intranet sites only by selecting the **Accelerate Host Inclusion List Only** and adding the IP addresses of select HTTPS servers to the list. Only hosts listed in the Host Inclusion List will be accelerated.

- Use **Add**, **Remove**, and **Remove All** to create the list.
- Click **Apply Changes** to save the changes.
- Use **Restore Defaults** to return to the default settings.

NOTE: Although host name and IP address fields are provided, only the destination IP address is used; the host name is for descriptive purposes only.

For more information on HTTPS Optimization, see the *Cisco WAAS Mobile Integration Guide*.

Disable Vista/IE7 Certificate Revocation List

When an HTTPS site is accessed on Windows Vista machines, IE7 tries to check the certificate revocation list (CRL) that belongs to the certificate issuer to determine if the certificate was revoked and to verify the certificate itself. This is done by OCSP protocol through series of online HTTP requests to the issuer.

To facilitate testing WAAS Mobile in a pre-production environment, a “dummy” Root CA ships with the product. To test with this CA, it is necessary to disable Vista/IE7 certificate revocation list checking.

NOTE: To test HTTPS performance in a lab environment with Vista clients, disable Vista/IE7 Certificate Revocation List checking. If this setting is not disabled, HTTPS performance may be unacceptably slow.

When deploying WAAS Mobile in a production environment it is recommended that a subordinate CA generated off of the enterprise CA be installed, and that Vista/IE7 Certificate Revocation List checking be enabled. This setting is enabled by default.

Process Acceleration List	By default, when HTTPS acceleration is enabled, Internet Explorer and Windows Explorer HTTPS traffic is accelerated. To accelerate other applications that communicate via HTTPS and that use the Microsoft Windows Socket APIs, the process names of these applications must be added to the Proxied Process List on the Client Configuration > Proxied Process List page. Once the processes are added, they can be enabled for HTTPS acceleration by using the drop-down menu on this page.
HTTPS Port Inclusion List	By default, only HTTPS traffic on port 443 is accelerated. To accelerate HTTPS traffic on other ports, add them to this list. Port numbers should be separated by commas with no spaces.
HTTP Port Inclusion List	By default, only HTTP traffic on ports 80 and 8080 are accelerated. To accelerate HTTP traffic on other ports, add them to this list. Port numbers should be separated by commas with no spaces.
Enable HTTP Bypass	To specify that certain file types are not to be proxied, but are instead to be downloaded directly from the original destination server, check the Enable HTTP Bypass box then add the file types in the text boxes that appear. Administrators who want to eliminate music and video downloads (or other file types) from being accelerated and from taking up space in the delta cache should use this feature.
Bypass Audio and Video Files	List the extensions of the audio and video file types to be bypassed here. If enabled, by default, the following file types will be bypassed: asf, au, avi, midi, mov, mp2, mp3, mpeg, mpg, qt, ra, vdo, vqf, vox, wav, wma, wmv, rm, rv, mvb, aac, m4a, m4u, m4p, ogg, flac, ape, ogm, mkv.
Bypass Miscellaneous Files	List the extensions of any other file types to be bypassed here. If enabled, the following additional file types will be bypassed: exe, zip, msn, vpg, gz, cab, rar, msi, 7z, ace, arj, lzh, tar, Z, jar, arc, bz2.

Exclusion Lists

The Exclusion List Settings allow administrators to specify destination ports and IP addresses which should be bypassed. For each feature, use the **Add**, **Remove**, and **Remove All** buttons to create the list, and then click **Apply Changes** to save or **Restore Defaults** to return to the default settings.

Exclusion Lists Settings Distribution:

Port Exclusion List

Port:

IP Exclusion List

IP Address:

Figure 11 Exclusion Lists Settings

Port Exclusion List	TCP connections bound for ports on the exclusion list will completely bypass the client software. These connections will not be proxied or accelerated.
IP Exclusion List	TCP connections bound for IP addresses on the IP exclusion list will completely bypass the client software. These connections will not be proxied or accelerated.

Accelerated Networks

The Accelerated Networks table defines which destination networks should be accelerated and which should be bypassed. Each entry in the table includes a network IP and a subnet mask; entries are read prior to establishing a server session when checked; the feature is disabled by default. If enabled, use the **Add**, **Remove**, and **Remove All** buttons to create the list, and then click **Apply Changes** to save or **Restore Defaults** to return to the default settings.

Accelerated Networks Distribution: **SampleClientDistribution** ▼

Enable Network Traffic Control

Accelerate Network Table Entries

Bypass Network Table Entries

IP:

Mask:

Figure 12 Accelerated Networks

Enable Network Traffic Control	Enabling this capability allows administrators to specifically include or exclude destination subnets that should be accelerated.
Accelerate Network Table Entries	When Accelerate Network Table Entries is selected, a TCP connection with a destination address matching an entry in the table will be accelerated. If a matching entry does not exist, the connection will be bypassed.
Bypass Network Table Entries	If Bypass Network Table Entries is selected then a TCP connection with a destination address matching an entry in the routing table will be bypassed, and will not be accelerated.
IP	Enter an IP address for the routing table.
Mask	Enter a network mask in dotted-decimal form to identify the subnet.

Proxied Process List

The Proxied Process List is used to determine which applications are to be accelerated. For each process, complete the field entries, and then click the **Add Process** and the **Apply Changes** buttons. You must click both buttons in order for the entries to appear in the process list.

Proxied Process List
Distribution: SampleClientDistribution ▼

Process Name:
example: iexplore.exe

Min Version: *
*Enter * for no minimum version*

Max Version: *
*Enter * for no maximum version*

Command Line: *
*Enter * for any command line*

Acceleration Type: 0 - Normal Acceleration ▼

Application Name:
(optional) Complete Application Name

Auto Reset Connection: Yes No
Select Yes to automatically reset connections for this process

Add Process
Remove Selected Processes
Restore Defaults
Apply Changes

Select	Process Name	Min Version	Max Version	Command Line	Acceleration Type	Application Name	Auto Reset Connection
<input type="checkbox"/>	explorer.exe	5.0	6.0	*	0	Windows Explorer	
<input type="checkbox"/>	Opera.exe	5.0	*	*	0	Opera Browser	
<input type="checkbox"/>	iexplore.exe	5	*	*	0	Internet Explorer	X
<input type="checkbox"/>	msimn.exe	5.0	6.0	*	0	Outlook Express	
<input type="checkbox"/>	netscape.exe	4.7	5.0	*	0	Netscape Browser	
<input type="checkbox"/>	eudora.exe	4.3	5.2	*	0	Eudora Mail Client	

Figure 13 Proxied Process List

Process Name	Enter the name of the process to be proxied.
Min Version	Enter the minimum version of the process.
Max Version	Enter the maximum version of the process.

Command line	Use this field to specify command line options that are applicable to the specified process. For example, to enable acceleration of Microsoft WebDAV, the svchost.exe process with the “-k LocalService” command option must be specified.
Acceleration Type	<p>There are five selections to choose from the pull-down menu:</p> <ul style="list-style-type: none"> 0 - Normal Acceleration 1 - Generic Acceleration 2 - VoIP (RTP) Monitoring Only 3 - Normal Acceleration with VoIP (RTP) Monitoring 4 - Generic Acceleration with VoIP (RTP) Monitoring <p><u>Normal Acceleration</u> includes application protocol optimizations, differencing and compression, and transport optimizations.</p> <p><u>Generic acceleration</u> includes differencing and compression and transport optimizations.</p> <p><u>VoIP Modes</u></p> <p>VoIP modes enable soft phones to interoperate with WAAS Mobile by reserving bandwidth for voice calls. This function works as follows:</p> <ul style="list-style-type: none"> ▪ Link bandwidth is continuously measured. ▪ When voice/video traffic associated with the identified process is present, bandwidth is reserved. ▪ The amount of bandwidth that is reserved is as follows: <ul style="list-style-type: none"> ○ If the link is <56 kbps, 85% of the link is reserved. ○ If the link is between 56 kbps and 240 kbps, 48 kbps is reserved. ○ If the link is > 240 kbps, 20% of the link is reserved. ▪ When the voice/video traffic stops, the bandwidth reservation ends. ▪ <u>VoIP (RTP) Monitoring Only</u> provides bandwidth reservation for the UDP traffic of the accelerated process. ▪ <u>Normal Acceleration with VoIP</u> will accelerate all TCP connections from the process while providing bandwidth reservation for the UDP traffic. ▪ <u>Generic Acceleration with VoIP</u> will provide generic acceleration for all TCP connections from the process while providing bandwidth reservation for the UDP traffic. <p>NOTE: VoIP UDP traffic is not placed into the ITP connection and is not destined for the WAAS Mobile server.</p>
Application Name	Enter the complete name of the process to be proxied (optional).

Auto Reset Connection	Acceleration of certain applications does not begin immediately if Cisco WAAS Mobile is started or restarted after the application has established TCP connections. If the Auto Reset Connection is enabled for a given application, – by selecting the radio button, and indicated by an “X” in the Auto Reset Connection field – then when WAAS Mobile starts, it will terminate the TCP connection(s) for that application so that when the application reconnects, it is accelerated. Auto Reset Connection is typically enabled when optimizing dynamic web applications (e.g., SharePoint).
-----------------------	---

File Shares

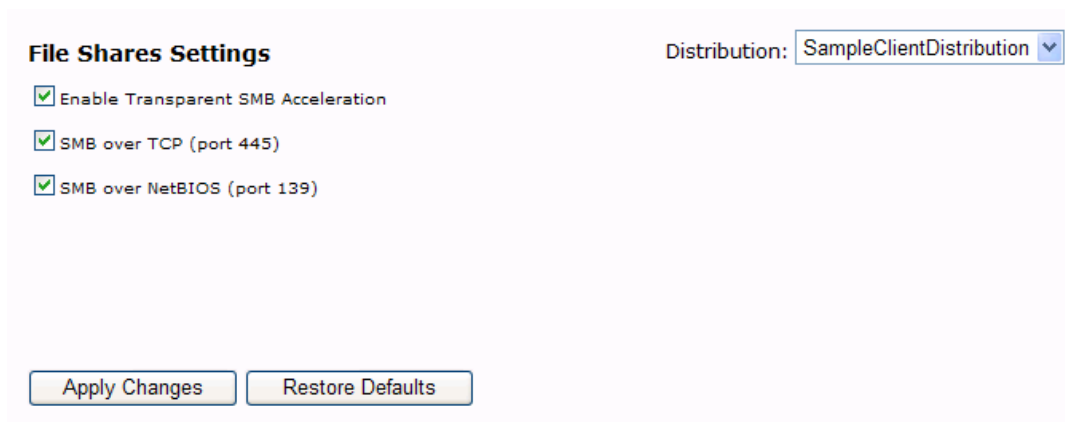


Figure 14 File Shares Settings

Enable Transparent SMB Acceleration	This checkbox enables acceleration of CIFS file share traffic.
SMB over TCP	Enable SMB over TCP when accelerating file shares running Windows 2000 or later.
SMB over NetBIOS	Enable SMB over NetBIOS when accelerating file shares running Windows NT or later.

Delta Cache Settings

Delta Cache Settings Distribution:

Desired Delta Cache Size: MB

Maximum Delta Cache Size: MB
Client delta cache size may not exceed this value.

Reduced Size Enabled:

Reduced Delta Cache Size: MB
Size if desired size does not fit.

Delta Cache Location:
Paths can include Windows environment variables. For instance, %USERPROFILE%, %Temp%, ...

HTTPS Caching:

Encryption:

Figure 15 Delta Cache Settings

Desired Delta Cache Size	Enter the desired client delta cache size. The default is 1024 MB. The client delta cache size must be smaller than the server delta cache.
Maximum Delta Cache Size	If the Advanced tab is enabled in the client configuration, users can change the size of their delta cache. Administrators can use this setting to control the maximum size of the user's delta cache.
Reduced Size Enabled	If there is insufficient disk space and the client is unable to create the desired delta cache size, it will, if this option is checked, attempt to create a reduced size delta cache.
Reduced Delta Cache Size	The fallback delta cache size is 256 MB by default, and may be modified by the administrator.
Delta Cache Location	Used to specify the delta cache location, if other than the default. By default, the delta cache is placed in the All Users area.
HTTPS Caching	Enables caching of data received via HTTPS. This feature should be enabled when HTTPS acceleration is enabled. To enable HTTPS acceleration, navigate to the Client Configuration > HTTP/HTTPS Settings screen. This feature is enabled by default.

Encryption

Enables encryption of cached data on the clients' PCs. It is disabled by default.

This capability is only available in Windows XP Professional, Windows Vista Business and Windows Vista Ultimate editions. (Not supported for XP Home, Vista Starter, Windows Vista Home Basic, Windows Vista Home Premium, and Windows CE editions).

This capability is only supported when the delta cache is built on NTFS.

Supports FIPS-140 evaluated cryptographic providers, and default encryption for XP SP2 and later is AES-256.

Chapter 5 Configuring the Cisco WAAS Mobile Server

This chapter addresses configurable features in the WAAS Mobile Manager **Server Configuration** area.

- *Licensing.* Enter license keys and view license information.
- *Authentication.* Configure user authentication options.
- *Logging.* Configure system logging options.
- *Server Farm.* Configure WAAS Mobile server farms.
- *Advanced Settings.* Configure advanced acceleration and diagnostic capabilities.
- *Import/Export.* Import and export configuration databases.

IMPORTANT: All server configuration changes require a restart of the server. This can be done by clicking **Restart Server** on the WAAS Mobile Manager **Home > Status** page.

