Cisco WAAS Mobile Administration Guide

Software Version 3.3.4
March 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-15416-02

Contents

About This Document **2**
Intended Audience 2
Document Outline 2
Related Documents 4
Chapter 1 System Requirements **5**
Software Compatibility 5
Chapter 2 Cisco WAAS Mobile Quick Start **7**
Chapter 3 Installing the Cisco WAAS Mobile Server **8**
Pre-Installation System Check 8
Installing 9
Entering the License Key 12
Uninstalling 13
Chapter 4 Creating and Installing the Cisco WAAS Mobile Client **14**
Creating a Client Distribution 14
Configuring a Client Distribution 15
Testing a Client 25
Manage Existing Client Distributions 27
Chapter 5 Configuring the Cisco WAAS Mobile Server **28**
Licensing 28
Authentication 28
Logging 29
Server Farm 31
Advanced Settings 31
System Reports Settings 35
Import/Export 37
Chapter 6 Managing Cisco WAAS Mobile **38**
Server Control 38
System Alarms 39
Monitoring 39
Active Session Reports 41
Session History 43
Checking Server Events 45
System Reports 46
Table of Figures **48**

About This Document

Intended Audience

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

- installing, configuring, and monitoring the Cisco WAAS Mobile Server
- packaging, distribution, and installing Cisco WAAS Mobile client on end user machines
- providing support for Cisco WAAS Mobile end users

Document Outline

The guide will discuss the following topics:

- *System Requirements*, which details all hardware and software requirements for optimal operation of the Cisco WAAS Mobile system
- *Cisco WAAS Mobile Quick Start*, outlining the minimal installation procedure for Cisco WAAS Mobile Server and Client software
- *Installing the Cisco WAAS Mobile Server*, describing all administrator operations for the Cisco WAAS Mobile Server
- *Creating and Installing the Cisco WAAS Mobile Client*, providing detailed instructions for creating, configuring, testing, and managing client software distributions
- *Configuring the Cisco WAAS Mobile Server*, which addresses the available features in the Server Configuration section of the Cisco WAAS Mobile Manager feature of Cisco WAAS Mobile
- *System Reports Settings*
- *Cisco* WAAS Mobile has a sophisticated diagnostic system which sends 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. These reports can be analyzed by Cisco TAC to validate the network configuration and to confirm that the expected performance gain is being achieved.

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 in the Cisco WAAS Mobile user interface.
- ***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 Cisco 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 UserName 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 TAC using a custom support tool, but a version of this tool will be available as a support download in the near future.

Triggering System Reports

There are a few different 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 Cisco WAAS Mobile client and server machines.
- By the administrator via Cisco WAAS Mobile Manager's Home Page. This triggers a report from the Cisco WAAS Mobile Server only.
- By the administrator for a specified client machine or machines via Cisco WAAS Mobile Manager's Active Session Management. This triggers a report from both Cisco WAAS Mobile client and server machines.

System Reports Configuration

Figure 25 System Reports Settings

System Reports URL	A value of "default" indicates that the system report server will be this Cisco WAAS Mobile Server for system reports generated by the server and any clients connecting to it. This should not be changed unless an administrator is setting up a centralized system report server. If this is the case, the URL in this field should have the form of a CGI URL up to and including the question-mark after the CGI executable name.
System Reports Directory	Configure the directory for the System Reports inbox here if something other than the default is desired.
Run daily cleanup at	The time at which a daily cleanup is run to delete System Report files older than the configured (below) number of days.
Delete files older than x days	System Report files older than the value (in days) specified here are deleted when the daily cleanup occurs.

System Reports are downloaded from the System Reports page under Home.

Import/Export

Exporting and Importing settings enables system administrators to backup and restore Cisco WAAS Mobile Server configuration when migrating to new server hardware or upgrading.

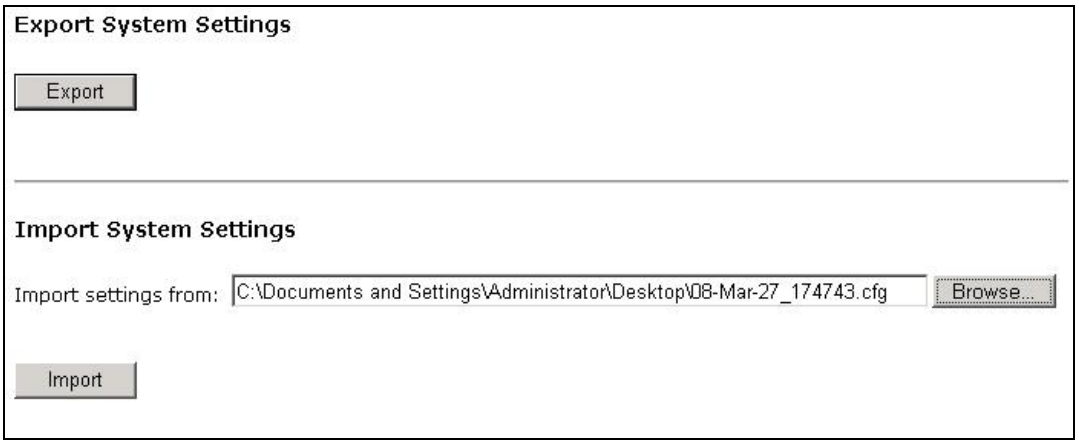


Figure 26 Import/Export Settings

Export	Click this to export. Respond to the file download dialog to save or open the configuration file.
Import Settings from:	Use this to browse to the location of the settings to be imported.
Import	Click this to import from the specified location.

- Managing , which addresses the available features in the Server Monitoring section of the Cisco WAAS Mobile Manager feature of Cisco WAAS Mobile

Related Documents

In addition to this Administrator's Guide which is the main Cisco WAAS Mobile product 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 Cisco WAAS Mobile Server. It provides detailed discussion of aspects of deployment such as firewalls, network topology, authentication and accounting.
- Cisco WAAS Mobile *User Guide* – A guide for the Cisco WAAS Mobile end user. This complements the on-line help system and provides a reference for offline study.
- *Product Technical Specifications* – Documents applications Cisco WAAS Mobile accelerates such as web browsers, email clients and other web-enabled applications. This document also lists the features of Cisco WAAS Mobile Client and Server.
- *Release Notes* – Release-specific information regarding features added, changed, and removed as well as known issues and issues fixed in the release.

Chapter 1 System Requirements

This section details all hardware and software requirements for ultimate performance of the Cisco WAAS Mobile system.

Table 1 Server System Requirements

	Minimum
Operating System	Windows Server 2003 R2 Standard SP2
CPU	Dual Core 1.8GHz
System Memory (RAM)	2GB
Hard Drive	80GB 7.2K RPM
Interface	Dual 1GBE NIC card

Table 2 Client System Requirements

	Minimum	Recommended
Operating System	Windows 2000 and later	Windows 2000 and later
CPU	750MHz	1.5GHz
System Memory (RAM)	256MB	512MB
Disk Space Available	80MB	1 GB

Table 3 Server Software Requirements

Cisco WAAS Mobile Server	Internet Information Server (IIS) version 6 or higher. ASP.NET v2.0 Framework. See Pre-Installation System Check in Chapter 3 below.

Table 4 Client Software Requirements

Client	Windows OS

Software Compatibility

The client software has been tested with and officially supports the following applications in the versions list. Older versions of the programs listed below as well as other software packages not listed may also work with Cisco WAAS Mobile.

Antivirus/Security Software

- 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

- Cisco VPN Client Versions: 4, 5
- Nortel Contivity VPN Client Versions: 5, 6

Chapter 2 Cisco WAAS Mobile Quick Start

The following is the minimal Cisco WAAS Mobile installation procedure:

1. Download CD distribution from link provided by Cisco
2. Provision server machine (see System Requirements).
3. Install server software.
   3.1. Verify that IIS is installed and running.
   3.2. Run AutoRun.exe from downloaded software distribution for installation menu.
   3.3. Review release notes from AutoRun menu.
   3.4. From AutoRun menu, install Cisco WAAS Mobile Manager (web-based administrator program).
   3.5. From AutoRun menu, install Cisco WAAS Mobile Server.
   3.6. In Internet Explorer, go to http://127.0.0.1/WAASMobile on the server machine to validate that server is installed properly and tour Cisco WAAS Mobile Manager.
4. Configure server via Cisco WAAS Mobile Manager.
   4.1. Click on Server Configuration, then copy and paste the license number sent in license.dat attachment and click Submit.
   4.2. Go to the Home page in Cisco WAAS Mobile Manager.
   4.3. Click Start Server.
5. Create client software distribution.
   5.1. Go to Client Configuration in Cisco WAAS Mobile Manager.
   5.2. Enter the IP or DNS host name of the server.
   5.3. Enter a name for the distribution.
   5.4. Click Create.
   5.5. Click Download.
   5.6. Save ClientDistribution.cab file
   5.7. Use a utility to extract the cab files to a folder. Note that all files must be extracted, not just the ClientSetup.exe.
6. Install the client software on test client machine.
   6.1. Begin client install by running ClientSetup.exe. Follow the instructions in the installation wizard to continue the installation.
   6.2. After restart, the client software will be running in the background and will automatically find and connect to the Cisco WAAS Mobile Server.
7. Test enterprise applications with and without Cisco WAAS Mobile.
   7.1. After "with Cisco WAAS Mobile" test case, you may want to send diagnostic info to Cisco via the Send System Report button on the Support tab so that Cisco can validate the network configuration and confirm that you are getting the expected performance gain.

Chapter 3 Installing the Cisco WAAS Mobile Server

This chapter describes procedures an administrator will need to use in order to install and maintain the Cisco WAAS Mobile system. To perform the procedures in this section, you must be logged into the server computer as a user with Administrator privileges.

This chapter contains the following sections.

