

# Cisco Wide Area Application Services: Secure, Scalable, and Simple Central Management



## What You Will Learn

Companies are challenged with conflicting requirements to consolidate costly remote-office infrastructure and to maintain adequate service levels for remote-office users. Cisco® Wide Area Application Services (WAAS) provides the technologies necessary to consolidate infrastructure in the data center while providing application acceleration and WAN optimization capabilities that achieve application delivery performance similar to that of a LAN. This document describes the secure, scalable, and simple central management framework for Cisco WAAS. This framework that allows companies easily manage a consolidated infrastructure.

## About Cisco WAAS Management

A Cisco WAAS deployment can consist of Cisco WAAS Appliances, Cisco Service Ready Engine modules in the Cisco Integrated Services Routers (ISRs) Virtual WAAS (vWAAS) appliances, and Cisco WAAS Express software embedded in Cisco Integrated Services Routers (ISRs). These Cisco WAAS devices work together to optimize TCP traffic and accelerate applications over the WAN. When client and server applications attempt to communicate with one another, the network intercepts these flows and redirects them to the local Cisco WAAS devices to transparently accelerate and optimize flows between the client and the server. The Cisco WAAS devices examine the traffic and use predefined and configurable application policies to determine whether the traffic should be optimized, and if so, how to optimize it, or whether it should be passed through unoptimized. Each Cisco WAAS device can be managed using the embedded command-line interface (CLI) (similar to the Cisco IOS® Software CLI), or the Cisco WAAS Central Manager GUI. The following sections discuss these management mechanisms.

## Cisco WAAS Central Manager

Cisco WAAS is centrally managed by a scalable, secure, and simple function called the Cisco WAAS Central Manager. This function can run on either Cisco Wide Area Virtualization Engine (WAVE) appliances or virtual central manager (vCM) virtual appliances. The Cisco WAAS Central Manager can be configured for high availability by deploying a pair of Cisco WAAS devices or virtual appliances as central managers. Configuration and monitoring data is automatically shared by the two central manager Cisco WAAS devices. The Cisco WAAS

---

Central Manager provides a centralized mechanism for configuring features, reporting, and monitoring. It can manage a topology containing thousands of Cisco WAAS nodes.

The Cisco WAAS Central Manager can be accessed from a web browser, allowing management from essentially anywhere in the world. Access to the Cisco WAAS Central Manager is secured and encrypted with SSL, and users can be authenticated through a local database or a third-party authentication service such as RADIUS, TACACS+, or Microsoft Active Directory.

The Cisco WAAS architecture uses an SSL-encrypted bidirectional channel between the Cisco WAAS Central Manager and the Cisco WAAS devices. This channel is used to exchange reporting information and statistics at a configurable interval as well as to communicate configuration or policy changes to a Cisco WAAS device or a group of Cisco WAAS devices (a device group) from the Cisco WAAS Central Manager. Cisco WAAS devices that are not available to receive the update will receive the update the next time they become available. The Cisco WAAS Central Manager is **not** in the critical path for system operations, so that if the Cisco WAAS Central Manager is unavailable or not accessible, there is no degradation of WAN optimization performance.