Licensing

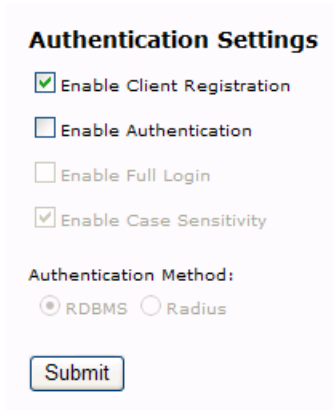
The WAAS Mobile Manager **Licensing** page allows administrators to enter and/or change the WAAS Mobile license key(s) and provides additional information about license entitlements, including number of users supported by the license. Refer to Chapter 3 for instructions on entering the license key.

Once the maximum number of users supported by the license is reached, no new user connections will be accepted, and those users will not be accelerated. To monitor license usage, navigate to the WAAS Mobile Manager Home **Monitoring > Sessions** page to view graphs of user session activity.

IMPORTANT: Changes to the license require a restart of the server. This can be done by clicking **Restart Server** on the WAAS Mobile Manager **Home > Status** page.

Authentication

Please review the *Cisco WAAS Mobile Integration Guide* for supplemental information on using and configuring the various supported authentication mechanisms.



Authentication Settings

Enable Client Registration

Enable Authentication

Enable Full Login

Enable Case Sensitivity

Authentication Method:

RDBMS Radius

Submit

Figure 16 Authentication Settings

Enable Client Registration	Client registration, which is enabled by default, associates a user name with the WAAS Mobile client. This enables administrators to correlate session monitoring data with users, which is helpful when troubleshooting user problems.
Enables Authentication	If checked, enables the Authentication.
Enable Full Login	If authentication is enabled, the default login requirement is a username only. To enable username/password login, check this box.
Enable Case Sensitivity	If checked, authentication and login are both case sensitive.
Authentication Method	Select either local RDBMS or RADIUS authentication. Refer to the <i>Cisco WAAS Mobile Integration Guide</i> for detailed information on configuring and using RADIUS.

User Management

The screenshot shows a web interface titled "User Management". It contains the following elements:

- Two input fields: "UserName:" and "Password:".
- Four buttons: "Add User", "Update Selected User", "Delete Selected User", and "Delete All".
- A label "Select a User:" above a large empty rectangular box.
- A section titled "Export User List" with an "Export User List" button.
- A section titled "Import/Export User List" with an empty input field and a "Browse..." button.
- An "Import User List" button.

Figure 17 User Management Screen

When user authentication is enabled and the administrator has selected the local RDBMS database option, the user authentication data may be entered, imported, and exported via this screen. See the *Cisco WAAS Mobile Integration Guide* for additional information on configuring and using user authentication.

UserName	Enter name of user.
Password	Enter user's password.
Export User List	Exports the current User List.
Import User List	Imports an already-created User List.

RDBMS Authentication

RDBMS Authentication Settings

Database Type:

MySQL MSSQL SQLite

DSN Name:

Users Table Name:

Figure 18 RDBMS Authentication Settings

Database Type	The default is SQLite, which uses an internal SQLite database. Select MySQL or MSSQL (for Microsoft SQL Server) if an alternate external database is to be used.
DSN Name	When a non-default database has been selected, enter the host name of its server as the Data Source Name (DSN). NOTE: If using one of the alternate back-end databases, make sure the ODBC DSN is a System DSN and that the database name has been created in the chosen SQL database beforehand.
Users Table Name	Enter the name of the table used to authenticate users.
Test Connection	Click this button to verify that the database management system is accessible to WAAS Mobile Manager.

Radius Authentication

Refer to the *Cisco WAAS Mobile Integration Guide* for detailed information on configuring and using RADIUS.

Radius Authentication Settings

Use Nas Identifier Value:

Use Nas IP Address Value:

Include Account Session Id

Acct-Session-Id Separator:

Enable Framed IP Address

Include Nas-Port Attribute

Nas-Port Value:

Nas-Port Type:

Include Service-Type Attribute

Service-Type:

Use Radius Attribute to Filter Access

Filter Attribute Value:

Server Count:

Radius Server Settings

Server1

Remote Address:

Port:

Shared Secret:

Request Retry Count:

Request Time Out:

Figure 19 Radius Authentication Settings

Use Nas Identifier Value	Enter Network access server (Nas) Identifier.
Use Nas IP Address Value	Enter Nas IP Address. if applicable.
Include Account Session ID	If checked, also enter Acct-Session-Id separator.
Enable Framed IP Address	If checked, enables framed IP addressing.
Include Nas-Port Attribute	If checked, allows inclusion of Nas-Port attributes. Enter the Nas-Port value and type in the appropriate fields.
Include Service-Type Attribute	If checked, enter value in the Service-Type field.
Use Radius Attribute to Filter Access	If checked, uses Radius Attribute to filter access to the server. Enter Filter Attribute value and the number of servers in the appropriate fields.
Radius Server Settings	From the pull-down menu, select the desired server.
Remote Address	Enter the remote address, if known.
Port	Enter the port number.
Shared Secret	Enter the secret code.
Request Retry Count	Enter the number of retries.
Request Time Out	Enter the length of time before server requests stop.

Logging

Logging Settings

Logging Settings

Log File Name:

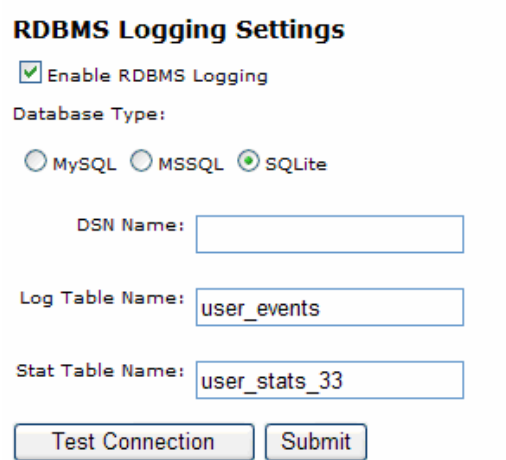
Log File Directory:

Basic Log Mode Disable Logging
 Debug Log Mode URL Only Logging

Figure 20 Logging Settings

Log File Name	Enter the log file name to be used if logging is enabled (see below).
Log File Directory	Enter the directory for the log file.
Basic Log Mode	Select this radio button to enable minimal logging.
Disable Logging	Select this radio button to disable logging. This is the default setting.
Debug Log Mode	Select this radio button to enable verbose logging. Do not enable this option in an active production environment.
URL Only Logging	Select this radio button to log only the URLs visited.

RDBMS Logging



RDBMS Logging Settings

Enable RDBMS Logging

Database Type:

MySQL MSSQL SQLite

DSN Name:

Log Table Name:

Stat Table Name:

Figure 21 RDBMS Logging Settings

Enable RDBMS Logging	Check this box to enable local logging to the RDBMS.
Database Type	The default is SQLite, which uses an internal SQLite database. Select MySQL or MSSQL (for Microsoft SQL Server) if an alternate external database is to be used.
DSN Name	When a non-default database has been selected, enter the host name of its server. NOTE: If using one of the alternate back-end databases, make sure the ODBC DSN is a System DSN and that the database name has been created in the chosen SQL database beforehand.
Log Table Name	Enter the name of the table used to store logged events.
Stat Table Name	Enter the name of the table used to store statistics for each client
Test Connection	Click this button to verify that the database management system is accessible to WAAS Mobile Manager.

Log Rotation

Log Rotation Settings

Enable Log Rotation

Daily

Weekly

Monthly

When Size Equals:

MB (Min 20-Max 500)

Number of Archived Log Files To Keep (Per Type)

Figure 22 Log Rotation Settings

Enable Log Rotation	Check this box to enable log rotation.
Daily/Weekly/Monthly	Select to rotate the logs once each day/week/month.
When File Size Equals	Select to rotate the logs when the size of the active log file reaches the value specified.
Number of Archived Log Files To Keep (Per Type)	Used to specify the number of archived log files to keep per log file type.

Server Farm

Cisco WAAS Mobile's advanced server selection capabilities allow the client making an informed decision on which server to connect to in the enterprise. This feature can be used to provide load balancing and high availability for a single server farm deployed in the enterprise data center or for the more complex scenario where an enterprise has deployed multiple WAAS Mobile server farms in more than one geographic location. In this case, the client must first determine which farm to connect to (farm selection) and second which server in that farm to connect to (server selection). The end result is a dynamic solution that is flexible and adaptable to any enterprise network infrastructure.

NOTE: Prior to configuring server farms, please also review the *Cisco WAAS Mobile Network Design Guide* for best practices in deploying WAAS Mobile servers in large scale enterprises.

A server may be configured as the Cisco WAAS Mobile controller server, a worker server, or both. A controller server is configured with a mapping table defining the server farm(s), containing one or more WAAS Mobile worker servers. This mapping table provides clients with dynamic instructions on how to select the appropriate farm and server within that farm regardless of where they connect to the enterprise WAN. Upon startup and periodically thereafter, the controller server will communicate the current mapping table to each worker server across all server farms. Each server will then communicate this information back to each client that is connected to it. The client will use a best effort approach to use the same worker server on the next login attempt in order to reap the benefits of persistent sessions and/or persistent delta cache.

Server Farm

Server List

Server
IP/HostName:

Farm Name:
(Optional)

Enter servers that you wish to add to your server list. Enter a farm name if you wish to configure multiple server farms.

Add Server

Remove Server

Update Server

Figure 23 Server Farm Settings

Server IP/HostName	DNS or IP address of the worker server. When servers are added to the controller server's server farm, the IP or Hostname of the controller server must be added via this screen.
Farm Name (Optional)	Enter Farm Name.

Single Server Farm Deployment

If the deployment has only one server farm, enter the **IP/Hostname** of each server to be in the farm into that field and click **Add Server**. The **Farm Name** field should be left blank, as this single farm will be treated as the default farm which simplifies configuration for the administrator by bypassing any farm selection settings since they are not applicable.

NOTE: The controller server's initial self-configuration as a worker server for clients to connect to becomes undone once a server is entered in the server farm. If the controller server is to remain a worker server in the configuration, it must be added to its own server list.

Server Farm
Server List

Server IP/HostName:

Farm Name:
(Optional)

Enter servers that you wish to add to your server list. Enter a farm name if you wish to configure multiple server farms.

Select	Server IP/HostName
<input type="checkbox"/>	10.13.1.21
<input type="checkbox"/>	10.13.4.20
<input type="checkbox"/>	10.13.4.29

Figure 24 Configure Single Server farm

Multiple Server Farm Deployment

Multiple server farms are created by entering the **IP/Hostname** of each server and entering a farm name in the **Farm Name** field (farm2 and farm3 in the below example; Default Farm will also function as a farm in this configuration).

Server Farm
Server List

Server IP/HostName:

Farm Name:
(Optional)

Enter servers that you wish to add to your server list. Enter a farm name if you wish to configure multiple server farms.

Select	Server IP/HostName	Farm Name
<input type="checkbox"/>	10.13.1.21	Default Farm
<input type="checkbox"/>	10.13.4.20	Default Farm
<input type="checkbox"/>	10.13.4.29	farm2
<input type="checkbox"/>	10.13.0.1	farm2
<input type="checkbox"/>	10.13.0.2	farm3
<input type="checkbox"/>	10.13.0.3	farm3

Figure 25 Configure Multiple Server Farms

Entering a farm name automatically disables the simpler default farm configuration used for a single farm deployment and necessitates **Server Selection Method** and **Farm Selection Method** configuration on the **Server Farm > Server Selection** page.

Server and Farm Selection

When using **Advanced Server Selection** capabilities, the controller server communicates all server selection settings to all other servers in its server farm.

IMPORTANT: All configuration changes to Server Selection require a server restart.

Server Selection

Enable Advanced Server Selection

This Server is the Controller Server

Server Selection Method

Random Selection

Prioritized Selection

Farm Selection Method

Client IP Map

Latency

Client IP Map

Client IP:

Subnet Mask:

Farm Name:

Enabled

There are no mappings in the Server Map

Figure 26 Server Selection and Farm Selection Methods

Server Selection Method

Enable Advanced Server Selection	Check the box to enable configuration of all server farm selection settings. The default setting is disabled.
This Server is the Controller Server	Check the box to identify the current WAAS Mobile server as the controller server.
Random Selection	With this setting, the client will attempt to connect to the server to which it was previously connected. If unable, it will randomly select another server in the farm from the list of server IPs (if more than one exists or if the DNS name resolves to more than one IP) and will continue in this fashion until all choices are exhausted.

NOTE: Random server selection will result the best overall delta compression and load balancing performance.

Prioritized Selection	With this selection, the client connects to the first server listed in the server farm and, if not available, tries the other servers in the farm in the order listed.
-----------------------	--

Farm Selection Method

The Farm Selection Method settings apply only in a deployment with multiple server farms. Once the client has selected the farm it is to connect to, the server within that farm is chosen based on the Server Selection Method.