- Pre-Installation System Check
- Installing
- Entering the License Key
- Uninstalling

Pre-Installation System Check

1. Verify that the computer on which you intend to install the server software meets the system requirements listed in System Requirements.

2. For Accelerated Folders, the server machine must be configured to resolve the network names used by its clients to access remote file servers. Optionally, for better performance disable NetBIOS over TCP/IP.

3. Do not run other applications, including the client software, on the Cisco WAAS Mobile Server machine. If anti-virus software is installed on the server, it must be configured to allow outgoing ports that Cisco WAAS Mobile Server may use (e.g., SMTP ports).

Installing

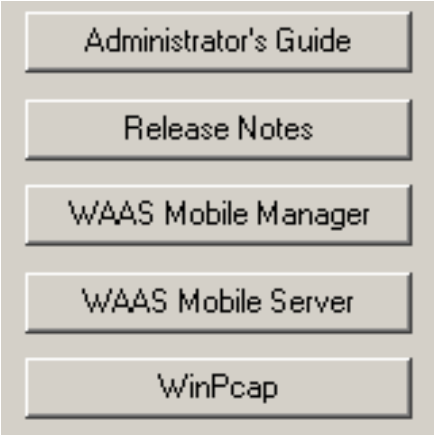


Figure 1 AutoRun Dialog Buttons

Follow these steps to install Cisco WAAS Mobile Server.

1. Start Autorun.exe.
2. Read the Release Notes.
3. Install Cisco WAAS Mobile Manager. If prompted, install SQLite Database Management System and .NET Framework 2.0. On Windows XP, ensure that .NET Framework 2.0 is registered and that IIS is configured to allow it to run. Cisco WAAS Mobile Manager installer sets IIS to use only NTLM authentication.
4. Install Cisco WAAS Mobile Server.
5. When installation completes, a browser window will open and display the Cisco WAAS Mobile Manager home page. *It may take some time to load the page for the first time.*
6. Enter the license key as described in the next section.
7. If this server is being installed in a testing environment, install the WinPcap library. This will automatically include packet captures in diagnostic information.

Cisco WAAS Mobile administration with Cisco WAAS Mobile Manager is covered below under

- Creating and Installing the Cisco WAAS Mobile Client
- Configuring the Cisco WAAS Mobile Server

System Reports Settings

Cisco WAAS Mobile has a sophisticated diagnostic system which sends 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. These reports can be analyzed by Cisco TAC to validate the network configuration and to confirm that the expected performance gain is being achieved.

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 in the Cisco WAAS Mobile user interface.
- ***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 Cisco 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 UserName 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 TAC using a custom support tool, but a version of this tool will be available as a support download in the near future.

Triggering System Reports

There are a few different 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 Cisco WAAS Mobile client and server machines.
- By the administrator via Cisco WAAS Mobile Manager's Home Page. This triggers a report from the Cisco WAAS Mobile Server only.
- By the administrator for a specified client machine or machines via Cisco WAAS Mobile Manager's Active Session Management. This triggers a report from both Cisco WAAS Mobile client and server machines.

System Reports Configuration

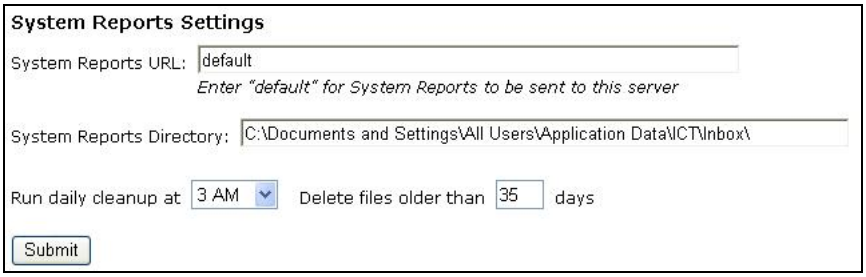


Figure 25 System Reports Settings

System Reports URL	A value of "default" indicates that the system report server will be this Cisco WAAS Mobile Server for system reports generated by the server and any clients connecting to it. This should not be changed unless an administrator is setting up a centralized system report server. If this is the case, the URL in this field should have the form of a CGI URL up to and including the question-mark after the CGI executable name.
System Reports Directory	Configure the directory for the System Reports inbox here if something other than the default is desired.
Run daily cleanup at	The time at which a daily cleanup is run to delete System Report files older than the configured (below) number of days.
Delete files older than x days	System Report files older than the value (in days) specified here are deleted when the daily cleanup occurs.

System Reports are downloaded from the System Reports page under Home.

Import/Export

Exporting and Importing settings enables system administrators to backup and restore Cisco WAAS Mobile Server configuration when migrating to new server hardware or upgrading.

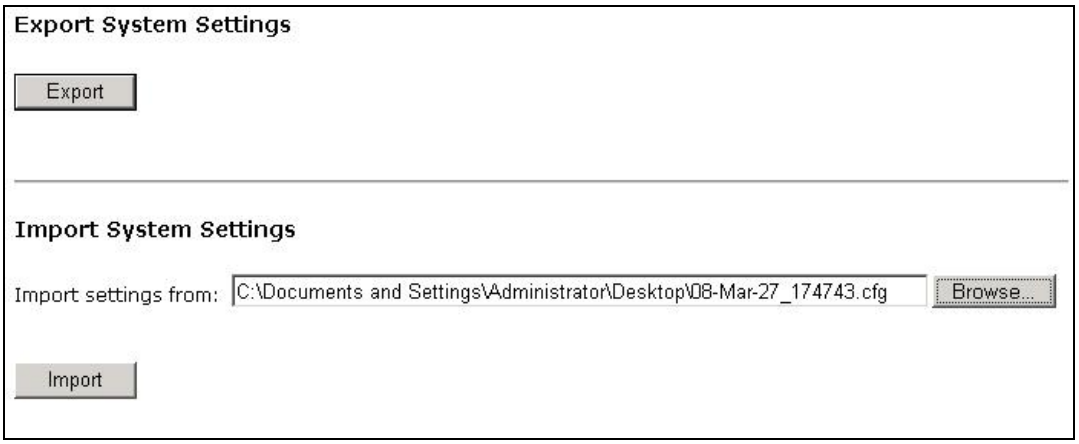


Figure 26 Import/Export Settings

Export	Click this to export. Respond to the file download dialog to save or open the configuration file.
Import Settings from:	Use this to browse to the location of the settings to be imported.
Import	Click this to import from the specified location.

- Managing

Entering the License Key

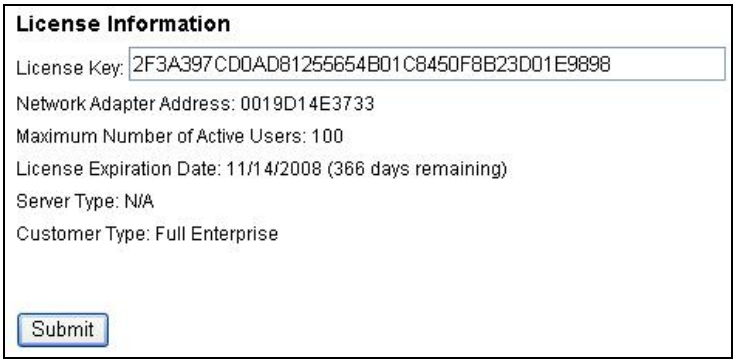


Figure 2 License Information

Obtain a license key by sending the Network Adapter Address of one of the NIC cards installed on the server machine to the vendor.

IMPORTANT: If your server is running on a virtual machine you must make sure the Network Adapter Addresses do not change or your license key may fail to work.

Select Server Configuration in the menu at the top of Cisco WAAS Mobile Manager to display the Licensing page.

Enter the license key in the appropriate field and click Submit. Entering the license key requires a server start/restart which can be done by navigating to Cisco WAAS Mobile Manager's Home page and clicking Start/Restart Server.. For full information on licensing schemes see the Licensing Schemes section of the Cisco WAAS Mobile Integration Guide.

Uninstalling

To uninstall the server, follow these steps:

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 will be removed from the system.
4. Do the same for Cisco WAAS Mobile Manager if desired.

NOTE: Use the above Uninstalling and Installing instructions when upgrading the server and Cisco WAAS Mobile Manager to a newer version.

Chapter 4 Creating and Installing the Cisco WAAS Mobile Client

To create a client distribution, go to the Client Configuration section of Cisco WAAS Mobile Manager.

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

This chapter contains the following sections:

- Creating a Client Distribution
- Configuring a Client Distribution
- Testing a Client
- Manage Existing Client Distributions

Creating a Client Distribution

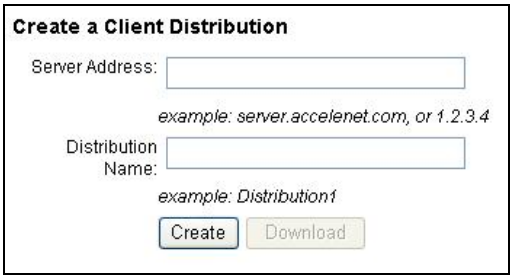


Figure 3 Client Distribution Creation

Enter the IP or DNS host name of the Cisco WAAS Mobile Server. The client uses this to establish an acceleration tunnel to the server. Enter a name to be given to the distribution.

Upon clicking Create, a message will say, "New distribution created successfully. Click Download to download the new distribution." Click download to bring up a dialog asking whether to open or save the file. The distribution created will have Cisco WAAS Mobile's default settings.

The downloaded distribution is in cab file form. Use a utility to extract the file ClientDistribution.cab. Note that all files must be extracted, not just the file ClientSetup.exe.

The administrator decides what method of distributing the client software is appropriate for their deployment. Options include burning the files to a CD to manually install the software or using a systems management tool for distribution.