## Cisco WAAS Central Manager User Interface

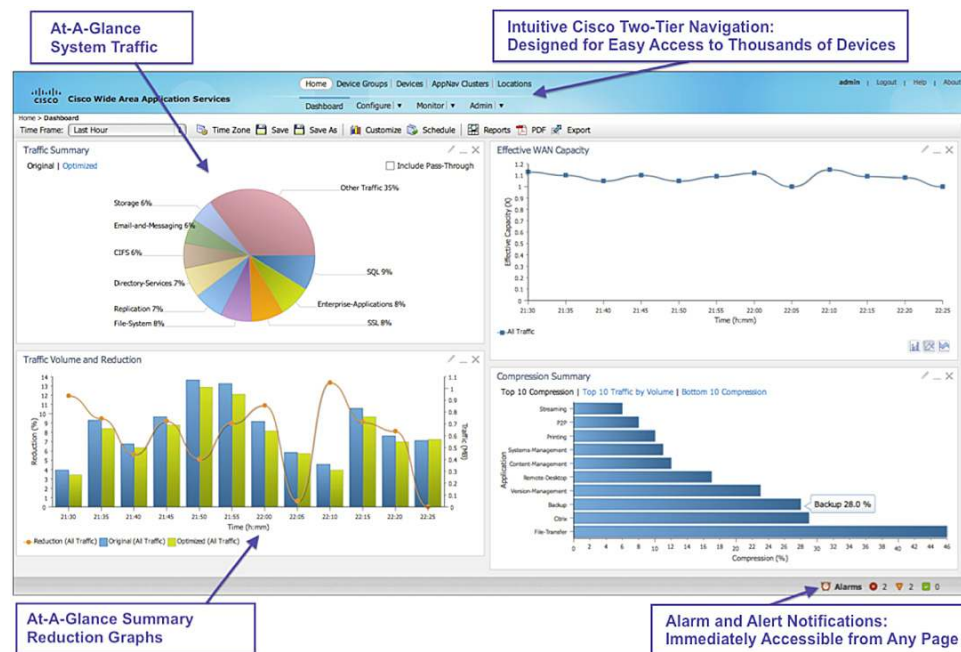
The Cisco WAAS Central Manager is used to centrally configure, manage, and monitor a topology of Cisco WAAS devices. The Cisco WAAS Central Manager device mode can be configured on a Cisco WAAS or vWAAS appliance to provide scalable, secure, robust, centralized web management for all Cisco WAAS devices in the deployment. The Cisco WAAS Central Manager gives the administrator device-specific and systemwide configuration, monitoring, and reporting capabilities, including policy configuration and distribution within the Cisco WAAS deployment.

The Cisco WAAS Central Manager GUI allows administrators to easily perform the following tasks:

- Configure system and network settings for an individual Cisco WAAS device or device group.
- Create, edit, and delete application policies that determine the actions (optimizations) that a Cisco WAAS device performs when it intercepts specific types of traffic.
- Configure application-specific acceleration, including Microsoft File Sharing, Citrix HDX, HTTP, SSL, video, Microsoft Encrypted Messaging API (EMAPI), NFS, and many other preconfigured applications.
- Create device groups to allow concurrent management and configuration of large groups of Cisco WAAS or WAAS Express devices.
- Configure role-based access control (RBAC) for management separation.
- Manage and acknowledge system and device alarms.
- View reports detailing the effectiveness of acceleration and optimization within a Cisco WAAS network.
- Examine per-connection statistics on an individual Cisco WAAS device, including connection details, applied optimization policy, and detailed reduction statistics.
- Install, manage, and transfer virtual blade virtual service instances to remote Cisco WAVE devices.

A successfully authenticated management user will see the Cisco WAAS Central Manager homepage, which provides such information as performance statistics, application traffic mix, deployment health, system-level alarms, notifications, and installed software versions, as shown in Figure 1.

**Figure 1.** Cisco WAAS Central Manager Homepage



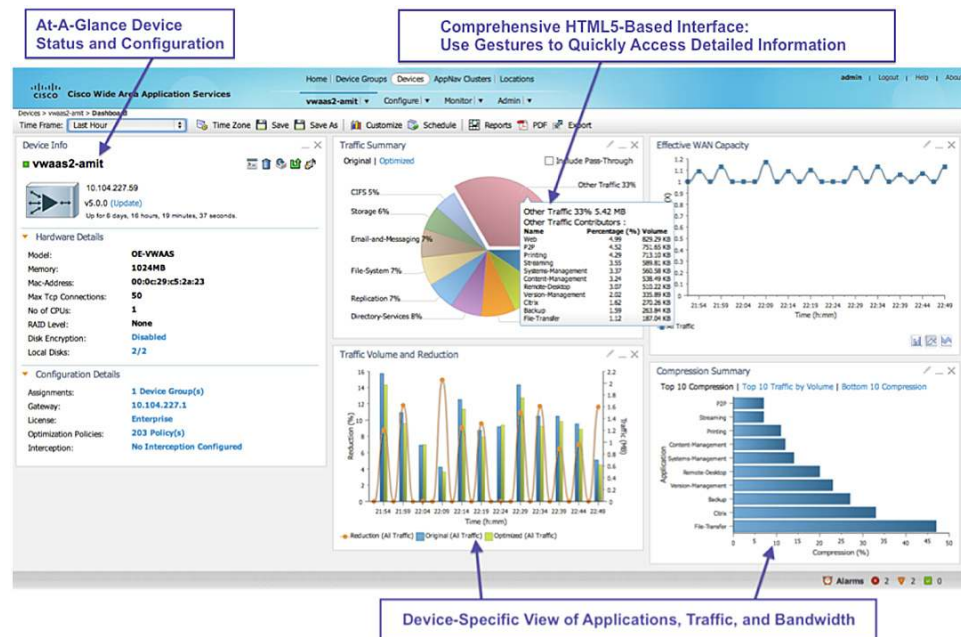
The administrator can also configure, manage, and monitor individual Cisco WAAS devices within the network. Figure 2 shows the device dashboard, which is displayed by default when you select an individual device. Administrators can choose from more than 60 different graphs and tables for monitoring on an hourly, daily, weekly, or monthly basis. Here is a small sample of the available graphs:

- **Traffic summary:** Shows the breakdown of TCP application traffic handled by the Cisco WAAS device
- **Effective WAN capacity:** Multiplier showing the effective performance of the WAN as a result of optimization
- **Traffic volume and reduction:** Shows the volume of original and optimized traffic, along with the reduction percentage
- **Compression summary:** Shows the top-10 applications by compression or volume, with the option to view the bottom 10 by compression
- **Compression summary over time:** Displays a graph of the percentage of application traffic that was reduced on the Cisco WAAS device using the Cisco WAAS compression techniques
- **HTTP and HTTPS charts:** Multiple charts showing connection details, WAN capacity, time savings, optimization techniques, and response-time savings for HTTP and HTTPS traffic
- **SSL charts:** Multiple charts with connection and capacity information and bypass details
- **MAPI charts:** Multiple charts detailing acceleration, response-time savings, connections, capacity, optimized requests, and accelerated client information for encrypted and unencrypted Microsoft Exchange sessions
- **Citrix charts:** Multiple charts with connection details, WAN capacity, bypass reasons, and client information about Citrix HDX traffic

- Common Internet File System (CIFS) and Server Message Block (SMB) charts: Multiple charts with client throughput, connection, WAN capacity, time-savings, request optimization, and client information about CIFS and SMB Versions 1 and 2.x traffic
- Video charts: Several charts with information about acceleration, stream optimization, and effective WAN capacity for video

This capability provides an administrative high-level summary of the most important statistics.

**Figure 2.** Cisco WAAS Central Manager Device-Specific Statistics



Administrators can also obtain detailed information about real-time application traffic patterns, traffic reduction, compression ratios, bandwidth savings, and other statistics for a given time period (the last hour, day, week, or month or a custom date range).

Device-specific or systemwide statistics can be easily exported to the comma-separated value (CSV) file format for offline use. The Cisco WAAS Central Manager can also present real-time connection details that were previously available only from the device CLI, including optimization characteristics (type of optimization applied), reduction statistics, and traffic statistics.

Figure 3 shows a snapshot of real-time connections monitoring; for each active connection, the administrator can see details such as connection source and destination, applied optimization policy, and compression ratio.