Client IP Map	With this selection, the client chooses a server farm based on administrator-defined mappings. Click Submit after selecting the radio button.
---------------	--

Latency	With this setting, the client performs a latency test by PINGing all servers in the controller server's server list, and then chooses the server farm with the least latency. The Client IP Map is grayed out when this selection is enabled. Click Submit after selecting the radio button.
---------	---

Client IP Map settings	Enter a Client IP address and subnet mask, then select from the pull-down list to specify the target server farm. Check the Enabled box if this mapping is to be enabled, and click Add Mapping (a "1" in the Enabled field indicates that the mapping is enabled). In the example below, any client with IP 10.13.1.x connects to the server farm named farm2 and any client with IP 10.13.4.x connects to farm3.
------------------------	---

Client IP Map

Client IP:

Subnet Mask:

Farm Name:

Enabled

Select	Client IP	Subnet Mask	Farm Name	Enabled
<input type="checkbox"/>	10.13.1.0	255.255.255.0	farm2	1
<input type="checkbox"/>	10.13.4.0	255.255.255.0	farm3	1

For mapping changes, select the checkbox next to the mapping; make the desired changes, then select **Update Mapping**.

To remove a mapping, select the checkbox next to the mapping and click **Remove Mapping**.

Advanced Settings

This section addresses the following:

- *Prefetching*. Configures various HTTP prefetching parameters. HTTP prefetching is an acceleration technique that improves web application and web browsing performance.
- *Delta Cache*. Configures delta cache settings.
- *Radius Accounting*. Configures RADIUS for use in user authentication and accounting.
- *Aliasing*. This feature maps client IP address pools to alias addresses.
- *Access Control*. Configures which client IP address ranges will be accelerated.
- *Upgrades*. Enables component upgrades and downgrades.
- *System Reports*. Configures system report parameters and associated alerts.

HTTP Prefetching

HTTP Prefetching Settings

Disable Prefetching

Prefetch Extension Bypass List:

Prefetch Hostname Bypass List:

Disable Prefetching with Cookies

Prefetch with Cookies for Private IP Addresses Only

Prefetch Cookie List:

Prefetch With Cookies Host List:

Figure 27 HTTP Prefetching Settings

Disable Prefetching	By default, HTTP prefetching is enabled. Check the box to disable it. HTTP prefetching is a server-side acceleration technique that models browser-to-web server behavior to predict and actively pre-fetch web objects prior to being requested.
Prefetch Extension Bypass List	Provide a comma-separated list to prevent prefetching specific file types from all hosts. By default, the following file types are not prefetched: php, php3, php4, cgi, pl, asp, cfm, jsp, exe, dll, swe, aspx.
Prefetch Hostname Bypass List	Provide a comma-separated list to prevent prefetching from specific host names.
Disable Prefetching With Cookies	Check this box to prevent sending HTTP cookies along with prefetched requests. For general use, this capability should not be disabled.
Prefetch With Cookies For Private IP Addresses Only	Enables prefetching with cookies for private IP addresses only.
Prefetch Cookie List	Provide a semicolon-separated list of cookie names to restrict the cookie names that can be used along with prefetched requests.
Prefetch With Cookies Host List	Provide a semicolon-separated list of host names to restrict the list of hosts for which cookie-based prefetching is enabled. For general use, this list should be left empty to ensure all sites get prefetched with cookies.

Delta Cache

Delta Cache Settings

Stop the server to enable the following options.

Clear Delta Cache

Delta Cache Size: GB

Delta Cache Location:
Enter a full path

HTTPS Caching:

Encryption:

Submit

Figure 28 Delta Cache Settings

IMPORTANT: The WAAS Mobile server must be stopped before changing Delta Cache settings.

Clear Delta Cache	Deletes the server delta cache history.
Delta Cache Size	Enter the desired cache size. The default is set to 275 GB. The maximum delta cache size is 1 TB.
Delta Cache Location	Used to specify a delta cache location other than the default. By default, the Delta Cache is located in the All Users area.
HTTPS Caching	By default, HTTPS caching is enabled. HTTPS traffic will not be accelerated and populate the delta cache unless HTTPS Acceleration is also enabled on the Client Configuration > HTTP/HTTPS Settings page.
Encryption	By default, encryption is disabled on the WAAS Mobile server. When enabled, AES-256 encryption is employed to secure the delta cache.

Radius Accounting

Refer to the *Cisco WAAS Mobile Integration Guide* for details on radius accounting configuration and monitoring.

Radius Accounting Settings

Enable Radius Accounting

Enable Failed Login and Server Failure Accounting

IdMode: 0

Session Id Separator: @

Nas IP Address: 0.0.0.0

Service Type: 12

Nas Port Mode: 3

Nas Port Value: 0

Server1 ▼

Name: unknown

Port: 1813

Shared Secret:

Max Tries: 3

Submit

Figure 29 Radius Accounting Settings

Aliasing

IP Aliasing is a feature of WAAS Mobile that allows each user session to be seen by the destination application or content server as a mapped or aliased IP address. This can be accomplished by dynamically assigning a local IP address for each client from a pool of IP aliases or by defining a mapping algorithm that allows the server to determine which IP to present to the destination servers from a given client IP. Once the IP is assigned and created on the network interface, this “local proxy address” will be used for all subsequent communication to destination application servers.

NOTE: All changes in IP Aliasing configuration require a restart of the WAAS Mobile server.

Refer to the *Cisco WAAS Mobile Integration Guide* for details on client IP mapping schemes.

Aliasing Settings

Use IP Aliasing

Many To One IP Aliasing

Public Network Interface:

Valid Sources:

IpPool:

Many To One IP Aliasing

Client IP:

Subnet Mask:

Farm Name:

Enabled

Figure 30 Aliasing Settings

Access Control

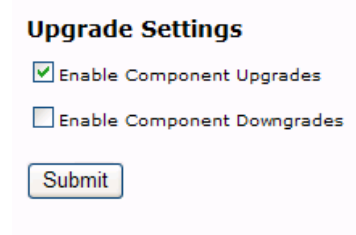
Access Control Settings support the deployment of WAAS Mobile in conjunction with WAAS WAE appliances. This feature should be used to support users who access applications and content via a combination of remote connections and fixed branch offices (e.g., laptop users). Access Control settings allow administrators to disable WAAS Mobile acceleration for subnets on which WAEs or other acceleration appliances have been deployed by including them in the “Deny List Access” so that they are not accelerated by WAAS Mobile.

The screenshot shows the 'Access Control Settings' configuration page. At the top, there is a checkbox for 'Enable Access Control List'. Below it are two radio buttons: 'Allow List Access' (which is selected) and 'Deny List Access'. There are two input fields for 'IP Address:' and 'Mask:'. Below these fields are three buttons: 'Add', 'Remove', and 'Remove All'. A large empty rectangular box is provided for listing subnets. At the bottom of the form is a 'Submit' button.

Figure 31 Access Control Settings

Enable Access Control List	Allows administrators to specify which client IP sub-networks should be accelerated or denied.
Allow/Deny List Access	If Allow List Access is checked, then any client connecting with an IP in any of the sub-networks added to the list box will be accelerated. If the client is connecting from an IP not in one of the ranges, then the software will disable itself and the user will not experience acceleration and all traffic will bypass WAAS Mobile completely. If Deny List Access is checked, list of sub-networks serves as a “blacklist”, indicating the client IP addresses that will NOT be accelerated. Enter all subnets accelerated by Cisco WAE appliances here.

Upgrades



Upgrade Settings

Enable Component Upgrades

Enable Component Downgrades

Submit

Figure 32 Upgrade Settings

Enable Component Upgrades	Check this to enable core WAAS Mobile components to be upgraded automatically when the client logs in. A client upgrade happens whenever a server is upgraded. The default setting is ON. The client automatically restarts after a component upgrade.
Enable Component Downgrades	Check this to enable core WAAS Mobile components to be downgraded automatically when a server is downgraded. The default setting is OFF, as servers are rarely downgraded. The client automatically restarts after a component downgrade.

System Reports

Cisco WAAS Mobile has a sophisticated diagnostic system which sends detailed system reports – from either or both the client and the server – when requested by the end user or administrator or when abnormal behavior is detected in the acceleration system.

NOTE: These reports may only be analyzed by the Cisco Technical Assistance Center (TAC). Cisco technicians use these reports to validate configuration settings, inspect performance, and perform advanced troubleshooting and diagnostics.

Contents of a System Report

A System Report is a .cab archive that contains several files:

- **Description.txt:** The system report only contains this file if the end user entered a description of the problem they experienced after triggering a system report. Administrators should encourage users to enter a comprehensive and detailed description of the actions that led up to the issue that was observed.
- **Blackbox.txt:** This file contains a wealth of information about the machine from which the report was sent including other software running, networking configuration, as well as the WAAS Mobile software configuration. This information is often very useful troubleshooting configuration or connectivity issues.
- **CustomInfo.xml:** This contains information about the user sending the report, including the User Name with which they logged onto the system.
- **Instrument.dat:** This file contains instrumentation data about what happened on the machine in the time leading up to the triggering of the report. This data is currently only readable by Cisco support personnel.

Triggering System Reports

There are several ways to trigger a system report:

- By the end user clicking the **Send System Report** button of the client user interface (if enabled in the client configuration); this triggers a report from both the WAAS Mobile client and server machines.
- By the administrator via the WAAS Mobile Manager **Home > Status** page; this triggers a report from the WAAS Mobile server only.
- By the administrator for one or more specified client machines via the WAAS Mobile Manager **Home > Active Sessions > Manage** page; this triggers a report from the server and one or more WAAS Mobile client machines.

System Reports Settings

System Reports Settings

System Reports URL:
Enter "default" for System Reports to be sent to this server

System Reports Directory:

Run daily cleanup at Delete files older than days

Enable E-mail Alert

From:

To:

Subject:

Frequency: mins

Outgoing mail server (SMTP): Port: Enable SSL

User Name:

Password:

Enable Packet Capture

Figure 33 System Reports Settings

System Reports URL	Identifies the location on the WAAS Mobile server where the system reports are sent and stored. A value of "default" identifies the current WAAS Mobile server as the target for system reports generated by this server and any clients connecting to it. When deploying multiple WAAS Mobile servers, it is recommended that the system reports from all servers and the clients connecting to them be sent to a single controller server. To push the system reports associated with this server to another WAAS Mobile server, enter: <code>http://<server-ip>/blackbox/BlackBoxCatch.exe?</code> <ul style="list-style-type: none">▪ <server-ip> is the address of the controller WAAS Mobile server▪ The "?" is required at the end of this path
System Reports Directory	Identify the directory for the system reports inbox if a location other than the default is desired. The default location is <code>%ALLUSERSPROFILE%\Application Data\Cisco\WAASMobile\Inbox</code>

Run daily cleanup at	The time at which a daily cleanup is run to delete system report files older than the configured number of days (below).
Delete files older than x days	The age (in days) after which system report files are to be deleted when the daily cleanup occurs.
Enable E-mail Alert	Enables e-mail alerts when system reports are created.
From	Name of sender.
To	Name(s) of recipients.
Subject	Email subject
Frequency	How often e-mail alerts are sent.
Outgoing mail server (SMTP)	Name of SMTP server used to deliver alerts.
Port	Port to use for outgoing mail.
Enable SSL	Enables SSL security.
User Name	SMTP server user name credentials.
Password	SMTP server password credentials.
Enable Packet Capture	If checked, enables packet captures to include in system reports.

Accessing System Reports

System Reports may be downloaded from WAAS Mobile Manager by navigating to **Home > System Reports**.

Import/Export

This section enables system administrators to backup and restore server configuration settings when migrating to new server hardware or upgrading.

Export System Settings

Export

Import System Settings

Import settings from: Browse...

Import

Figure 34 Import/Export Settings

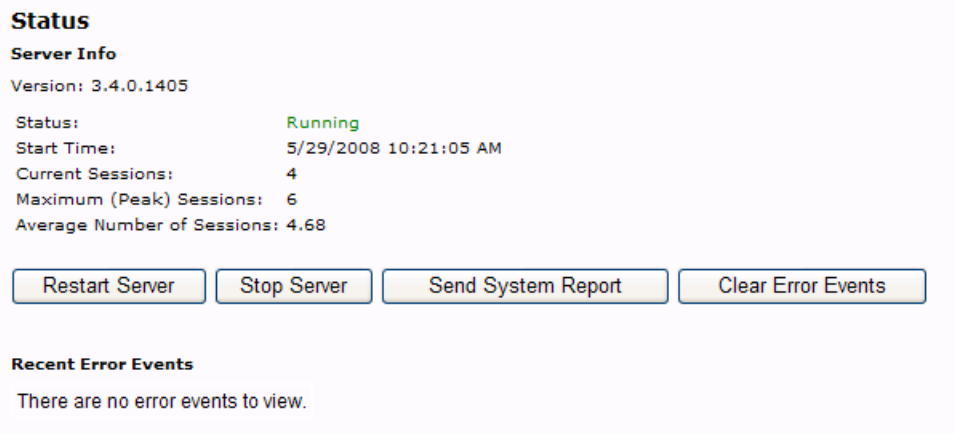
Export	Click to export and respond to the dialog box to save or open the file.
Import Settings from:	Browse to the location of the configuration file to be imported.
Import	Click this to import from the specified location.

Chapter 6 Managing WAAS Mobile

This chapter addresses the features available from the WAAS Mobile Manager **Home** page.

- *Status and Server Control.* Start/start server and view current server status.
- *System Alarms.* Monitor system errors and alarms.
- *Performance Monitoring.* Monitor acceleration performance, links, sessions, and server resource utilization.
- *Active Session Reports.* Monitor currently active user session performance, link characteristics, and session length.
- *Past Session.* Review previous user session performance, link characteristics, and session length.
- *Log Files.* View, download, and delete log files.
- *System Reports.* Download and delete system reports.