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

Configuring a Client Distribution

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

- Network Settings
- User Interface Settings
- Bypass Settings
- HTTPS Settings
- Exclusion Lists Settings
- Acceleration Routing Table
- Proxied Process List
- File Shares Settings

Network Settings

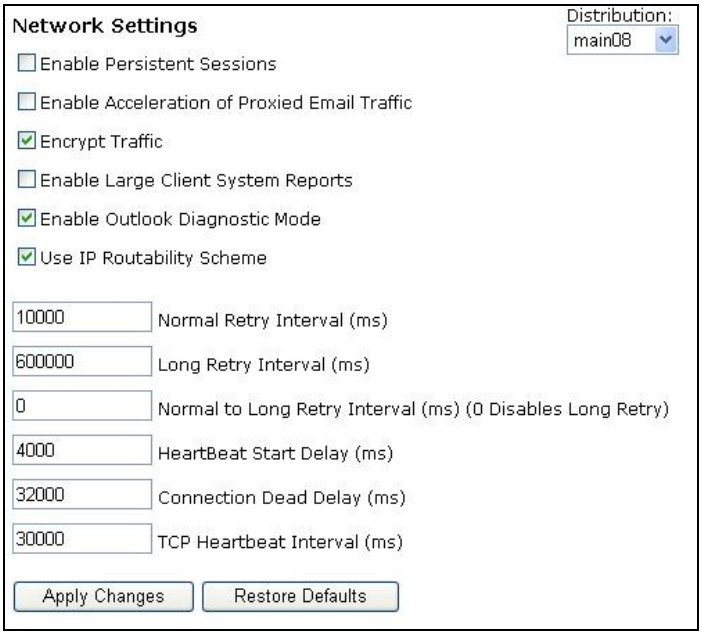


Figure 4 Network Settings

Enable Persistent Sessions	This setting controls whether or not Persistent Sessions functionality will be enabled on the client by default. The end user can always disable persistent session functionality via the client user interface, as described in the Cisco WAAS Mobile User Guide and online Help. The Persistent Sessions feature maintains acceleration sessions even when web connectivity is lost or when a mobile client switches to a different network such as from WiFi to cellular. When connectivity is restored, the current session is sustained to create a seamless access experience regardless of the changes in the underlying network structure. Downloads and uploads are resumed without loss of data, and no additional log-ins are required. For more information on Persistent Sessions see the Cisco WAAS Mobile Integration Guide under Cisco WAAS Mobile Persistent Sessions.
Enable Acceleration of Proxied Email Traffic	This setting causes Cisco WAAS Mobile to attempt to accelerate email that is passing through virus scanning software. The software automatically detects that a given connection is being intercepted by a locally running virus scanner and lets the connection pass. Cisco WAAS Mobile then redirects the connection to the destination email server and redirects it into the acceleration tunnel. This option allows Cisco WAAS Mobile to interoperate transparently with other applications that perform local and transparent redirection of smtp/pop3 traffic – typically email virus scanners.
Encrypt Traffic	Enables SSL traffic encryption.
Enable Large Client System Reports	Enables system reports of more advanced detail for diagnostic purposes. This setting should be used in coordination with Cisco TAC support.
Enable Outlook Diagnostic Mode	Enables a diagnostic mode for System Reports that has advanced information on Outlook.
Use IP Routability Scheme	If this feature is enabled, Cisco WAAS Mobile detects destination servers that are not accessible through the Cisco WAAS Mobile Server so that they are bypassed. If a client system is connected to the Internet via a high-latency connection, but is also connected to a LAN, when the client tries to connect to another system on the LAN, that traffic will not go through the Cisco WAAS Mobile Server. The IP Routability scheme detects this situation and bypasses the local traffic.
Normal Retry Interval	This controls the frequency of reconnect attempts to the server (in milliseconds).
Long Retry Interval	This controls the frequency of reconnect attempts to the server after the Normal to Long Interval has expired if it is non-zero (in milliseconds).

Normal to Long Retry Interval	Allows Cisco WAAS Mobile to decrease the frequency of attempts to connect to an unreachable server. After the interval (in milliseconds), frequency of attempts goes to Long.
HeartBeat Start Delay	The client and server periodically send heartbeat packets to each other. These are used to detect when the link has failed. Heartbeat Start Delay specifies the interval between heartbeats (in milliseconds).
Connection Dead Delay	If the receiver does not receive any packets within this interval (in milliseconds), the receiver assumes the link is dead.
TCP Heartbeat Interval	In some modes of operation, Cisco WAAS Mobile maintains a TCP control connection throughout the session to provide faster response if client or server disconnects (in milliseconds).

User Interface Settings

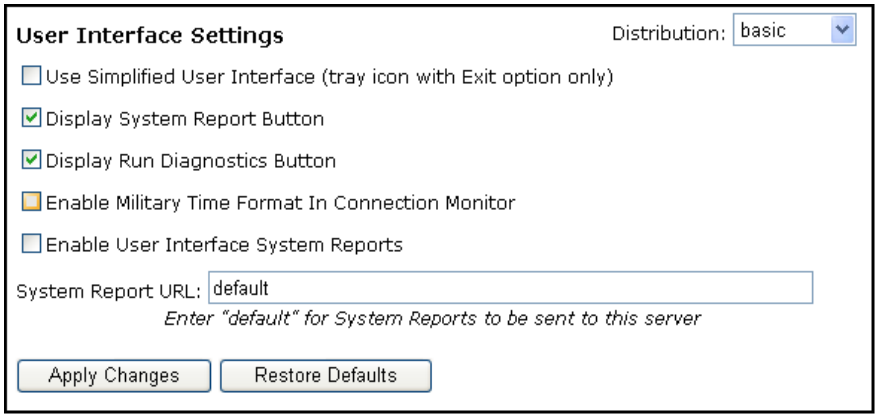


Figure 5 Client User Interface Settings

Use Simplified User Interface	If this box is checked, the client user interface is simplified to just a tray icon with an exit option
Display System Report Button	If this box is checked, the System Report button will appear in the Support dialog box of the client application user interface.
Display Run Diagnostics Button	If this box is checked, the Run Diagnostics button will appear in the Support dialog box of the client application user interface.
Enable Military Time Format In Connection Monitor	If this box is checked, the time displayed in the Connection Monitor of the client application user interface will be displayed in military time.
System Report URL	This is the URL for sending System Reports. It has the form of a CGI URL up to and including the question-mark after the CGI executable name. It is relevant for the end user only if the box for Display System Report Button is checked. This URL should not be changed unless the administrator is configuring his or

her own separate System Report server.

Bypass Settings

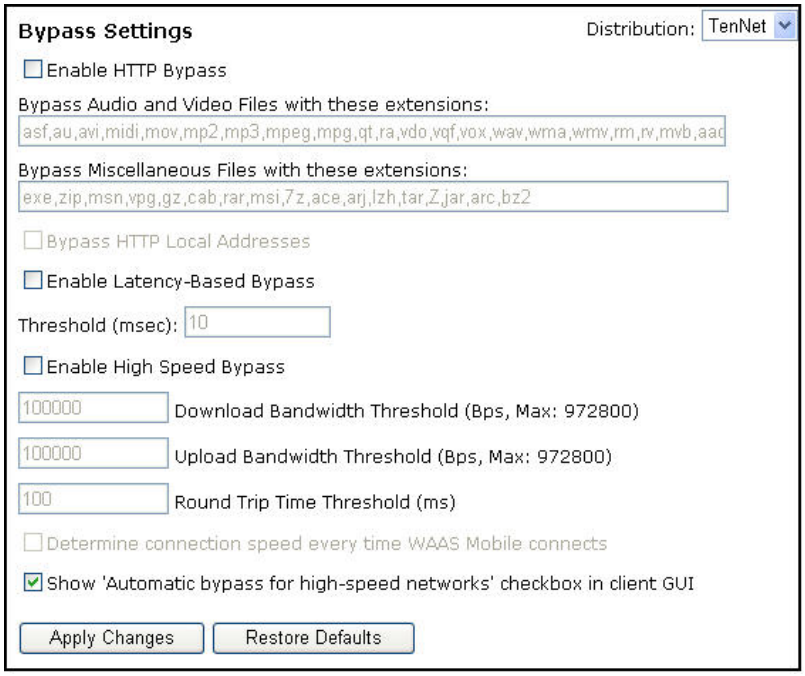


Figure 6 Bypass Settings

Enable HTTP Bypass	To specify certain file types that 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.
Bypass Audio and Video Files	List the extensions of the audio and video file types to be bypassed here.
Bypass Miscellaneous Files	List the extensions of any other file types to be bypassed here.
Bypass HTTP Local Addresses	If enabled, HTTP traffic to local Intranet web servers will not be accelerated.
Enable Latency-Based Bypass and Threshold	The Latency-Based Bypass feature allows Cisco WAAS Mobile to accelerate individual TCP connections if the latency of the network between the client machine and the destination server exceeds the Threshold value in milliseconds.
Enable High Speed Bypass	If checked, high-speed connections as determined by Threshold settings discussed below will take effect.

Threshold Settings	The three threshold values are: ▪ Download Bandwidth Threshold ▪ Upload Bandwidth Threshold ▪ Round Trip Time Threshold These are used to determine if a connection is high-speed. 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 Cisco 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." We recommend this checkbox remain unchecked unless Cisco WAAS Mobile will be 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.
Show 'Automatic bypass for high-speed networks' checkbox in client GUI	This selection enables a checkbox to appear on the Setup tab under Options in the client's menu and gives the client the option to decide whether to automatically bypass (i.e., not proxy TCP connections through Cisco WAAS Mobile) for high-speed networks.