**Figure 3.** Cisco WAAS Real-time TCP Connection Details

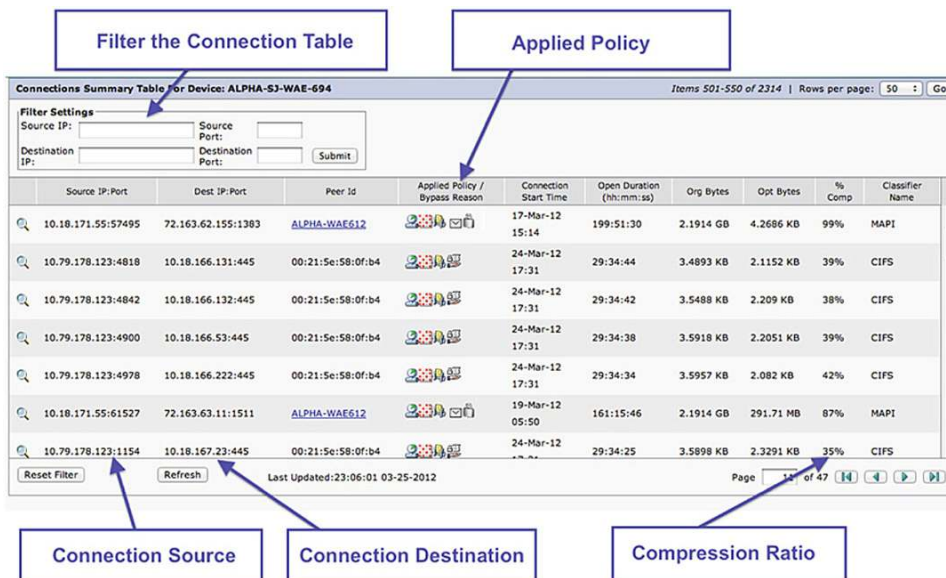
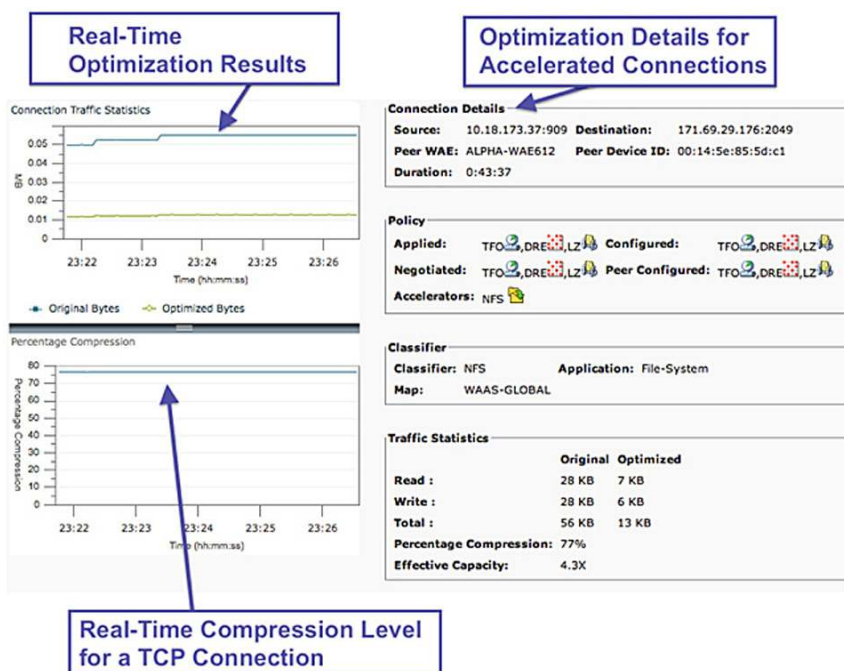


Figure 4 shows the details for a specific connection; real-time compression, connection traffic detailed graphs, and detailed statistics are available for real-time analysis.

**Figure 4.** Cisco WAAS View of Selected Optimized Connection Details

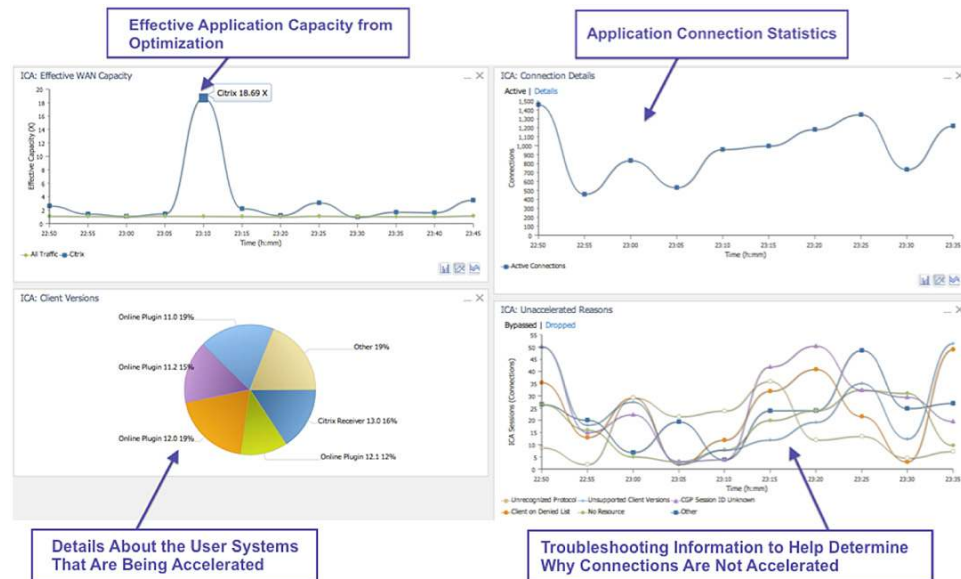


The Cisco WAAS Central Manager also presents individual application acceleration statistics for a variety of applications, including graphs, charts, and detailed information about time and request handling.



Figure 5 shows four sample graphs that give the administrator application acceleration statistics to help the administrator quantify the effectiveness of optimizations and the load on the system.