Status and Server Control



Status

Server Info

Version: 3.4.0.1405

Status: **Running**

Start Time: 5/29/2008 10:21:05 AM

Current Sessions: 4

Maximum (Peak) Sessions: 6

Average Number of Sessions: 4.68

Restart Server Stop Server Send System Report Clear Error Events

Recent Error Events

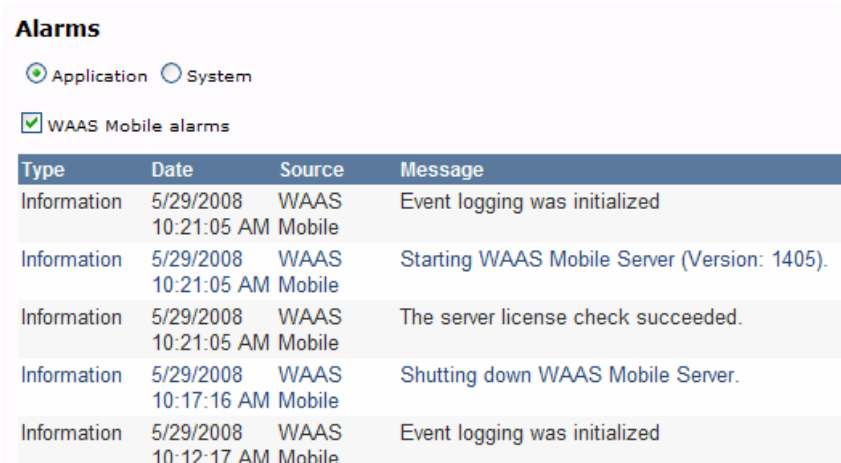
There are no error events to view.

Figure 35 Status

Status	Indicates whether the server is running, stopped, starting, etc.
Start Time	Shows the time and date of last server start (or restart).
Current Sessions	Number of clients currently connected to the server.
Maximum Sessions	Displays the maximum concurrent user count since last restart.
Average Number of Sessions	Shows the average session count since last server restart.
Restart Server	Start or restart the server by clicking this button.
Stop Server	Stop the server by clicking this button.
Send System Report	Creates and posts a server system report. A dialog box will be displayed to enable a description to be sent with the System Report. When ready, click the Send System Report button on the dialog box, or click Cancel.
Clear Error Events	Clears Recent Error Events list.
Recent Error Events	This list contains recent errors reported by the server.

System Alarms

The Alarms page lists NT Events or SNMP Alarms as well as relevant system events such as when the system was rebooted. Refer to Chapter 8 for information on alarm messages.



The screenshot shows the 'Alarms' section of a management interface. It includes radio buttons for 'Application' (selected) and 'System', and a checked checkbox for 'WAAS Mobile alarms'. Below is a table with columns for Type, Date, Source, and Message.

Type	Date	Source	Message
Information	5/29/2008 10:21:05 AM	WAAS Mobile	Event logging was initialized
Information	5/29/2008 10:21:05 AM	WAAS Mobile	Starting WAAS Mobile Server (Version: 1405).
Information	5/29/2008 10:21:05 AM	WAAS Mobile	The server license check succeeded.
Information	5/29/2008 10:17:16 AM	WAAS Mobile	Shutting down WAAS Mobile Server.
Information	5/29/2008 10:12:17 AM	WAAS Mobile	Event logging was initialized

Figure 36 System Alarms

Application	Displays application-level NT events and SNMP alarms associated with this server. This selection also enables the checkbox to view only alarms associated with the WAAS Mobile application.
System	Displays system-level NT events and SNMP alarms associated with this server.
WAAS Mobile alarms	Checking this box will filter the application alarms to those associated with the WAAS Mobile application only.

Performance Monitoring

This area of WAAS Mobile Manager contains a series of pages with graphs based on performance counters that monitor application traffic performance, user sessions, HTTP details, disk system usage, and system statistics, and delta cache utilization.

Use the drop-down menus on each page to view several graphs in each area and to specify the time interval to be graphed.

Update the graphed information at any time by clicking the **Refresh** button.

Traffic Summary

WAAS Mobile provides two overall traffic summary reports – Application Summary and Compression Summary. The Application Summary graph displays the raw volume (in MB) and percent of bandwidth used by each application protocol. The compression summary shows the effect of WAAS Mobile’s compression by displaying the raw and compressed data volume, as well as the compression ratio for each application protocol.

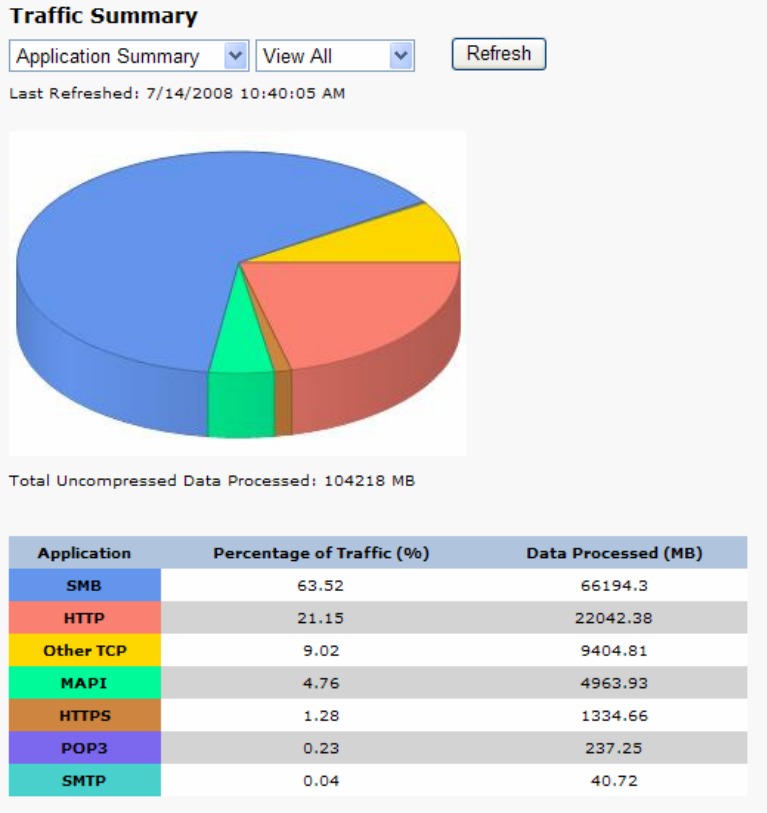


Figure 37 Traffic Summary - Application Summary

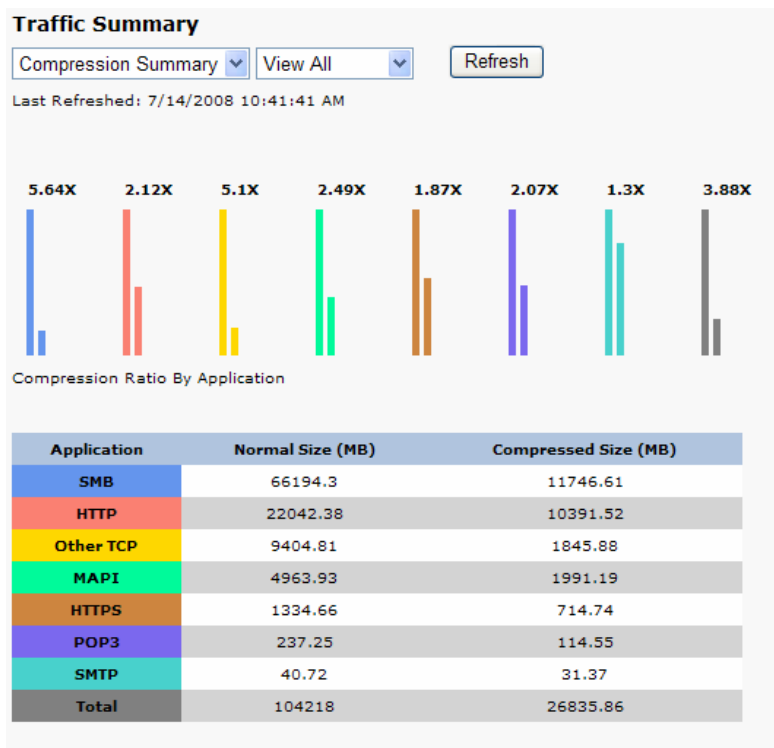


Figure 38 Traffic Summary - Compression Summary

Application Traffic

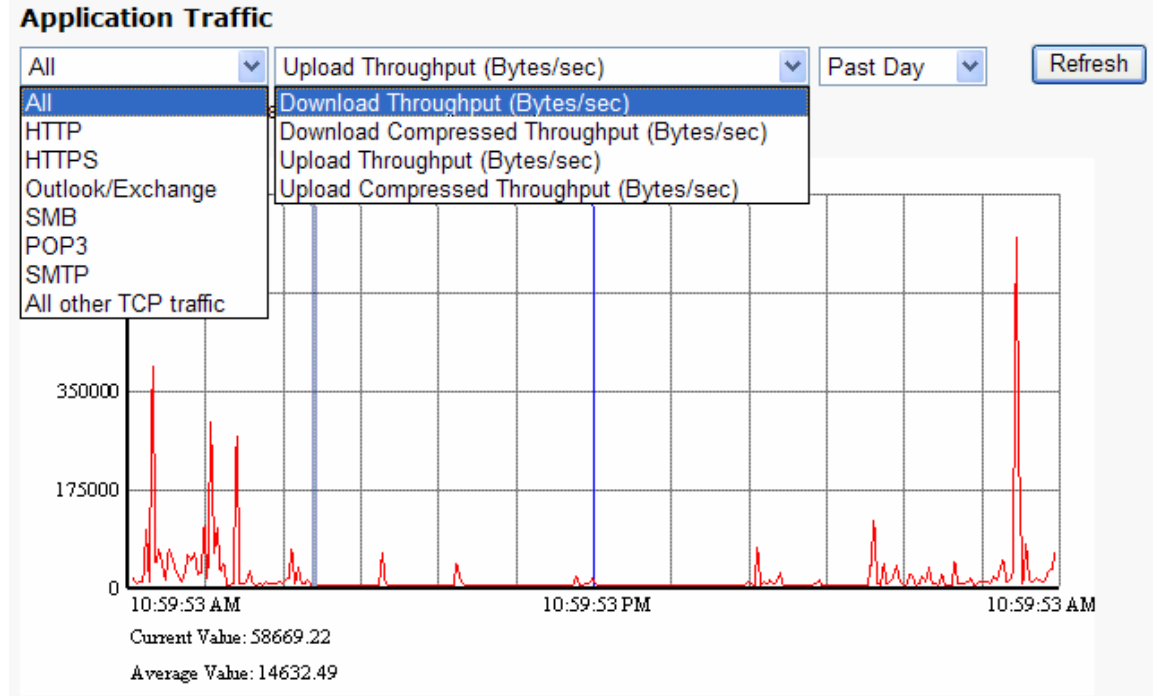


Figure 39 Application Traffic

Use the drop-down menus to display different types of TCP traffic activity over different time periods. Click **Refresh** to update the graph.

NOTE: "All other TCP traffic" includes other TCP traffic that is being proxied and accelerated by the WAAS Mobile client. It does not include TCP traffic that is not being accelerated.

The performance metrics which may be displayed graphically from the pull-down menu include:

- Download Throughput (Bytes/sec)
- Download Compressed Throughput (Bytes/sec)
- Upload Throughput (Bytes/sec)
- Upload Compressed Throughput (Bytes/sec)

Sessions

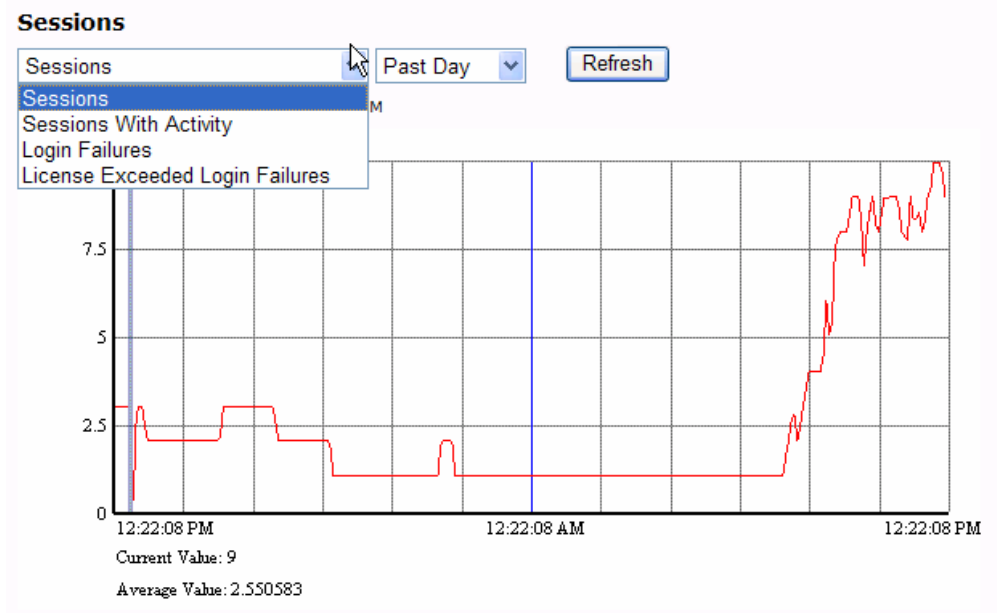


Figure 40 Session Monitoring

Use the drop-down menus to display user session activity recorded over different time periods. Click **Refresh** to update the graph.