HTTPS Settings

Figure 7 HTTPS Settings

Enable HTTPS Acceleration	To enable HTTPS acceleration (for Internet Explorer only) check the Enable HTTPS Acceleration checkbox. By default, HTTPS is not accelerated. Cisco WAAS Mobile provides a secure proxy for SSL traffic. This enables SSL traffic to be compressed, just like other non-secure traffic, without compromising security.
Accelerate All HTTPS Sites	All HTTPS traffic will be accelerated if this radio button is selected.
Accelerate Host Inclusion List Only	HTTPS acceleration is typically an enterprise-only feature. The reason for this is that individual enterprises will choose to allow their users to accelerate enterprise encrypted SSL traffic explicitly, giving Cisco WAAS Mobile express permissions to act as a proxy for enterprise encrypted data. This can be done by selecting

	Accelerate Host Inclusion List Only and adding HTTPS servers to the Host Inclusion List. Only hosts listed in the Host Inclusion List will be accelerated. Use the buttons Add, Remove, and Remove All to create the list, and then use Apply Changes to save the changes. Use Restore Defaults to return to the default settings. For more information see the Cisco WAAS Mobile Integration Guide under HTTPS Optimization.
Process Acceleration List	Select from the Proxied Process List drop down menu the processes to which HTTPS acceleration is to apply. iexplorer.exe and explorer.exe are HTTPS accelerated automatically if HTTPS acceleration is enabled.

Exclusion Lists Settings

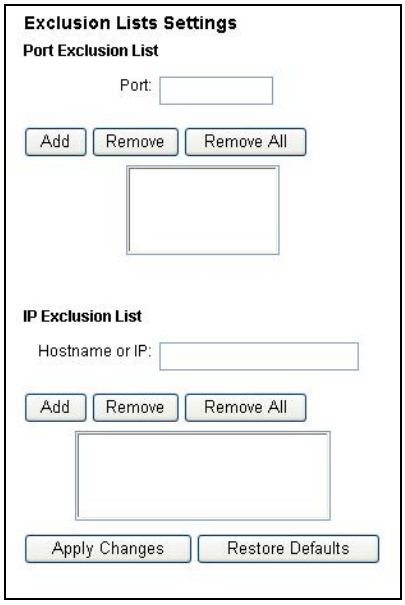


Figure 8 Exclusion Lists Settings

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. Create the exclusion list with the Add, Remove and Remove All buttons.
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.

Acceleration Routing Table

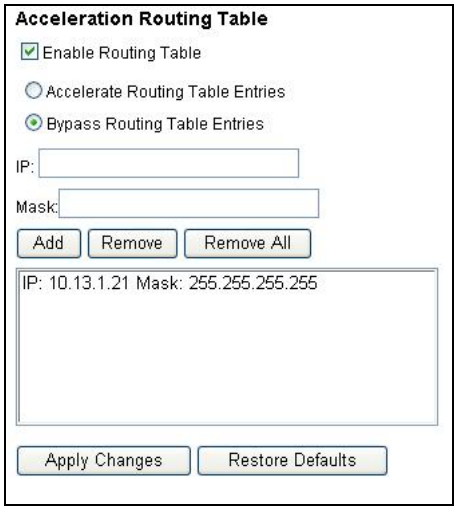


Figure 9 Acceleration Routing Table

Enable Routing Table	Check the box to enable acceleration of traffic to and from specific networks. The default is for acceleration routing to be off.
Accelerate Routing Table Entries	If this radio button is selected, all the entries in the table are accelerated.
Bypass Routing Table Entries	If this radio button is selected, all entries in the table below will be bypassed.
IP	Enter an IP address for the routing table.
Mask	Enter a network mask in dotted-decimal form to identify the subnet. The Acceleration Routing table is a complete IP-based routing table. Each entry includes a network IP and a subnet mask; entries are read prior to establishing a server session when checked; the feature is off by default. The routing table can either specify destination networks which should be accelerated, or those which should be bypassed. When Accelerate Routing Table Entries is selected, a connection matching an entry in the routing table will be accelerated. If a matching entry does not exist, the connection will be bypassed. If Bypass Routing Table Entries is selected then a connection matching an entry in the routing table will be bypassed, not accelerated. If a matching entry does not exist, the connection will be accelerated.

Proxied Process List

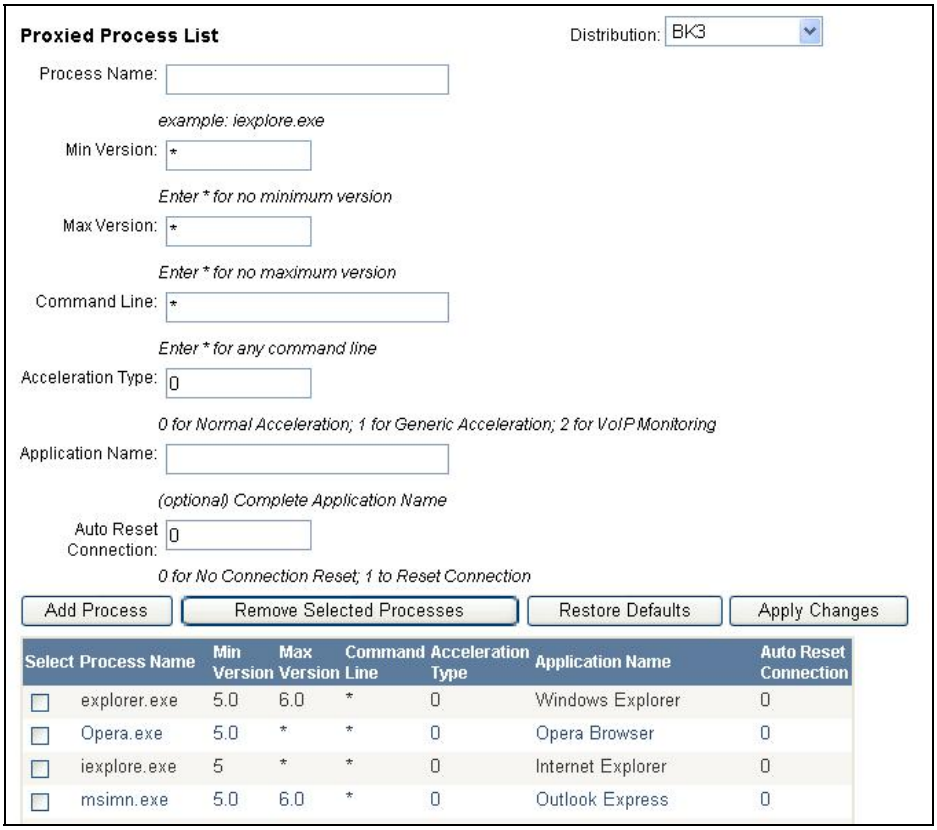


Figure 10 Proxied Process List

Cisco WAAS Mobile uses the Proxied Process List to determine which applications are to be accelerated.

Add Process	Enter the process details in the text boxes provided. Click Add Process. Click Apply Changes.
Remove Selected Processes	Select one or more processes for removal by checking their boxes. Click Remove Selected Processes. Click Apply Changes. To edit a process, you must remove the process and then add it again with the new settings.
Restore Defaults	Click Restore Defaults. Click Apply Changes.
VoIP Monitoring	This setting can detect when a conversation occurs over a selected VoIP (Voice over IP) application and insure that accelerated network traffic does not interfere with the audio quality. Enter a 2 in the Acceleration Type field to enable this VoIP monitoring.

Auto Reset Connection	Acceleration of certain applications does not begin right away if Cisco WAAS Mobile is started or restarted after the application has been running. If the Auto Reset Connection is enabled for a given application, by entering a "1" in the Auto Reset Connection field, then when Cisco WAAS Mobile starts it will reset the connection for that application so that acceleration is instant. The client user interface has a checkbox so the user can choose whether to enable this feature for applications so configured here.

File Shares Settings

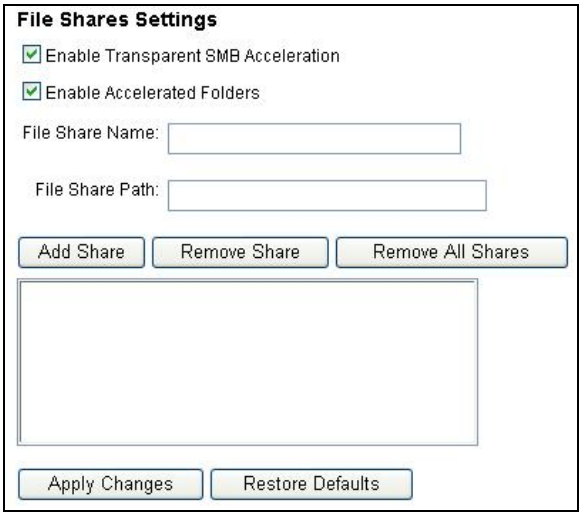


Figure 11 File Shares Settings

Enable Transparent SMB Acceleration	This checkbox enables acceleration of traffic for file shares. This is referred to as Native SMB Acceleration.
Enable Accelerated Folders	This checkbox enables the acceleration of remote file shares as Accelerated Folders. The performance of Accelerated Folders is better than that of Native SMB Acceleration but they are less convenient in some situations. Use Add Share, Remove Share and Remove All Shares buttons to configure a list of accelerated shares for users of the current client distribution. See the Cisco WAAS Mobile User Guide for more detail on configuring and using this feature.