**Figure 5.** Cisco Application Optimizer Statistics



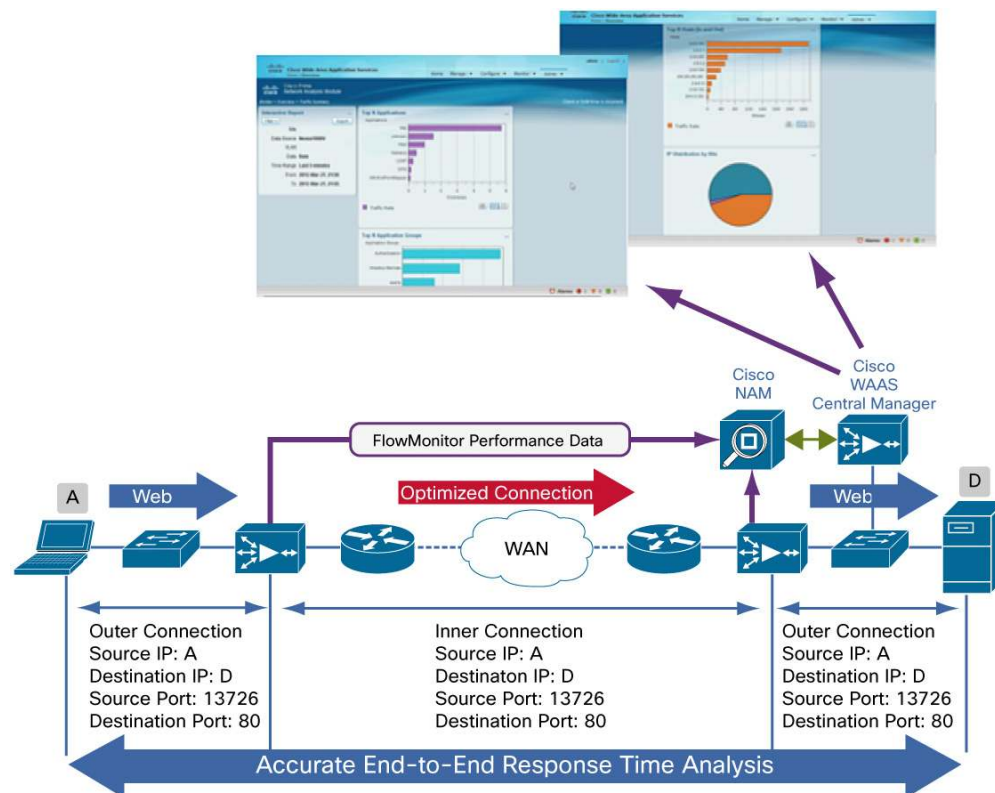
## Integrated Application Performance Monitoring

Providing full visibility into end-to-end performance is a crucial component of the Cisco WAAS Central Manager (Figure 6). Looking beyond bandwidth and into the actual performance of the applications at every point on the WAN gives visibility far beyond traditional bandwidth and usage graphs.

As WAN optimization solutions optimize data, they change the makeup and amount of data traversing the WAN. Traditional monitoring applications are not always designed to handle this dynamic modification of network throughput and performance efficiently. Most traditional WAN optimization solutions require agents or clients running in the branch office to compensate for this lack of visibility into the network.

Cisco WAAS can provide direct, native access to application response-time data without the need for complex agents or clients installed at the branch office. Using the Cisco Network Analysis Module (NAM) monitoring framework, the Cisco WAAS Central manager can provide a single point to view items such as network performance, top talkers, bandwidth use, and application response-time information.

**Figure 6.** Application Performance Monitoring Using the Cisco WAAS Central Manager



In addition, the Cisco WAAS Central Manager can also publish WAN optimization statistics directly to common third-3<sup>rd</sup> party management solutions, providing This provides the most comprehensive, open WAN optimization monitoring framework available.

## Simplified Management Using Groups, Locations, and Clusters

The Cisco WAAS Central Manager allows the administrator to create groups, locations, and clusters to simplify management of the entire Cisco WAAS network. Groups, locations, and clusters provide a means for grouping common configurations and statistics so that they can be applied to a large number of devices.