Session data which may be displayed includes:

- Sessions: Total number of sessions
- Sessions With Activity: Number of active sessions
- Login Failures: Sessions with authentication failures
- License Exceeded Login Failures: Sessions that were rejected due to insufficient licenses

HTTP Details

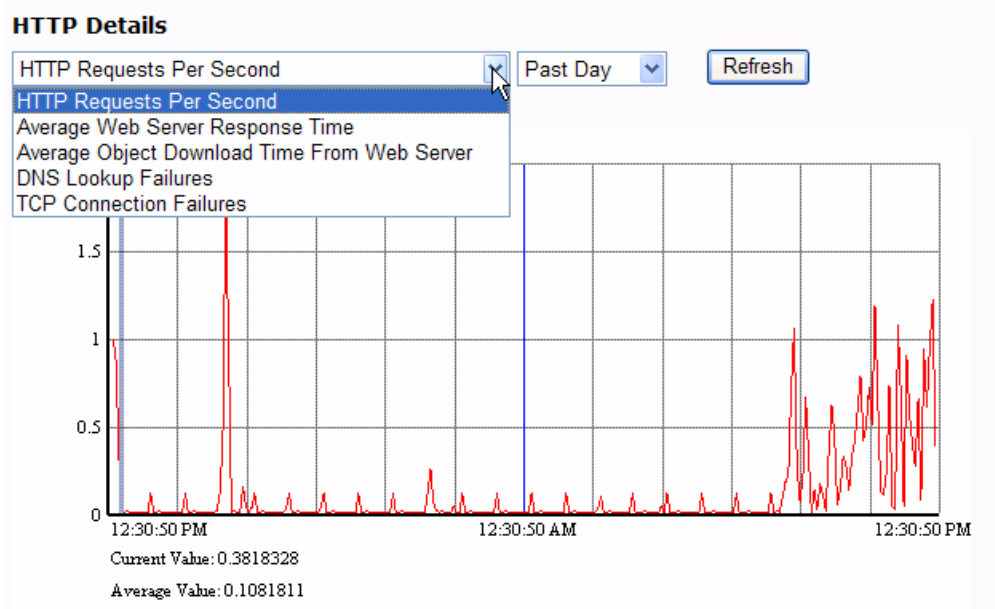


Figure 41 HTTP Details Monitoring

Use the drop-down menus to display HTTP statistics recorded over different time periods. Click **Refresh** to update the graph.

HTTP monitoring metrics include:

- HTTP Requests Per Second
- Average Web Server Response Time
- Average Object Download Time From Web Server
- DNS Lookup Failures
- TCP Connection Failures

Disk System

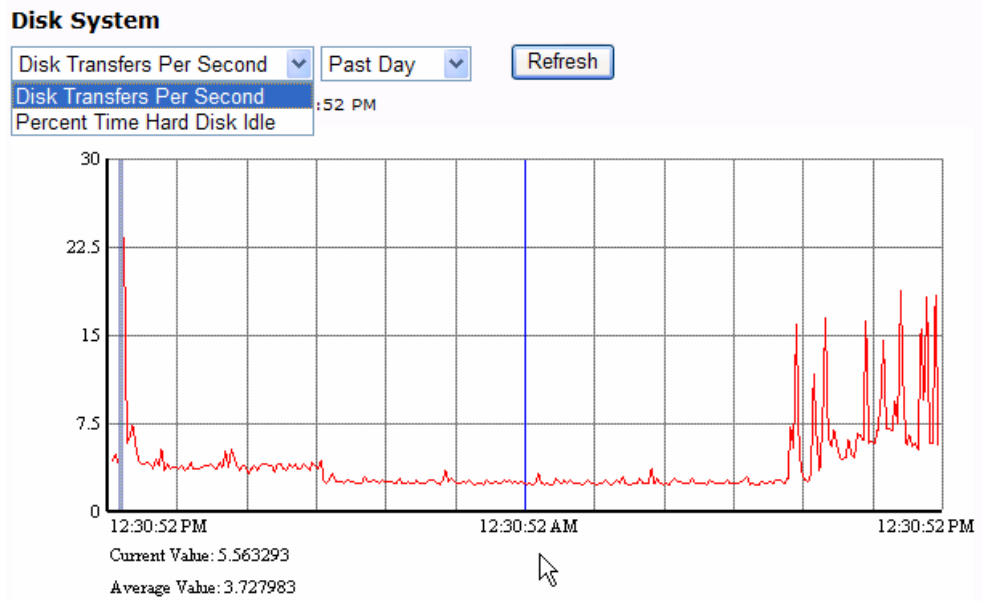


Figure 42 Disk System Monitoring

Use the drop-down menus to display disk activity and usage recorded over different time periods.

Click **Refresh** to update the graph.

Disk activity metrics include:

- Disk Transfers Per Second
- Percent Time Hard Disk Idle

System Stats

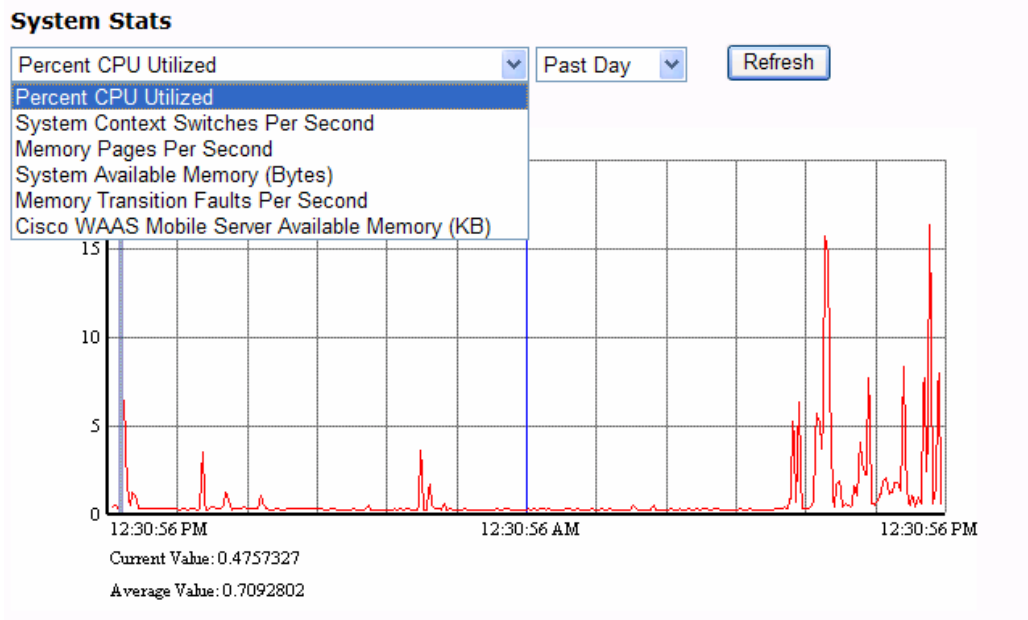


Figure 43 Server System Statistics Monitoring

Use the drop-down menus to display server activity and utilization over different time periods. Click **Refresh** to update the graph.

Server statistics include:

- Percent CPU Utilized
- System Context Switches Per Second
- Memory Pages Per Second
- System Available Memory (Bytes)
- Memory Transition Faults Per Second
- Server Available Memory (KB)

Delta Cache

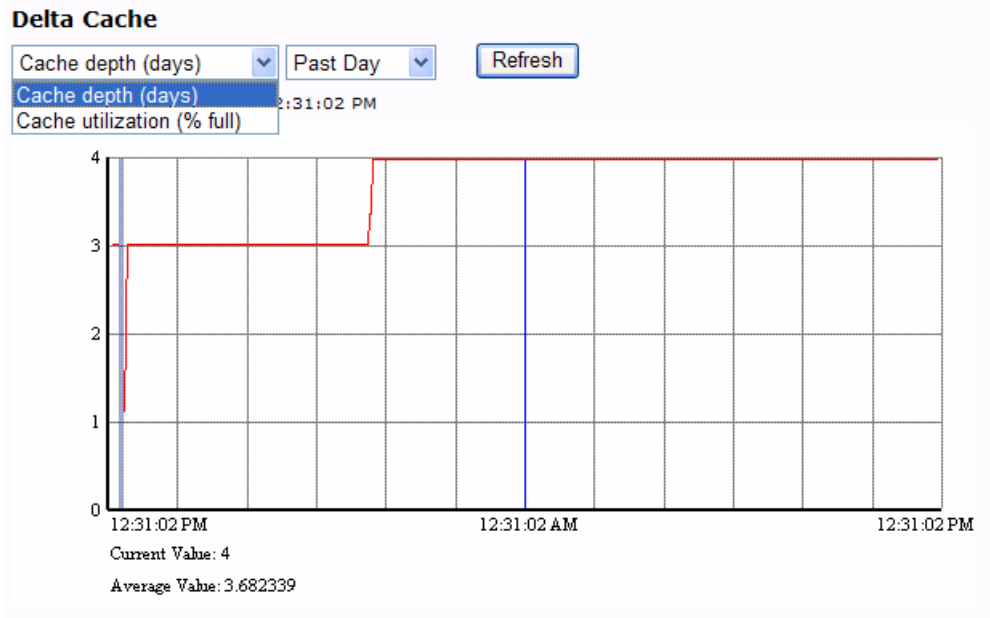


Figure 44 Delta Cache Monitoring

The delta cache is a circular buffer. After initial usage, the delta cache will reach 100% full and remain at that level. From that point on, the cache depth should be monitored. Cache depth informs the user of the age of the items being deleted to make room for new history traffic.

NOTE: If the cache depth is small (e.g., only a couple of weeks), consider provisioning additional storage.

Active Sessions Reports

Use Active Sessions Reports to obtain information about currently active user sessions and to manage those sessions. User information is displayed based on authentication and client registration settings. Clicking **Update Now** displays the current information.

- *Connection* provides connection time information.
- *Traffic* provides traffic volume information.
- *Link* provides link performance information.
- *Installation* provides distribution label and other installation-related information.
- *Delta Cache* monitors the client's cache utilization and cache depth.
- *Manage* allows users to be messaged or removed and enables system reports to be triggered from selected users.

Active Sessions Connection Time

The **Active Sessions > Connection** report provides connection information for active sessions. A "1" in the **Persisting** column indicates that there has been recent activity on the connection.

Active Sessions

Data Last Updated: 9:25:46 AM

Session Id	User ID	Client IP	Alias IP	Session Length (seconds)	Persisting	Distribution Label
5	david@company.com	10.13.1.65	0.0.0.0	9	1	SampleClientDistribution

Figure 45 Active Sessions - Connection Time

Active Sessions Traffic Volume

The **Active Sessions > Traffic** report shows sent/received data compression performance for each active session.

Active Sessions

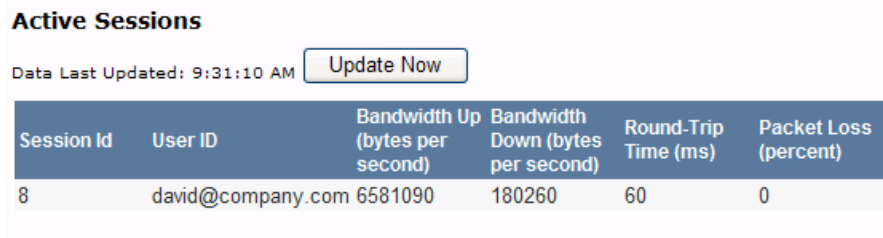
Data Last Updated: 9:28:42 AM

Session Id	User ID	Raw Bytes Sent	Compressed Bytes Sent	Raw Bytes Received	Compressed Bytes Received
5	david@company.com	85938	19483	4701340	1345203

Figure 46 Active Sessions - Traffic Volume

Active Sessions Link Performance

The **Active Sessions > Link** report shows the actual bandwidth, delay, and packet loss measured when the clients connected to the WAAS Mobile server.



The screenshot shows a report titled "Active Sessions" with a sub-header "Link Performance". It includes a "Data Last Updated" timestamp of 9:31:10 AM and an "Update Now" button. Below this is a table with the following data:

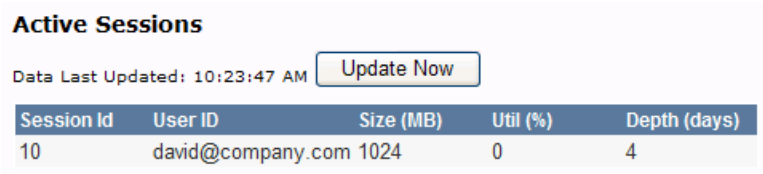
Session Id	User ID	Bandwidth Up (bytes per second)	Bandwidth Down (bytes per second)	Round-Trip Time (ms)	Packet Loss (percent)
8	david@company.com	6581090	180260	60	0

Figure 47 Active Sessions - Link Performance

Active Sessions Delta Cache

The **Active Sessions > Delta Cache** report displays the configured size and utilization/depth of each user's cache. The delta cache is a circular buffer. After initial usage, the delta cache will fill to 100% and remain full. Once the buffer fills, the cache depth should be monitored. Cache depth informs the user of the age of the items being deleted to make room for new history traffic.

NOTE: If the cache depth is small (e.g., only a couple of weeks), consider provisioning additional storage.