Testing a Client

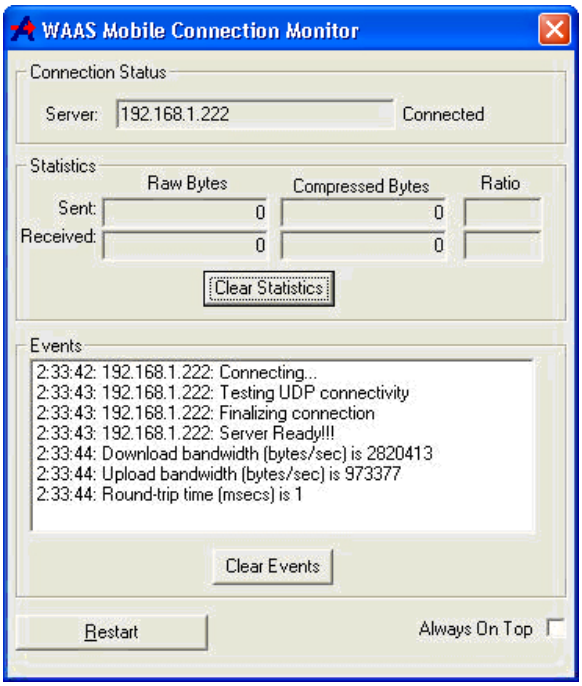


Figure 12 Connection Monitor Dialog Box

Once the client is installed, perform a quick test to make sure the client has connected to the server. If the client is connected, the Cisco WAAS Mobile Accelerated icon in the lower right system tray is lit up. If this test fails, check the client's Connection Monitor Events window as shown in Figure 12.

In the image above, the client has connected successfully. When the connection is not successful, one of the following messages may appear in the Connection Monitor's Events window. If no events show in the Connection Monitor, reboot the machine and see if that resolves the issue.

Server Not Reachable

This message usually means the server is either not running or the client has a network issue preventing it from connecting. If the server is running, ping the server address from the client machine to confirm that the problem is a network issue.

No Internet Connection Present

This message occurs if the client machine has no internet connection — for example, if the modem was not connected or if the Ethernet card was off.

Send System Report

Figure 13 Client Options Dialog – Support Tab

If a problem occurs while testing Cisco WAAS Mobile, send a System Report from the client machine. Left- or right-click the Cisco WAAS Mobile Accelerated system tray icon to display the client system menu. Select Options, then the Support tab to open the dialog window shown in Figure 13.

Click the Send System Report button. A form similar to the one below will appear:

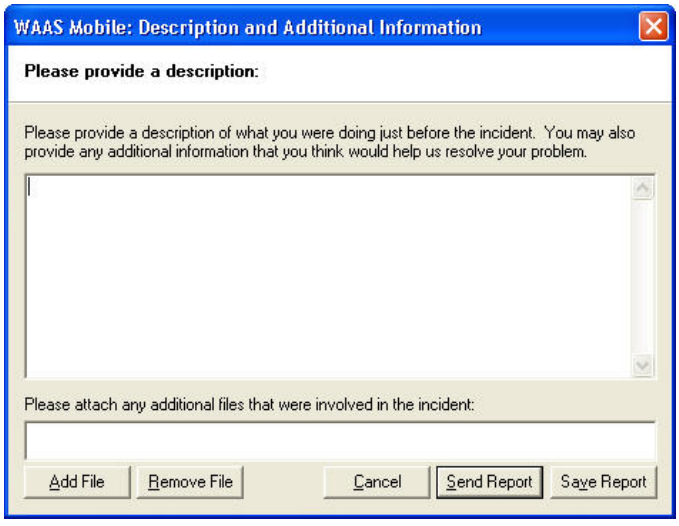


Figure 14 System Report – Adding Additional Information

Enter any information you think will be useful 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. When finished, click Send Report and the system report will be sent to Cisco TAC.

Manage Existing Client Distributions

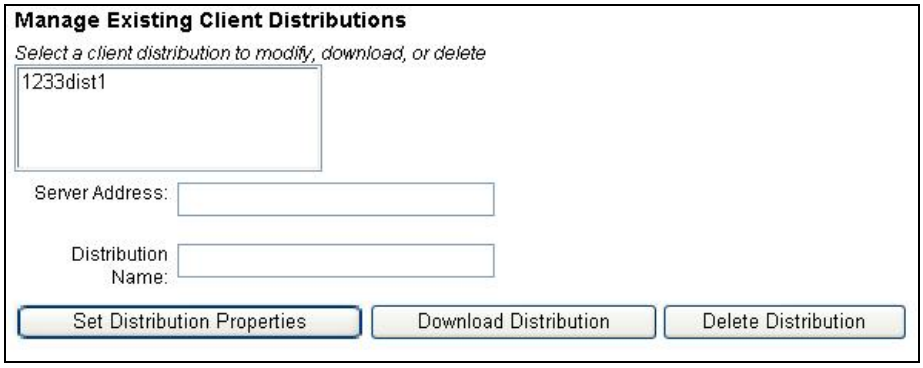


Figure 15 Managing Existing Client Distributions

On the Manage Existing Client Distributions page, a distribution can be modified, downloaded or deleted. Note that changing the Server Address and Distribution Name requires a new download of the distribution.

Once a distribution has been created, the remaining pages of Cisco WAAS Mobile Manager's Client Configuration section allow an administrator to adjust many of Cisco WAAS Mobile's settings for the end users. A drop down menu will appear in the upper right hand corner of each page to select the distribution to be viewed or modified. Note that the Apply Changes button on each page that has been modified must be clicked before navigating away from that page in order for the changes to take effect.

Chapter 5 Configuring the Cisco WAAS Mobile Server

This chapter addresses each of the areas available in the Server Configuration section of Cisco WAAS Mobile Manager.

- Licensing
- Authentication
- Logging
- Server Farm
- Advanced Settings
- System Reports
- Import/Export

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

Licensing

Licensing for Cisco WAAS Mobile is discussed in detail in the Cisco WAAS Mobile Integration Guide under Licensing Schemes.

Authentication

See the Cisco WAAS Mobile Integration Guide under Configuring User Authentication.

Logging

Logging Settings

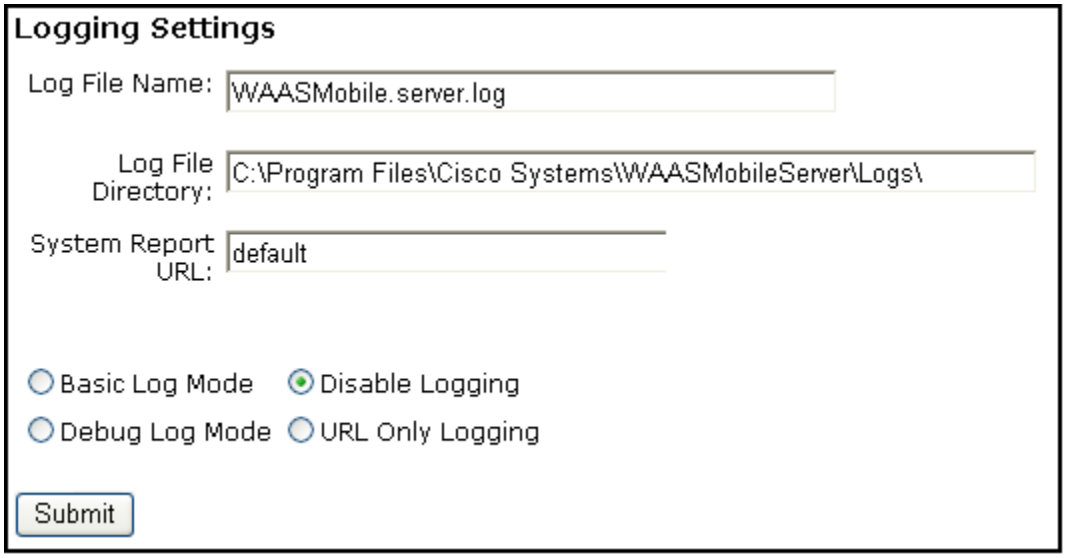


Figure 16 Logging Settings

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 for logging.
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 the URLs visited.

RDBMS Logging Settings

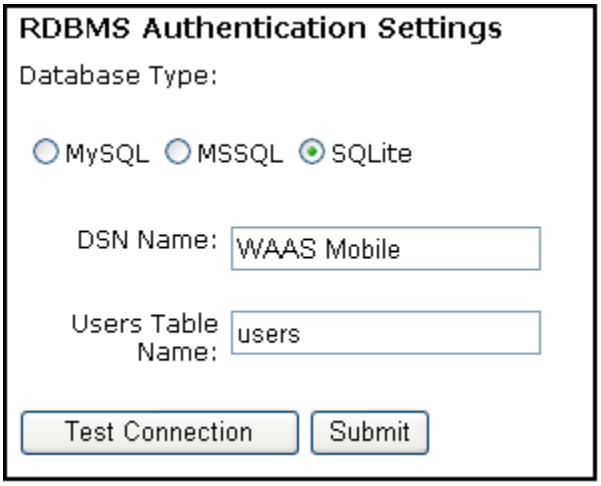


Figure 17 RDBMS Logging Settings

Enable RDBMS Logging	Check this box to enable RDBMS logging.
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.
Log Table Name	Enter the name of the table used to store logged events.
Test Connection	Click this button to verify that the database management system is accessible to Cisco WAAS Mobile Manager.

Log Rotation Settings

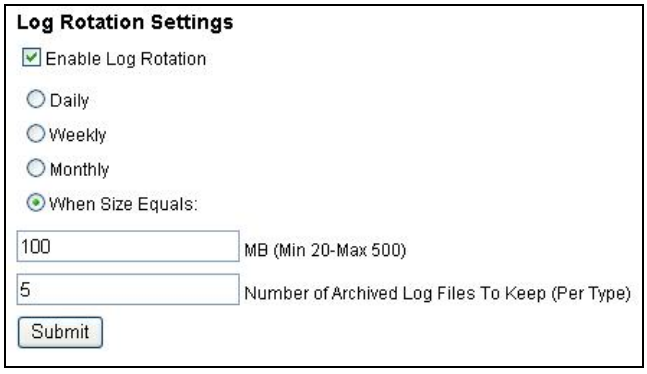


Figure 18 Log Rotation Settings

Enable Log Rotation	Check this box to enable log rotation.

Daily	Select to rotate the logs once each day.
Weekly	Select to rotate the logs once each week.
Monthly	Select to rotate the logs once each month.
When File Size Equals	Select to rotate the logs when the size of the active log file reaches the value specified in the MB text box.
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

See the Cisco WAAS Mobile Integration Guide under Advanced Server Selection.

Advanced Settings

Upstream Proxy Settings

See the Cisco WAAS Mobile Integration Guide under Upstream Server Configurations.

HTTP Prefetching Settings

Access this page using the Prefetching entry in the left-hand pane of Server Configuration.

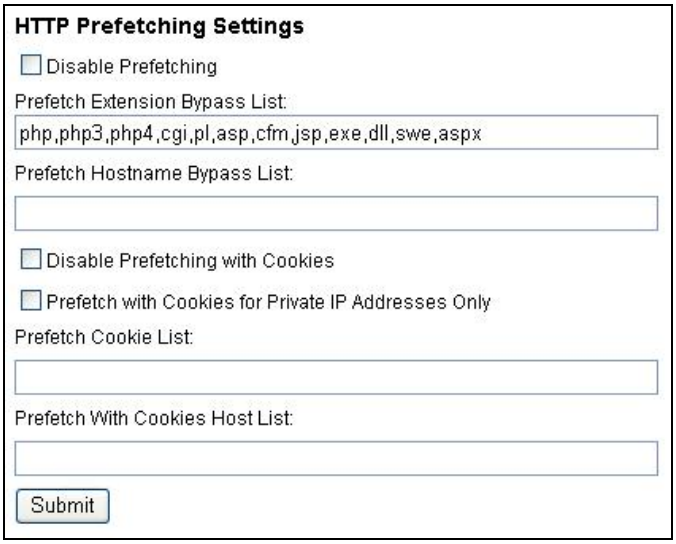


Figure 19 HTTP Prefetching Settings

Disable Prefetching	Check the box to disable all HTTP prefetching.
Prefetch Extension Bypass List	Provide a comma-separated list to prevent prefetching specific file types from all hosts.

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.
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.

Delta Cache Settings

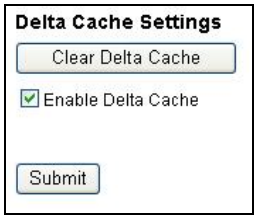


Figure 20 Delta Cache Settings

Clear Delta Cache	Click this button to clear the cache used for delta compression on the server. There is also an option for this to be done using the Clear Delta Cache button on the client user interface on the Setup tab under Options in the Cisco WAAS Mobile menu.
Enable Delta Cache	Check this to enable use of the delta cache.

Radius Accounting Settings

See RADIUS Accounting Configuration & Monitoring in the Cisco WAAS Mobile Integration Guide for details.

Set a Registry Value

Figure 21 Set a Registry Value Setting

Key	Enter the key name. HKEY_LOCAL_MACHINE\AcceleNetServer is added as a prefix to the name supplied.
Value	Enter the value. It will be interpreted according to the value type selected below.
Value Type	Select one of the radio buttons. Select DWORD for an integer and STRING for text.

Aliasing Settings

See Client IP Mapping Schemes in the Cisco WAAS Mobile Integration Guide for details.

Access Control Settings

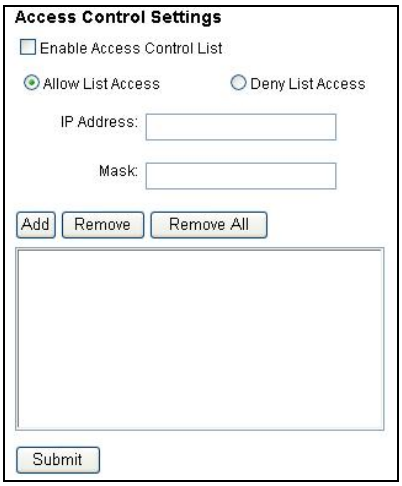


Figure 22 Access Control Settings

Enable Access Control List	This control allows administrators to specify which Client IP sub-networks should be accelerated. 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 experience acceleration. 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 Cisco WAAS Mobile completely. Clicking Deny List Access causes the list of sub-networks to serve as a "blacklist", indicating the client IP addresses that will not be accelerated.

Upgrade Settings

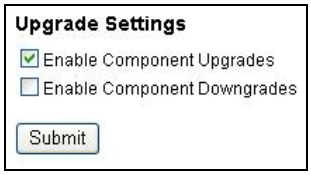


Figure 23 Upgrade Settings

Enable Component Upgrades	Check this to enable core Cisco WAAS Mobile components to be automatically upgraded when the client logs in. A client upgrade happens whenever a server is upgraded (see Installing and Uninstalling above). This setting is on by default. The client automatically restarts after a component upgrade.

Enable Component Downgrades	Check this to enable core Cisco WAAS Mobile components to be downgraded automatically when a server is downgraded (see Installing and Uninstalling above). This is off by default as servers are rarely downgraded. The client automatically restarts after a component downgrade.

Network Settings

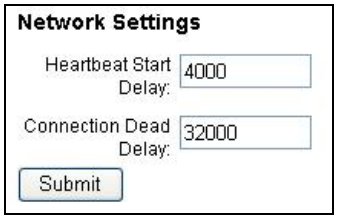


Figure 24 Network Settings

Heartbeat Start Delay	The client and server periodically send heartbeat packets to each other. These are used to detect when the link has failed. Heartbeat Start Delay specifies the interval between heartbeats (in milliseconds).
Connection Dead Delay	If the receiver does not receive any packets within this interval (in milliseconds), the receiver assumes the link is dead.

System Reports Settings

Cisco WAAS Mobile has a sophisticated diagnostic system which sends 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. These reports can be analyzed by Cisco TAC to validate the network configuration and to confirm that the expected performance gain is being achieved.

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 in the Cisco WAAS Mobile user interface.
- ***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 Cisco 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 UserName 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 TAC using a custom support tool, but a version of this tool will be available as a support download in the near future.

Triggering System Reports

There are a few different 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 Cisco WAAS Mobile client and server machines.
- By the administrator via Cisco WAAS Mobile Manager's Home Page. This triggers a report from the Cisco WAAS Mobile Server only.
- By the administrator for a specified client machine or machines via Cisco WAAS Mobile Manager's Active Session Management. This triggers a report from both Cisco WAAS Mobile client and server machines.

System Reports Configuration

Figure 25 System Reports Settings

System Reports URL	A value of "default" indicates that the system report server will be this Cisco WAAS Mobile Server for system reports generated by the server and any clients connecting to it. This should not be changed unless an administrator is setting up a centralized system report server. If this is the case, the URL in this field should have the form of a CGI URL up to and including the question-mark after the CGI executable name.
System Reports Directory	Configure the directory for the System Reports inbox here if something other than the default is desired.
Run daily cleanup at	The time at which a daily cleanup is run to delete System Report files older than the configured (below) number of days.
Delete files older than x days	System Report files older than the value (in days) specified here are deleted when the daily cleanup occurs.

System Reports are downloaded from the System Reports page under Home.

Import/Export

Exporting and Importing settings enables system administrators to backup and restore Cisco WAAS Mobile Server configuration when migrating to new server hardware or upgrading.

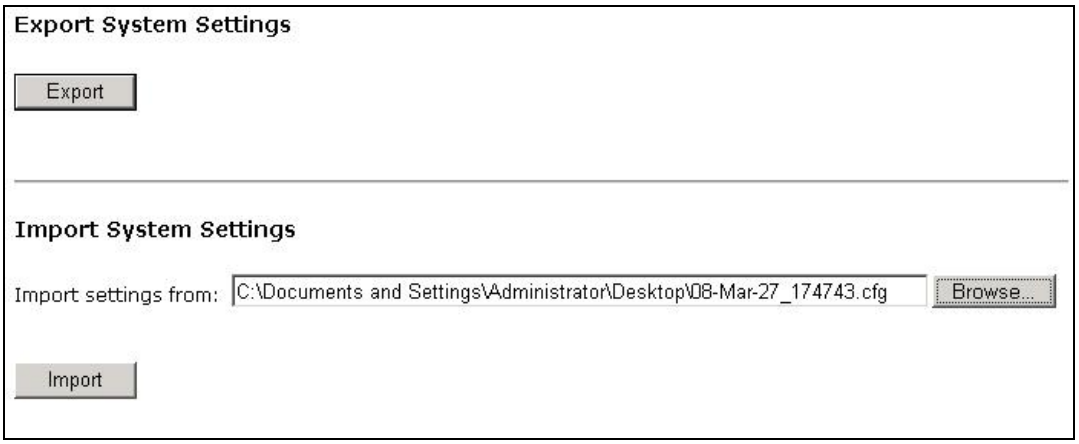


Figure 26 Import/Export Settings

Export	Click this to export. Respond to the file download dialog to save or open the configuration file.
Import Settings from:	Use this to browse to the location of the settings to be imported.
Import	Click this to import from the specified location.

Chapter 6 Managing Cisco WAAS Mobile

This chapter addresses each of the pages available in the server monitoring section of Cisco WAAS Mobile Manager found under Home.