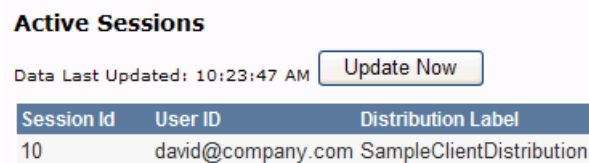
The screenshot shows a report titled "Active Sessions" with a sub-header "Delta Cache Performance". It includes a "Data Last Updated" timestamp of 10:23:47 AM and an "Update Now" button. Below this is a table with the following data:

Session Id	User ID	Size (MB)	Util (%)	Depth (days)
10	david@company.com	1024	0	4

Figure 48 Active Sessions - Delta Cache Performance

Active Sessions Installation Information

The **Active Sessions > Installation** page shows the currently installed client distribution associated with each user.



The screenshot shows a report titled "Active Sessions" with a sub-header "Installation Information". It includes a "Data Last Updated" timestamp of 10:23:47 AM and an "Update Now" button. Below this is a table with the following data:

Session Id	User ID	Distribution Label
10	david@company.com	SampleClientDistribution

Figure 49 Active Sessions - Installation Information

Active Sessions Management

The **Active Sessions > Manage** page allows the administrator to send messages to users, trigger client-side system reports, and disconnect hung user sessions.

Active Sessions

Data Last Updated: 10:23:47 AM

Message:

Select	Session Id	User ID
<input type="checkbox"/>	10	david@company.com

Figure 50 Active Sessions - Management

Message Selected Users	In the Message field, type a message to be sent to selected users. Click the button to send the message. It will be displayed on the screen of the user involved.
Kick Selected Users	Select the session(s) to be removed by checking a box. Click the button to remove the selected session(s).
Trigger System Reports	Select the session(s) from which a System Report is to be triggered.

Past Sessions Reports

Use Past Sessions Reports to obtain information about session history. User information is displayed based on authentication and client registration settings. If the **UserID** entry field is left blank, the table will display information for all users.

- *Connection* provides connection time history information for past sessions.
- *Traffic* provides traffic volume history information for past sessions.
- *Link* provides link performance history information for past sessions.
- *Delta Cache* monitors the client's cache utilization and cache depth.
- *Installation* provides distribution label and other installation-related history information for past sessions.

Past Sessions Connection Time History

The **Past Sessions > Connection** report provides session length statistics for past sessions.

Time Stamp	User ID	Session Length (seconds)	Client IP	Alias IP
2008-07-14 09:31:02	david@company.com	316	10.13.1.65	0.0.0.0

Figure 51 Past Sessions - Connection Time History

Past Sessions Traffic Volume History

The **Past Sessions > Traffic** report shows sent/received data compression performance for each previously completed session.

Time Stamp	User ID	Raw Bytes Sent	Compressed Bytes Sent	Raw Bytes Received	Compressed Bytes Received
7/14/2008 9:31:02 AM	david@company.com	86678	19678	4701840	1345315

Figure 52 Past Sessions - Traffic Volume History

Past Sessions Link Performance History

The **Past Sessions > Link** report shows the actual bandwidth, delay, and packet loss measured when the clients connected to the WAAS Mobile server.

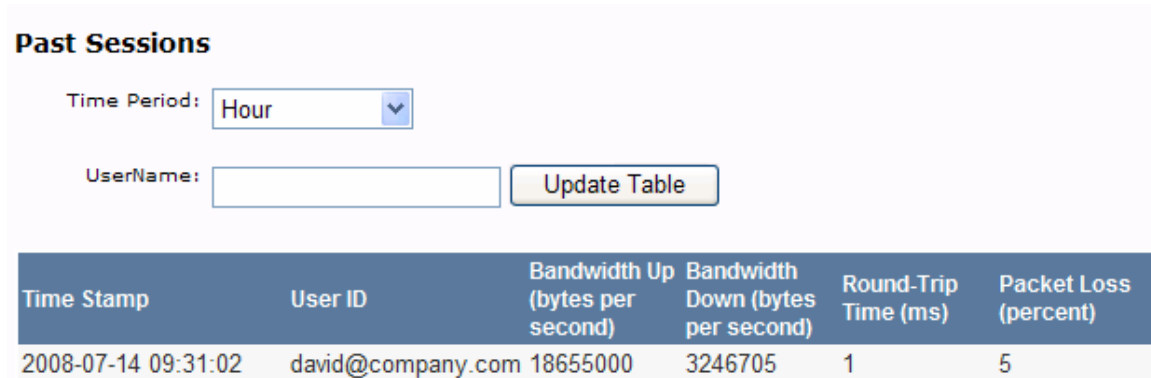


Figure 53 Past Sessions - Link Performance History

Past Sessions Delta Cache History

The **Past Sessions > Delta Cache** report displays the configured size and utilization/depth of each user's cache. The delta cache is a circular buffer. After initial usage, the delta cache will fill to 100% and remain full. Once the buffer fills, the cache depth should be monitored. Cache depth informs the user of the age of the items being deleted to make room for new history traffic.

NOTE: If the cache depth is small (e.g., only a couple of weeks), consider provisioning additional storage.

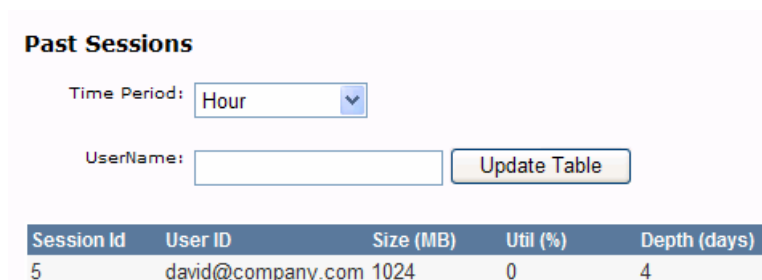


Figure 54 Past Sessions - Delta Cache History

Past Sessions Installation History

The **Past Sessions > Installation** report shows the installed client distribution associated with each user.

Past Sessions

Time Period:

UserName:

Time Stamp	User ID	Distribution Label	Major Version	Minor Version	Patch Number	Build Number
2008-07-14 10:23:15	david@company.com	SampleClientDistribution	3	4	0	1454

Figure 55 Past Sessions - Client Installation History

Log File

For

From **To**

Figure 56 Log File

For	Select to show the log file for one of the pre-defined time periods
From/To	Select to define a time period for event viewing using dates.
View	Displays the log file events corresponding to the selected time period.
Download	Downloads a copy of the log file.
Delete	Deletes the current log file; a new log file is created to replace the old one.
Show The Next 25	Page through the events; the button is disabled if there are fewer than 25 events.

System Reports

By default, system reports from both client and server are directed to the WAAS Mobile server and are available on the **System Reports** page of WAAS Mobile Manager. Mousing over each system report entry displays the size of that system report file.

Download	Name	Build	Computer Name	TimeStamp	Description	OSType
Download	56_Client_3.4.0.1404_5811E9_10.13.1.65.cab	1404	LP-DLERNER-WXP	5/29/2008 9:54:17 AM		5.1.2600 (SP 2.0) Windows XP Service Pack 2
Download	56_Server_3.4.0.1404_5311E8_127.0.0.1.cab	1404	DONALD	5/29/2008 9:52:52 AM		5.2.3790 (SP 2.0) Windows 2003 Service Pack 2

Figure 57 System Reports Monitoring

Refresh	Refreshes the page
Disk Space in Use For System Reports	Shows the total amount of disk space being used for reports in the system reports directory, as well as the free space available on the drive in parentheses.
Total files	Displays the total number of system reports in the in the directory.
Delete All	Deletes all reports from the system reports directory.
Download	Click this to download the system report .cab file for analysis.

System Reports Naming Convention

Reports listed on the WAAS Mobile Manager **System Reports** page use the following naming convention:

- *aaa_Client_[build number]_xxxxxx_[WAAS Mobile client IP].cab*: This report is generated by the main acceleration module on the client machine. If a customer entered a text description, it will be contained in this report.
- *aaa_Server_[build number]_zzzzzz_[WAAS Mobile server IP].cab*: This report is generated by the WAAS Mobile server whenever a client generates a system report, when a crash occurs on the server, or when an administrator triggers a system report via WAAS Mobile Manager.

where:

- *aaa* is a number that indicates the session where the problem occurred. It will usually be the same on both reports (client and server) associated with a user session.
- *xxxxxx* and *zzzzzz* are unique system-generated numbers to ensure that file titles are not duplicated.

If a crash occurs on the WAAS Mobile server, only the server report will be generated. If a crash occurs in the WAAS Mobile client, only a client report will be generated (if client system reports are enabled).

Associating Client and Server System Reports

When an end user reports an issue and sends a system report via the user interface, this will trigger both the client and server software to send system reports to the server. It is typically important to send both system reports to Cisco in order to diagnose and resolve the issue. This can be done by finding the "Client" and "Server" system reports in the table above that have the same session id number, which is the first component in the system report name ("*aaa*") defined above.

Chapter 7 Diagnostics

WAAS Mobile provides a comprehensive set of diagnostics tools that provide detailed information on system health and performance. This chapter provides an overview of the various types of information that are available and the information available from each information source.

Diagnostics include:

- Server-side diagnostics
 - Client monitoring
 - System monitoring
 - System events and alarms
 - System reports
 - Logs
- Client-side diagnostics
 - Icon colors
 - Connection statistics
 - System reports

Server-Side Diagnostics

Client monitoring

Client monitoring, as described in Chapter 6 enables the administrator to monitor each user's acceleration performance, link capacity, delta cache capacity, software version, and configuration. The administrator may monitor either currently active or past sessions of any particular user. In order to facilitate effective client monitoring, the administrator should require users to register the WAAS Mobile software upon installation. Registration information is transmitted only to the WAAS Mobile server and is only used to correlate activity to users in order to assist with troubleshooting and support. (By default, this registration step is enabled.)

System monitoring

System monitoring, as described in Chapter 6 enables the administrator to monitor overall acceleration performance, system performance and server status. This information is displayed graphically through WAAS Mobile Manager.

The data that is displayed in these graphs is obtained from Windows Performance Monitor (PerfMon) counters. These PerfMon counters may be monitored directly using standard tools. Additionally, the same data that is available via the PerfMon counters is also available via the MIB, and may be displayed via any standard network management tool.

The graphs are generated via calls to a back-end database, which by default is SQLite. For larger deployments, the administrator may use a MySQL or Microsoft SQL database instead by navigating to the **Server Configuration > RDBMS Logging** menu and configuring a different database.

Additionally, the administrator may use RADIUS accounting to aggregate session data, including user, session length, up/down raw and compressed bytes, from multiple WAAS Mobile servers onto a single external server.

System events and alarms

As described in Chapter 6, the most recent alarms are displayed on the WAAS Mobile Manager **Home > Status** page and all alarms are displayed on the **Home > Alarms** page.

Internally, these alarms are generated as NT events and, as such may be monitored by Microsoft System Manager or, using any number of 3rd party utilities, may be pushed to a syslog. In addition, for each NT event, an SNMP trap is also set, enabling standard network management tools to monitor WAAS Mobile system events. The WAAS Mobile server MIB is installed with the server software in the `\Program Files\Cisco\WAASMobileServer` folder.

System reports

See Chapter 9 for a complete description of system reports. System reports are not human-readable, and are sent to Cisco for advanced troubleshooting support. To ensure that all necessary troubleshooting information is captured:

- Enable **Network Monitoring** (prior to generating the system report) by navigating to the WAAS Mobile Manager **Client Configuration > Diagnostics** menu. This feature is disabled by default, as there may be interoperability issues with certain IPsec VPNs (e.g., CheckPoint)
- Ensure that both the WAAS Mobile client and server are running. If the user **Disables** the client, the troubleshooting information is preserved, but if he/she **Exits** the client, all debug information is lost
- Generate the system report shortly after an event occurs since, by default, the system report only covers a short traffic interval. To enable the capture of more history, enable **Large Client System Reports** by navigating to the WAAS Mobile Manager **Client Configuration > Diagnostics** menu, but still ensure that the system report is generated as soon after the event occurs as possible.
- Enter a concise description of the issue in the system report description field, including the sequence of steps that led up to the occurrence of the issue. This will guide the Cisco engineers who examine the report.
- Capture both a client and server system report. The prefix numbers in the system report title associate the report with a user session and facilitate the matching of server and client reports associated with the same event, as they will start with the same prefix.

Logs

There are multiple types of logs that may be generated, including:

- Installation log. This is only generated if the installer is run via the `misexec` command.
- System logs. In general, system log information is more meaningfully displayed via the monitoring functions described in Chapter 6. In some cases, enabling the debug log level may provide additional information. Use the WAAS Mobile Manager **Server Configuration** options to control log rotation and logging level, as described in Chapter 5.
- Debug logs. Debug logging should not be enabled on production servers.

Client-Side Diagnostics

Icon Colors

While running, an “acceleration icon” will be displayed in the Windows system tray to indicate the WAAS Mobile software status.

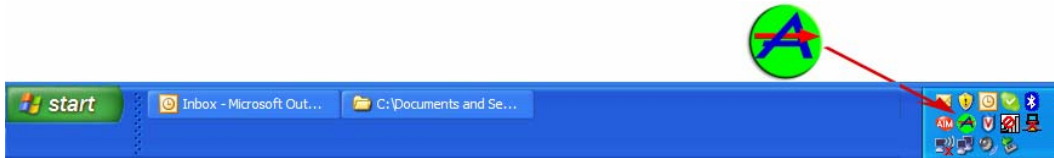


Figure 58 Acceleration Icon in System Tray

The icon states and corresponding descriptions are as follows:



Cisco WAAS Mobile is running and accelerating applications



Cisco WAAS Mobile is running but application acceleration has been disabled by the user



Cisco WAAS Mobile has lost connection to the WAAS Mobile server and is not accelerating applications



Cisco WAAS Mobile has lost connection to the WAAS Mobile server but is still active and the connection is persisting (only occurs if persistent sessions is enabled)

Connection Statistics

When the user selects **Client Manager** from the tray icon menu, the **Connection Monitor** tab is displayed. Using the information displayed in the fields and event log on this screen, the end user can rapidly determine if traffic is correctly passing through WAAS Mobile and being accelerated.