- Server Control
- System Alarms
- Monitoring
- Active Session Reports
- Session History
- Checking Server Events

Server Control

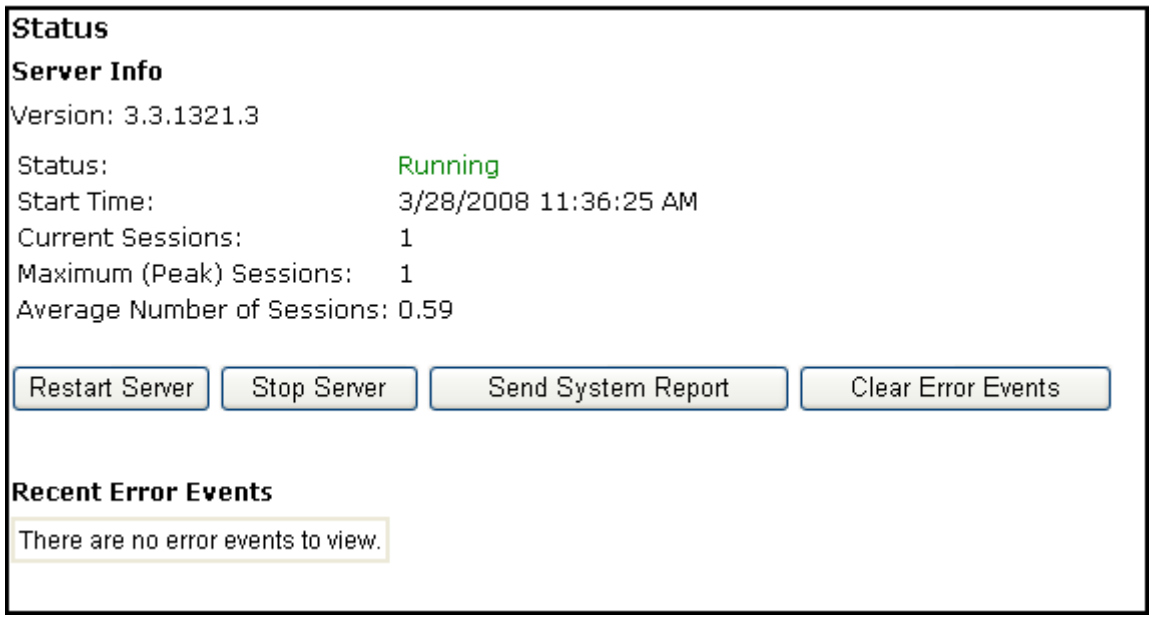


Figure 27 Home Page

Home Page

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	Send a system report to the System Report Server URL configured on the Logging Settings page. 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. Either the System or Application Alarms is selected. When Application is selected the administrator has the option of only viewing Cisco WAAS Mobile-related alarms by checking Cisco WAAS Mobile Alarms Only.

For more information see Cisco WAAS Mobile Integration Guide under SNMP Counters and Alarms.

Monitoring

Traffic Summary

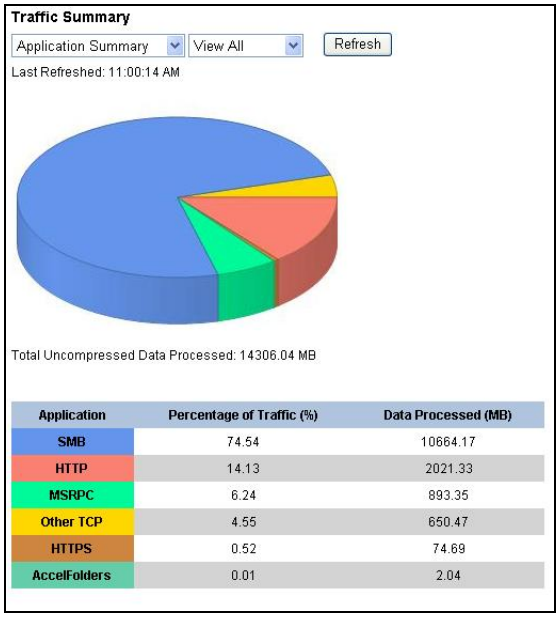
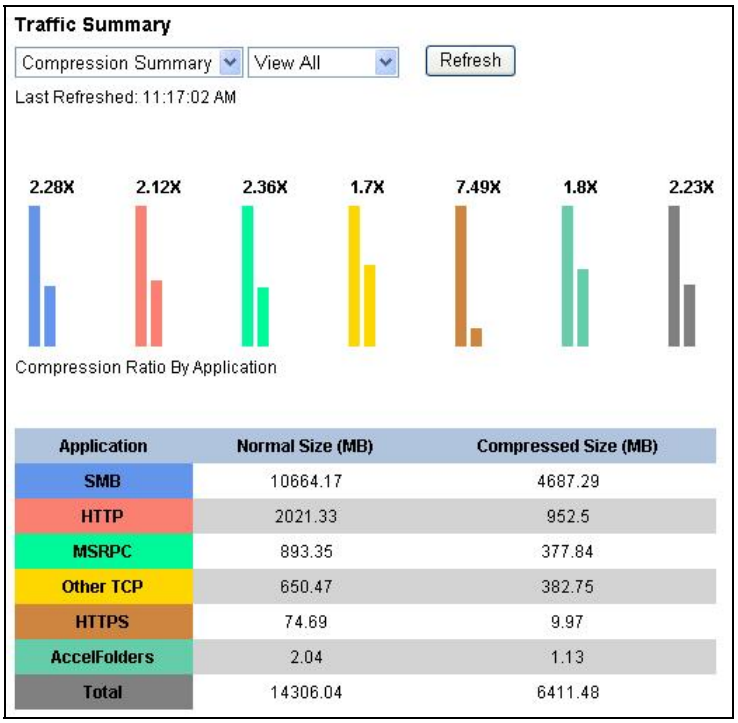


Figure 27 Application Summary

The Application Summary graph uses Cisco WAAS Mobile's session history to display the percentage of traffic by application. Use the drop-down menu to the right of the summary type to change the time interval displayed. Update the graphed information using the Refresh button.



Application	Normal Size (MB)	Compressed Size (MB)
SMB	10664.17	4687.29
HTTP	2021.33	952.5
MSRPC	893.35	377.84
Other TCP	650.47	382.75
HTTPS	74.69	9.97
AccelFolders	2.04	1.13
Total	14306.04	6411.48

Figure 28 Compression Summary

Use the drop-down menu on the Traffic Summary page to display the Compression Summary. This shows compression ratios by application and gives the normal and compressed traffic totals. Use the drop-down menu to the right of the summary type to change the time interval displayed. Update the graphed information using the Refresh button.

Monitoring Graphs

Figure 30 System Stats

A series of graph pages uses performance counters to monitor Application Traffic, Sessions, HTTP Details, Disk System, and System Stats. Use the drop-down menus on each page to change

what is being graphed and for what time interval. Update the graphed information using the Refresh button.

Active Session Reports

Active Sessions Page

Figure 31 Active Sessions

Use the links on this page to obtain information about currently active user sessions and to manage those sessions. Information in the UserName column of these pages varies depending 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.
- *Manage* allows users to be messaged or removed and enables system reports to be triggered from selected users.

Active Sessions Connection Time – provides connection information for active sessions. A "1" in the Is Active column indicates the user is actively sending data through Cisco WAAS Mobile.

Session Id	UserName	Is Active	Session Length (seconds)	Client IP	Alias IP	Delta Cache Size (bytes)
4	earear	1	1715	10.13.1.38	0.0.0.0	89392064
9	jh	1	430	10.13.1.21	0.0.0.0	37748928

Figure 29 Active Sessions Connection Time

Active Sessions Traffic Volume – provides traffic volume information for active sessions.

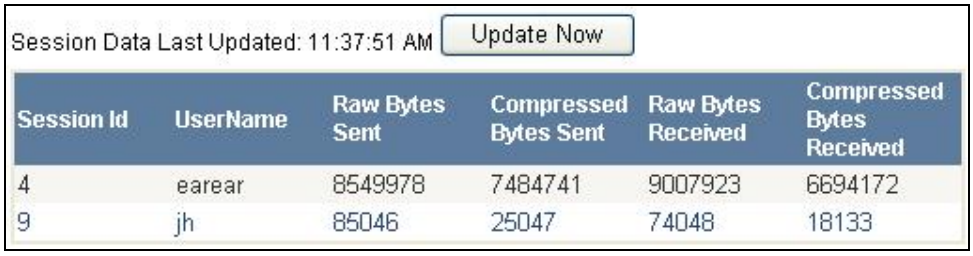


Figure 30 Active Sessions Traffic Volume

Active Sessions Link Performance – provides link performance information for active sessions.

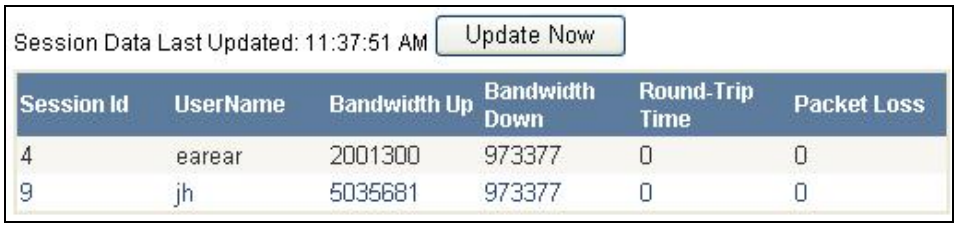


Figure 31 Active Sessions Link Performance

Active Sessions Distribution Label – provides distribution label and other installation information for active sessions.

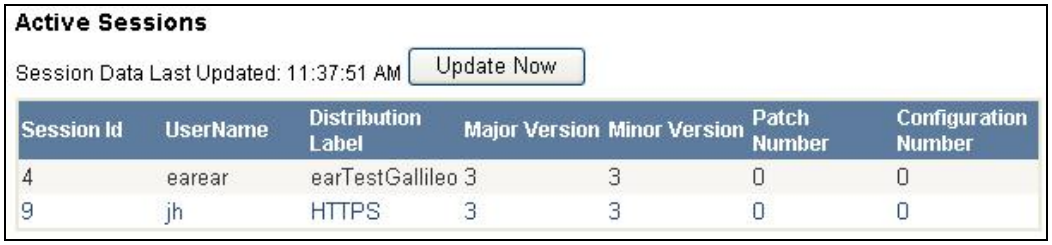


Figure 32 Active Sessions Distribution Label

Active Session Management

Figure 33 Active Session 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.