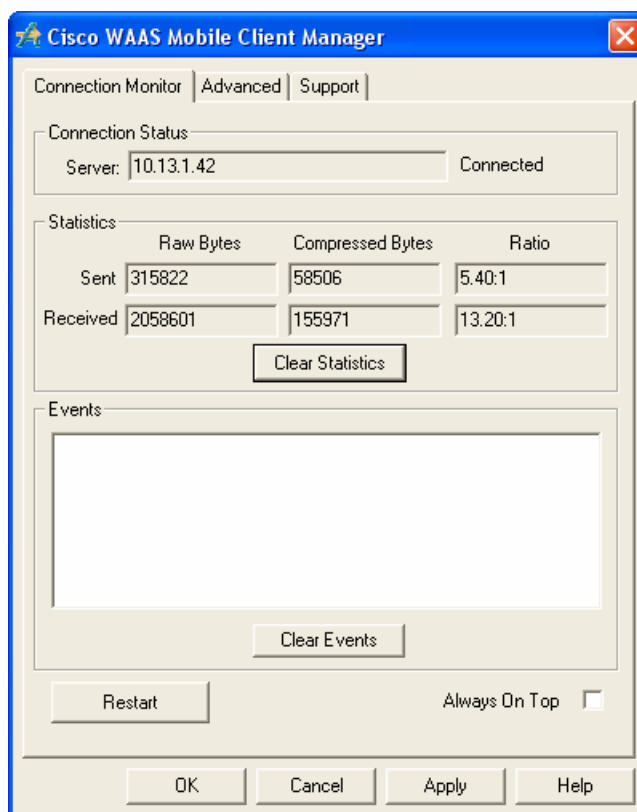


Figure 59 Client Manager - Connection Monitor Tab

Connection Status

The status reported in the **Connection Status** section of the Client Manager will be one of the following:

Connected: This is the “normal” mode and indicates that the server is ready and able to send data to (and receive data from) the client.

User Disabled: Indicates that the user has disabled acceleration manually from the acceleration icon menu. Data is still sent and received over the communications link, but not at accelerated rates.

Not Connected: Indicates that the server currently is not able to provide acceleration, even though client acceleration is enabled. Data is still sent and received over the communications link, but not at accelerated rates.

Statistics	Provides data compression information, which is one measure of the acceleration performance of Cisco WAAS Mobile. Separate cumulative statistics are provided for data being sent from and data being received by the computer. Although compression is only one aspect of acceleration performance, it's generally true that if the compression ratio is high, acceleration performance is high as well. Clicking on the Clear Statistics button resets these statistics.
Events	Displays messages indicating a variety of system activities. Clicking on the Clear Events button resets the event log. Upon start-up, WAAS Mobile detects the actual amount of bandwidth and latency for the user's link and displays the information here.
Restart	Clicking Restart while the client is running temporarily disconnects the client from the server, and then automatically reconnects again.
Always on Top	Displays the Client Manager dialog on top of all other open windows.

System Reports

Chapter 9 provides a complete description of how to generate a system report. Note that system reports must be generated while the WAAS Mobile client is running and shortly after the issue has occurred. When the client generates a system report, information is captured on both the WAAS Mobile client and server is automatically uploaded to the WAAS Mobile server.

Chapter 8 Troubleshooting

This chapter is divided into two sections: the first is intended to guide administrators in determining exactly what type of issue the user is having, and the second can then be used to help troubleshoot and resolve the issue. If necessary or if the support issue is beyond the scope of this document, escalate the issue to the Cisco Technical Assistance Center (TAC) for assistance.

Installation & Integration

- General installation issues
 - Please confirm that the client or server in question meets the minimum hardware requirements and that the server meets all software requirements as noted in Chapter 2.
 - For server installation issues, see Table 6 in this chapter.
 - For client installation issues, see Table 7 in this chapter.
- Networking issue relating to server integration
 - Refer to Table 6 in this chapter; in general, the server should be setup in similar fashion to other application servers co-located with it.

NOTE: The Cisco WAAS Mobile system is not in the critical path, which means when properly configured it will never restrict access to resources. If the server or client crashes the client machine will simply lose acceleration to network resources, not access.

Functionality

- Client unable to connect to WAAS Mobile server
 - This could be a problem on the client machine, server machine or the network so, while a common problem, it is also complex in nature. It is recommended to check the **Events** window in the client's **Connection Monitor** and then refer to Table 8.
- Server not running
 - Confirm that a valid license key being used, then refer to Table 6.
 - Check the WAAS Mobile Manager **Home > Alarms** screen for related messages.
- Client unable to connect to network resource when connected to the WAAS Mobile server
 - Confirm that the problem is resolved when WAAS Mobile is not running.
 - Check that the WAAS Mobile server has access to resource.

Performance

- Acceleration is not occurring
 - Check the client **Connection Monitor** to verify connectivity and whether the sent/received statistics are incrementing.
 - Refer to Table 7 for further troubleshooting techniques.
 - Send a system report for analysis.

Problem Isolation

WAAS Mobile Server Issues and Isolation

Table 6 WAAS Mobile Server Issues and Isolation

Activity	Symptom	Possible Causes	Resolution
Installation	License key issues	No license key has been input, invalid license key input	Input a valid license key in the Server Configuration > Licensing page.
	General installation issues	Missing operating system components (for example, IIS)	Verify server software and hardware requirements found in Chapter 2.
Networking	Network or Specific Resource is Inaccessible	General Networking Issue on Server During Setup	Use the command line tool <i>ipconfig.exe</i> along with Windows Network Connections module to verify the WAAS Mobile server has the proper network settings.
WAAS Mobile Manager	An "Under Construction" page is presented when opening WAAS Mobile Manager	Incorrect URL or Firewall issues	Verify the URL is in the form of <code>http://ServerName/Cisco WAAS Mobile/</code> . Verify network path to the server and that WAAS Mobile Manager will open using the browser on the server.

WAAS Mobile Client Issues and Isolation

Table 7 WAAS Mobile Client Issues and Isolation

Activity	Symptom	Possible Causes	Resolution
Client Installation	Conflicting Components Found Message	Another program on client machine conflicts with networking layer in WAAS Mobile. Typically this is security, firewall or anti-virus software.	Capture the information on the conflict, including screen shots. Check the Release Notes and Chapter 2 of this guide for known software conflicts. Other LSP-based software will cause this problem. Contact Cisco support if the conflicting program cannot be removed.
Client Installation	Client Fails to Install	The client installation components may be inaccessible if hosted on a network share	Restart the client computer and retry the installation.
Client Installation	Client Fails to Install	In the rare case where an install fails after multiple attempts a machine may have a bad OS configuration	Contact Cisco support for assistance.
Client Startup	The user is asked for user name and password credentials when starting WAAS Mobile.	Client registration has been enabled and the user has not entered authorized login credentials.	Use the WAAS Mobile Manager Server Configuration > Authentication and User Management pages to review or modify the settings. See also the <i>Authentication</i> section in Chapter 5.

Activity	Symptom	Possible Causes	Resolution
Client Connection	Icon in system tray shows not connected	If this is happening for all users, the server may not be running.	First, go to the WAAS Mobile Manager Home > Status page to verify that the server is running. Then, on the client PC, open the Client Manager , view Events , and refer to Table 8.
Client Operations	WAAS Mobile is connected but HTTP traffic is not being accelerated	Proxy settings can cause protocol specific errors	Check the user's browser settings for an incorrect proxy address.
Client Operations	Unable to access site or network share	The WAAS Mobile server must have access to the site	Confirm this issue occurs when WAAS Mobile is not running. Once WAAS Mobile is running, all accelerated traffic is routed through the WAAS Mobile server; confirm the WAAS Mobile server is able to access this resource via the WAAS Mobile server OS.
Client Operations	Application is not being accelerated	Configuration issue can result in traffic bypassing WAAS Mobile.	First, determine if the traffic is passing through WAAS Mobile by viewing the client Connection Monitor statistics. If it is not, review the WAAS Mobile Manager Client Configuration > Proxied Process List and verify that the process generating the traffic on the client is listed. If not, add the process to this list. If after reviewing all these settings and data is going through WAAS Mobile but does not seem to be accelerating as expected, send a system report for analysis.

Activity	Symptom	Possible Causes	Resolution
Client Operations	Application is not being accelerated	WAAS Mobile is bypassing a network resource	Check the WAAS Mobile Manager Client Configuration > Connection Settings ; a client may bypass resources if Latency Based Bypass is on and the latency value is below the threshold. If latency bypass is not causing the problem, verify all settings for Client Configuration > Accelerated Networks Table, HTTP/HTTPS Settings and Exclusion Lists .

Client Event Messages

The table below includes commonly-seen messages in the **Events** window of the **Client Manager Connection Monitor**.

Table 8 WAAS Mobile Client Event Messages

Event Text	Cause	Resolution
Client registration information required	User registration is enabled in the server configuration.	Use the WAAS Mobile Manager Server Configuration > Authentication page to manage client registration options.
Connected	This is the normal state when the client is connected to the server.	No action required.
Connecting...	This a normal transitory state while establishing the connection between the client and the server.	No action required.
Connection inactive too long	IIP reported that the session was inactive too long (no data received from server).	Trigger a system report for analysis. Verify the state of the server. If the server is running, contact technical support.

Event Text	Cause	Resolution
Could Not Resolve Server Address	Client is unable to resolve DNS name of the WAAS Mobile server.	Consider DNS issues. Confirm that the server address can be resolved by the client system.
Disconnected by server	The administrator has actively disconnected the client.	See the WAAS Mobile Manager Home > Active Sessions > Manage page to manage client connections. The client software must be actively restarted to re-establish the connection.
Download bandwidth (bytes/sec) is XX Upload bandwidth (bytes/sec) is YY Round-trip time (ms) is ZZ	This is a normal event after establishing the connection between the client and the server.	No action required. The bandwidth displayed is based on a small one-time sample of network traffic; a more accurate assessment will be displayed after the connection is established.
Downloaded new settings	This is a normal transitory state while establishing the connection between the client and the server. It indicates that new settings were acquired from the server.	No action required.
Entering Persistent Mode	Persistent mode is enabled for this client and the connection between the client and the server is not available.	No action required. This is a per-client distribution setting.
Finalizing connection	This is a normal transitory state while establishing the connection between the client and the server.	No action required.
High-speed connection present	High speed bypass is on and connection speed exceeds the configured settings.	Clients on a LAN may be configured to bypass acceleration. If you wish to change this setting adjust the High Speed Bypass settings on the WAAS Mobile Manager Client Configuration > Connection Settings page.

Event Text	Cause	Resolution
High-speed connection present	No network path to server	Verify the network path and/or DNS resolution from client to server using a system tool such as the Windows ping command.
Incorrect User Name	Server configuration requires users to authenticate prior to connecting; the user's credentials have been rejected.	Users must enter valid credentials; administrators can use the WAAS Mobile Manager Server Configuration > Authentication and User Management settings to enable/disable authentication and manage user credentials.
License expired or invalid	A licensing issue is indicated.	Use the WAAS Mobile Manager Server Configuration > Licensing page to verify a license has been set.
License granted successfully	This a normal transitory state while establishing the connection between the client and the server.	No action required.
License request failed	A licensing issue is indicated.	Use the WAAS Mobile Manager Server Configuration > Licensing page to verify a license has been set.
Login attempt timed out	Server did not respond in time to session initiation.	Trigger a system report for analysis. If there are no known issues with the network or the condition persists, contact technical support.
Maximum number of allowed sessions exceeded	A licensing issue is indicated.	Use the WAAS Mobile Manager Server Configuration > Licensing page to verify a license has been set.
New server selection settings, reconnecting	Client received new server selection table, reconnecting based on new selection mode.	No action required; client will reconnect and begin using new settings.

Event Text	Cause	Resolution
Network Problem	Transport (ITP) reported an error in network.	Trigger a system report for analysis. If there are no known issues with the network or the condition persists, contact technical support.
No Internet Connection Present	Transport (ITP) reported an error in network.	Trigger a system report for analysis. If there are no known issues with the network or the condition persists, contact technical support.
Old session invalid, creating new one	Client attempted to restore a persistent connection, but it wasn't found on the server.	No action required. The client will create a new session and connect automatically.
Protocol or Data Problem	Error in application data parsing code (encode/decode).	Trigger a system report for analysis and contact technical support.
Reconnected to Server	This a normal transitory state while establishing the connection between the client and the server.	No action required.
Server Busy	Server authorization timed out, or no UDP port available.	Trigger a system report for analysis and contact technical support.
Server Disconnected	Server was stopped.	Verify server status. The client will reconnect automatically when the server is available.
Server licenses exceeded	Licenses are all in use.	No acceleration will be available until a license is free. Confirm licenses are all in use by comparing the number of Current Sessions on the WAAS Mobile Manager Home > Status page to the Maximum Number of Active Users on the Server Configuration > Licensing page.

Event Text	Cause	Resolution
Server not reachable	Server is not running or the license is not available.	Verify that the server state and licensing. Contact technical support if required.
Server not reachable	Network	Perform network diagnostics to see that client can ping the WAAS Mobile server and that a firewall would not be blocking port 1182 UDP and TCP.
Server not reachable	Client firewall	Check to see if a firewall on the user's machine is blocking port 1182 UDP and TCP.
Server problem, will try again later	Encryption setting mismatch between client/server, or bad state transition on server	Trigger a system report for analysis and contact technical support.
Server Ready!!!	This a normal transitory state while establishing the connection between the client and the server.	No action required.
Testing UDP connectivity	This a normal transitory state while establishing the connection between the client and the server.	No action required.
UDP test failure	Firewall issue relating to UDP port 1182 - general network issues.	Confirm there is not firewall between the client and the server that is blocking port 1182 UDP.
Unknown connection failure	Encryption error on server.	Trigger a system report for analysis and contact technical support.
Upgrade Notification	Client received notification from server that an upgrade is available.	No action required. Upgrade will proceed automatically on the next client restart.

Event Text	Cause	Resolution
Version Mismatch	Server and client are running different versions.	Check client version and compare to server; enable Component Upgrades on the WAAS Mobile Manager Server Configuration > Advanced Settings > Upgrades page to avoid version mismatches.
Waiting to retry...	This a normal transitory state while establishing or re-establishing the connection between the client and the server.	No action required. Additional events will be presented if problems are detected.

Server Event Messages

The table below includes commonly seen messages in the **Alarms > Application > WAAS Mobile** and/or the **Home > Status** window of WAAS Mobile Manager.

Table 9 WAAS Mobile Server Event Messages

Event Text	Cause	Resolution
The server encountered an error during license validation. The license key was not found.	The license key was not found.	Make sure your license is valid, reapply it and restart the server.
The server encountered an error during license validation. The license key appears to be invalid.	The license key appears to be invalid or missing.	Make sure your license is valid, reapply it and restart the server.
The server encountered an error during license validation. The license key was not valid.	The license key was not valid.	Make sure your license is valid, reapply it and restart the server.
The server encountered an error during license validation. Unable to create network info object.	Unable to create network info object.	Make sure your license is valid, reapply it and restart the server.
The server encountered an error during license validation. Maximum number of total users in license terms exceeded in user database.	Maximum number of total users in license terms exceeded in user database.	Decrease number of users or buy more licenses.
The server encountered an error during license validation. The license key did not match required parameters.	The license key did not match required parameters, i.e. something is different on the machine from when the license was created.	Make sure your license is valid, reapply it and restart the server.

Event Text	Cause	Resolution
The server failed to initialize. Server Health Check failed at startup.	Server health check failed at startup.	Verify WAAS Mobile Manager > Server Configuration > Advanced Settings > Delta Cache settings. Check if machine is running low on disk space.
Server failed to initialize. Failed to run the proxy system manager.	Failed to run the proxy system manager.	This is a general error in response to a more specific one. Make note of any error events prior to this in the Windows Event Viewer. View server log (if enabled) for more information.
Server failed to initialize. Failed to run the server link manager.	Failed to run the server link manager.	This is a general error in response to a more specific one. Make note of any error events prior to this in the Windows Event Viewer. View server log (if enabled) for more information.
Event logging was initialized	Event logging has just been initialized.	Informational only; no action required.
The server license check succeeded.	The server license check succeeded.	Informational only; no action required.
Starting WAAS Mobile Server	The server started successfully.	Informational only; no action required.
Shutting down WAAS Mobile Server.	The server has started shutting down.	Informational only; no action required.
Generating a black box, request received from <i>usersession</i>	A black box is being generated.	Informational only; no action required.
Transport Thread Health Check Failed.	The transport thread was hung for at least 60 seconds. The server will now restart.	Informational only; no action required.
3-GB switch enabled.	The 3-GB switch happens to be enabled.	Informational only; no action required.
3-GB switch disabled.	The 3-GB switch happens to be disabled.	Informational only; no action required.
The server internet connection check failed.	The server internet connection appears to be broken.	Fix the server's internet connection.

Event Text	Cause	Resolution
Server failed to initialize. Failed to initialize the SSL proxy.	Failed to initialize the SSL proxy.	This is a general error in response to a more specific one. Make note of any error events prior to this in the Windows Event Viewer. View server log (if enabled) for more information.
Server failed to initialize. Failed to initialize the persistent delta.	Failed to initialize the persistent delta.	Verify settings are correct under WAAS Mobile Manager Server Configuration > Advanced Settings > Delta Cache . Check if machine is running low on disk space.
Server failed to initialize. Server Health Check failed at startup.	Server health check failed at startup.	Verify settings are correct under WAAS Mobile Manager Server Configuration > Advanced Settings > Delta Cache . Check if machine is running low on disk space.
Server failed to initialize. Failed to run the proxy system manager.	Failed to run the proxy system manager.	This is a general error in response to a more specific one. Make note of any error events prior to this in Windows Event Viewer. View server log (if enabled) for more information.
Server failed to initialize. Failed to run the server link manager.	Failed to run the server link manager.	This is a general error in response to a more specific one. Make note of any error events prior to this in Windows Event Viewer. View server log (if enabled) to see if there is any more information.
The server encountered an error during license validation. The license key was not found.	The license key was not found.	Make sure your license is valid, reapply it and restart the server.
The server encountered an error during license validation. The license key appears to be invalid.	The license key appears to be invalid or missing.	Make sure your license is valid, reapply it and restart the server.

Event Text	Cause	Resolution
The server encountered an error during license validation. The license key was not valid.	The license key was not valid.	Make sure your license is valid, reapply it and restart the server.
The server encountered an error during license validation. Unable to create network info object.	Unable to create network info object.	A memory error occurred while trying to verify the license key. Verify that the server has sufficient memory available, and restart.
The server encountered an error during license validation. Maximum number of total users in license terms exceeded in user database.	Maximum number of total users in license terms exceeded in user database.	Decrease number of users or buy more licenses.
The server encountered an error during license validation. The license key did not match required parameters.	The license key did not match required parameters, i.e. something is different on the machine from when the license was created.	In the WAAS Mobile Manager Home > Licensing page, verify the key displayed exactly matches the key that was issued.
The WAAS Mobile Manager encountered a run error. Failed to initialize the FIF Config.	A memory error occurred while trying to initialize the configuration subsystem.	Verify that the server has sufficient memory available, and restart.

Chapter 9 System Status Reports

System status reports are used by Cisco support technicians and software engineers when in-depth system analysis is required for problem isolation. These reports include system state as well as a brief history up to the point in time when the system report was generated. In the unlikely event the WAAS Mobile client crashes, it will trigger a report automatically.

System reports may also be triggered manually from the server or any of the client computers. This is often helpful when system anomalies are observed. Reports generated from a client computer will include the status of the server.

Generating a System Report from a Client Computer

1. Right-click the acceleration icon in the system tray.

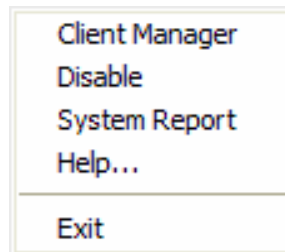


Figure 60 WAAS Mobile System Tray Icon Menu

2. There are two ways to generate a system report from the menu list.
 - 2.1. Click **System Report**.
 - 2.2. Click **Client Manager**, select the **Support** tab and click on **Send System Report**.

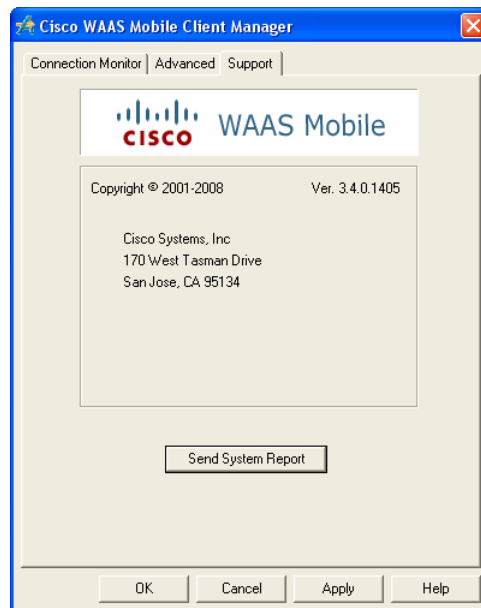


Figure 61 Client Manager – Support Tab

3. When the **Cisco WAAS Mobile: Description and Additional Information** window appears:
 - 3.1. Enter any information that could be helpful in diagnosing the situation you have encountered, including a description of the problem and what you were doing when the problem occurred. If the issue involves the transmission of a particular file, select **Add File** to attach the file to the System Report (multiple files may be attached).
 - 3.2. When finished, click **Send Report** and the system report will be sent to the server where it can be downloaded along with the matching server-side report. All system reports can be retrieved from **WAAS Mobile Manager > Home > System Reports** page. By default, system reports can also be found in the following directory: C:\Documents and Settings\All Users\Application Data\Cisco\Inbox.

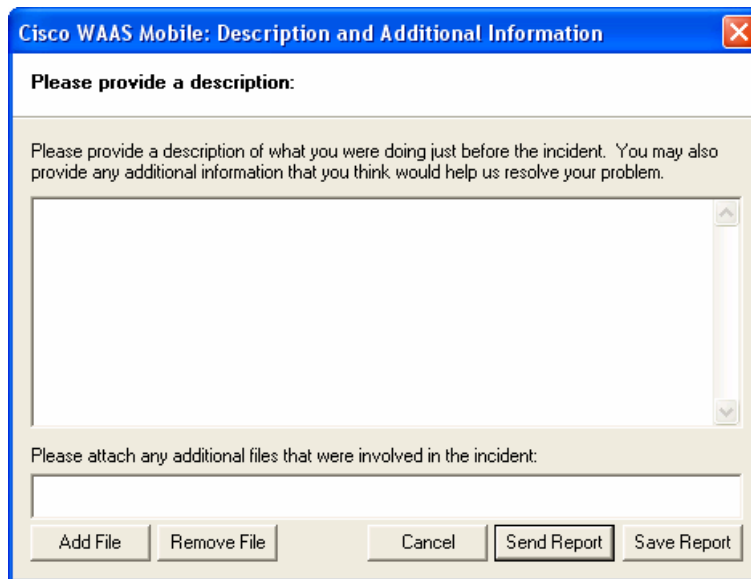


Figure 62 System Report – Additional Information

Generating a System Report from the WAAS Mobile Server

There are two options for generating system reports from the WAAS Mobile server:

1. From the WAAS Mobile Manager **Home > Status** page, click **Send System Report** to generate a server status report.
2. From the WAAS Mobile Manager **Home > Active Sessions** page, select one or more users and click **Trigger System Report** to generate reports for the server and selected clients.

If system reports cannot be sent to the WAAS Mobile server, they may be saved locally on the client's PC by choosing **Save Report** on the **Product Description and Additional Info** screen.

Chapter 10 List of Acronyms

Acronym	Definition
API	Application Programming Interface
ASP	Active Server Page(s) (Microsoft web scripting language and file extension)
CGI	Common Gateway Interface (web scripting facility)
CIFS	Common Internet File Services (Microsoft)
DNS	Domain Name Service/System
DSN	Data Source Name (database source)
EVDO	Evolution Data Only (optional version of CDMA 2000)
FTP	File Transfer Protocol
GB	Gigabyte
GBE	Gigabit Ethernet (IEEE 802.3z-1998)
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol (world wide web protocol)
HTTPS	Hyper Text Transfer Protocol over SSL
IMAP4	Internet Messaging Access Protocol 4 (Netscape)
IML	Information Markup Language
IP	Internet Protocol
IIS	Internet Information Services (Microsoft)
IT	Information Technology
ITP	Intelligent Transport Protocol
LAN	Local Area Network
LSP	Layered Service Provider
MAPI	Microsoft Outlook Messaging API
MSSQL	Microsoft SQL Server
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card (PC Ethernet network card)
NLA	Network Location Awareness
NTFS	New Technology File System (Microsoft Windows NT/2000/XP)
ODBC	Open Database Connectivity
OS	Operating System
PC	Personal Computer

Acronym	Definition
POP3	Post Office Protocol version 3 (Internet email protocol)
RAID	Redundant Array of Independent Disks
RAM	Random-Access Memory
RDBMS	Relational Database Management System
RDP	Remote Desktop Protocol
RPM	Revolutions Per Minute
RRAS	Routing and Remote Access Service
RTT	Round-Trip Time
SMB	Server Message Block (protocol)
SMTP	Simple Mail Transfer Protocol (internet email)
SNMP	Simple Network Management Protocol
SQL	Structured Query Language (database query language)
SSL	Secure Sockets Layer (Netscape; web security protocol)
TAC	Technical Assistance Center
TCP	Transmission Control Protocol
UDP	Universal Datagram Protocol
URL	Uniform Resource Locator (world wide web address)
UTC	Coordinated Universal Time (Greenwich Mean Time, GMT)
VoIP	Voice Over IP
VPN	Virtual Private Network
WAAS	Wide Area Application Services
WAE	Wide Area Application Engine
WAN	Wide Area Network
WiFi	Wireless Fidelity (IEEE 802.11b wireless networking)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCVP, Cisco Eos, 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, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, 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. (0801R)

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.

Cisco WAAS Mobile Administration Guide

© 2008 Cisco Systems, Inc. All rights reserved.