Session History

Session Reports

Figure 34 Session Reports

Use the links on this page to obtain information about session history. Information in the UserName column of these pages varies depending on Authentication and Client Registration settings. If the UserName field is left blank on these pages, clicking Update Table will show information for all users.

- *Connection* provides connection time information for past sessions.
- *Traffic* provides traffic volume information for past sessions.
- *Link* provides link performance information for past sessions.
- *Installation* provides distribution label and other installation-related information for past sessions.

Connection Time History – provides connection time information for past sessions.

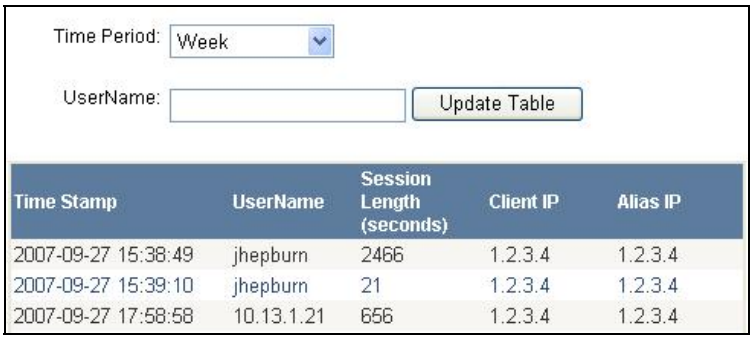


Figure 35 Connection Time History

Traffic Volume History – provides traffic volume information for past sessions.

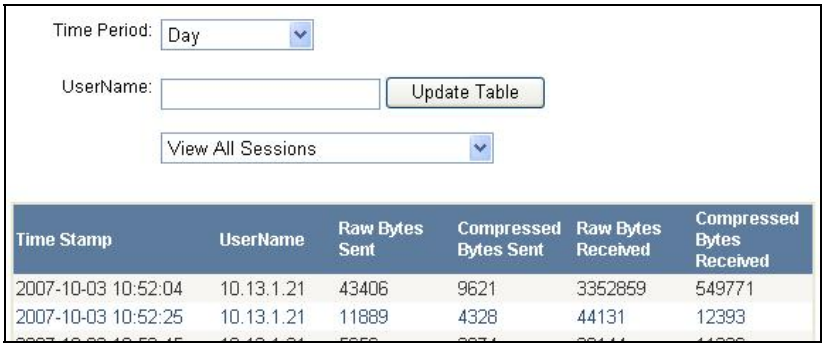


Figure 36 Traffic Volume History

Link Performance History – provides link performance information for past sessions.

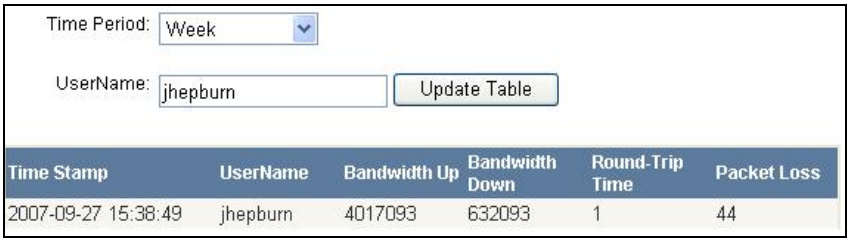


Figure 40 Link Performance History

Installation History – provides distribution label and other information for past sessions.

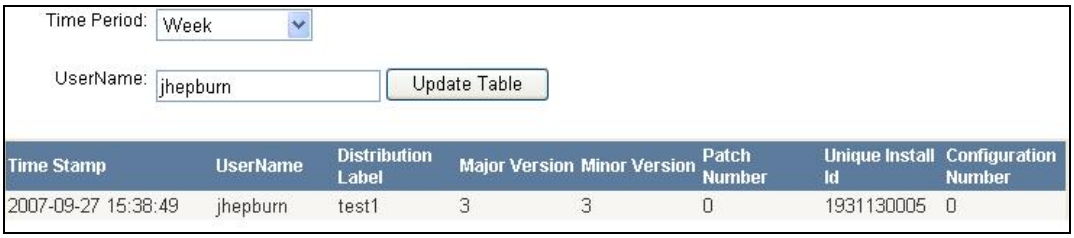


Figure 41 Installation History

Checking Server Events

Log File

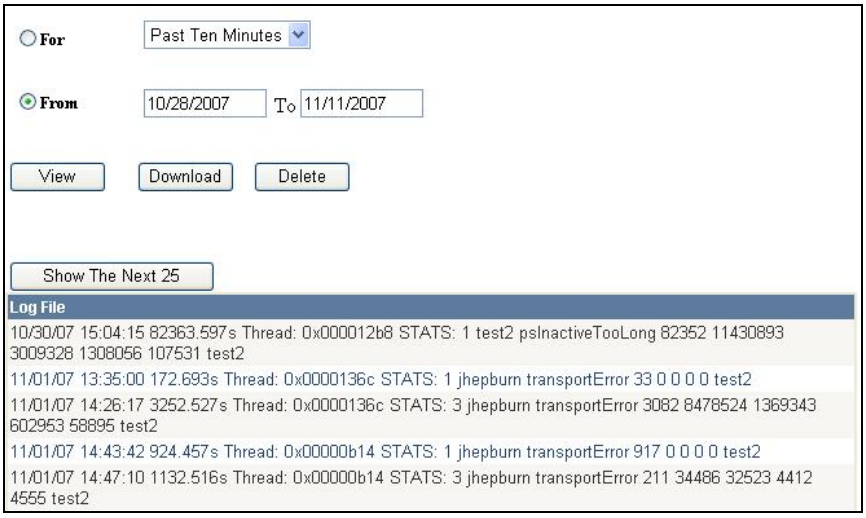


Figure 37 Log File

For	Select to show the log file for one of the pre-defined time periods
From	Select to define a time period for event viewing using dates.
View	Updates the page.
Download	Downloads a copy of the log file.
Delete	Delete 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 Cisco WAAS Mobile server and are available on the System Reports page of Cisco WAAS Mobile Manager. Mousing over each System Report entry displays the size of that System Report file.

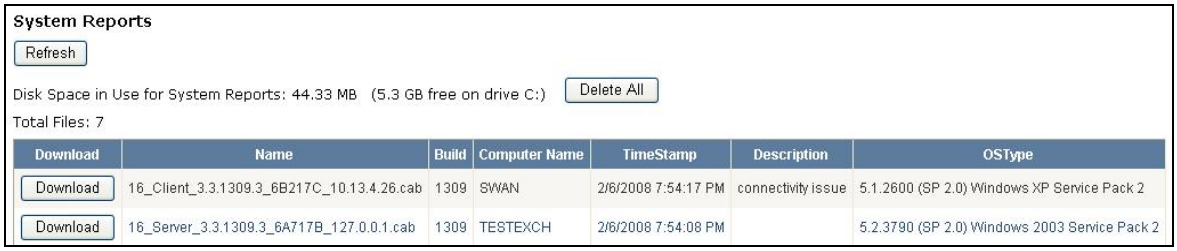


Figure 38 System Reports Monitoring

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.
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

The reports that appear on the System Reports page of Cisco WAAS Mobile Manager use the following naming convention:

- aaa_Client_[build number]_xxxxxx_[Cisco 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]_zzzzzzz_[Cisco WAAS Mobile server IP].cab: This report is generated by the Cisco 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 Cisco WAAS Mobile Manager.

where:

- aaa_: This number 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,_yyyyyy,_zzzzzz: Unique numbers to insure that file titles are not duplicated.

If a crash occurs on the server, only the Server report will be generated. If a crash occurs in the Cisco WAAS Mobile GUI, only an Cisco WAAS Mobile Client report will be generated (if the client is so configured).

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 Cisco WAAS Mobile Client software and the Cisco WAAS Mobile Server software to send system reports to the server. It is typically important to send both system reports to Cisco TAC 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.

Table of Figures

Figure 1 AutoRun Dialog Buttons 9

Figure 2 License Information 12

Figure 3 Client Distribution Creation 14

Figure 4 Network Settings 15

Figure 5 Client User Interface Settings 17

Figure 6 Bypass Settings 18

Figure 7 HTTPS Settings 20

Figure 8 Exclusion Lists Settings 21

Figure 9 Acceleration Routing Table 22

Figure 10 Proxied Process List 23

Figure 11 File Shares Settings 24

Figure 12 Connection Monitor Dialog Box 25

Figure 13 Client Options Dialog – Support Tab 26

Figure 14 System Report – Adding Additional Information 26

Figure 15 Managing Existing Client Distributions 27

Figure 16 Logging Settings 29

Figure 17 RDBMS Logging Settings 30

Figure 18 Log Rotation Settings 30

Figure 19 HTTP Prefetching Settings 31

Figure 20 Delta Cache Settings 32

Figure 21 Set a Registry Value Setting 32

Figure 22 Access Control Settings 33

Figure 23 Upgrade Settings 34

Figure 24 Network Settings 35

Figure 25 System Reports Settings 36
Figure 26 Import/Export Settings 37
Figure 28 Application Summary 39
Figure 29 Compression Summary 40
Figure 32 Active Sessions Connection Time 41
Figure 33 Active Sessions Traffic Volume 42
Figure 34 Active Sessions Link Performance 42
Figure 35 Active Sessions Distribution Label 42
Figure 36 Active Session Management 42
Figure 37 Session Reports 43
Figure 38 Connection Time History 43
Figure 39 Traffic Volume History 44
Figure 42 Log File 45
Figure 44 System Reports Monitoring 46

Cisco WAAS Mobile Administration Guide