### Device Groups

Device groups enable simplified configuration management of Cisco WAAS devices. Device group allows settings to be applied to multiple devices at the same time, improving administrative efficiency. Application policies and other items configured through a device group propagate automatically to all devices that are members of that group. After a device group is configured, the administrator can use the Cisco WAAS Central Manager to configure almost every aspect of the Cisco WAAS devices that are members of that device group, including the following:

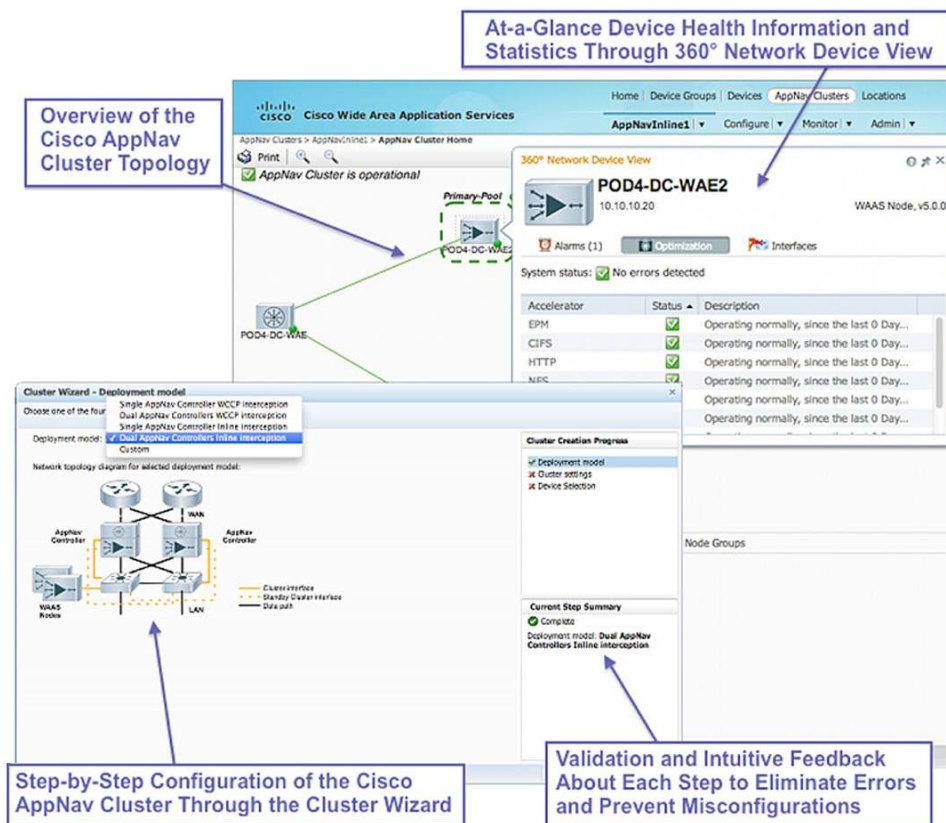
- Software version: Control the version of the software that is installed on a single Cisco WAAS device or group of Cisco WAAS devices.
- Application acceleration configuration: Configure and monitor application-specific acceleration parameters and policy elements.
- WAN optimization policy configuration: Define applications, classifiers, and policy maps.

- Network interception configuration: Configure network interception mechanisms such as physical Inline interception, Cisco Virtual Network Service Data Path (vPATH), and Web Cache Communication Protocol Version 2 (WCCPv2), and subsequent delegation to a Cisco AppNav cluster.
- Login authentication: Define and configure the user login authentication method (local database, Active Directory, etc.).
- Cisco WAAS CLI users: Create accounts that can be used to access the Cisco WAAS CLI and Cisco WAAS Central Manager.
- Alerts and notifications: Configure email and logging servers for remote notification.

### Cisco AppNav Clusters

Cisco WAAS Central Manager is the central point for Cisco AppNav configuration and cluster management (Figure 7). Cisco AppNav is the only comprehensive and network-integrated WAN optimization solution available with virtualization technology that dramatically reduces operation complexity in enterprisewide WAN optimization deployments. Cisco AppNav clusters in the Cisco WAAS Central Manager enable configuration, control, and real-time monitoring of the Cisco AppNav clusters, providing rapid scaling and fault isolation in any environment. In addition, the Cisco WAAS Central Manager provides an intuitive cluster wizard to accelerate and simplify initial deployments.

**Figure 7.** Application Performance Monitoring Using the Cisco WAAS Central Manager





---

## Locations

Locations allow reports and statistics to be easily collected for devices in a common physical location. Every Cisco WAAS device registered to the Cisco WAAS Central Manager is assigned a location automatically. If devices are configured to use the same location, graphs and reports can be configured through the Cisco WAAS Central Manager to show the cumulative data for all devices at a given location. This collection provides a simple, intuitive way to view and query optimization and traffic volume across multiple Cisco WAAS devices.

## Automatic Registration

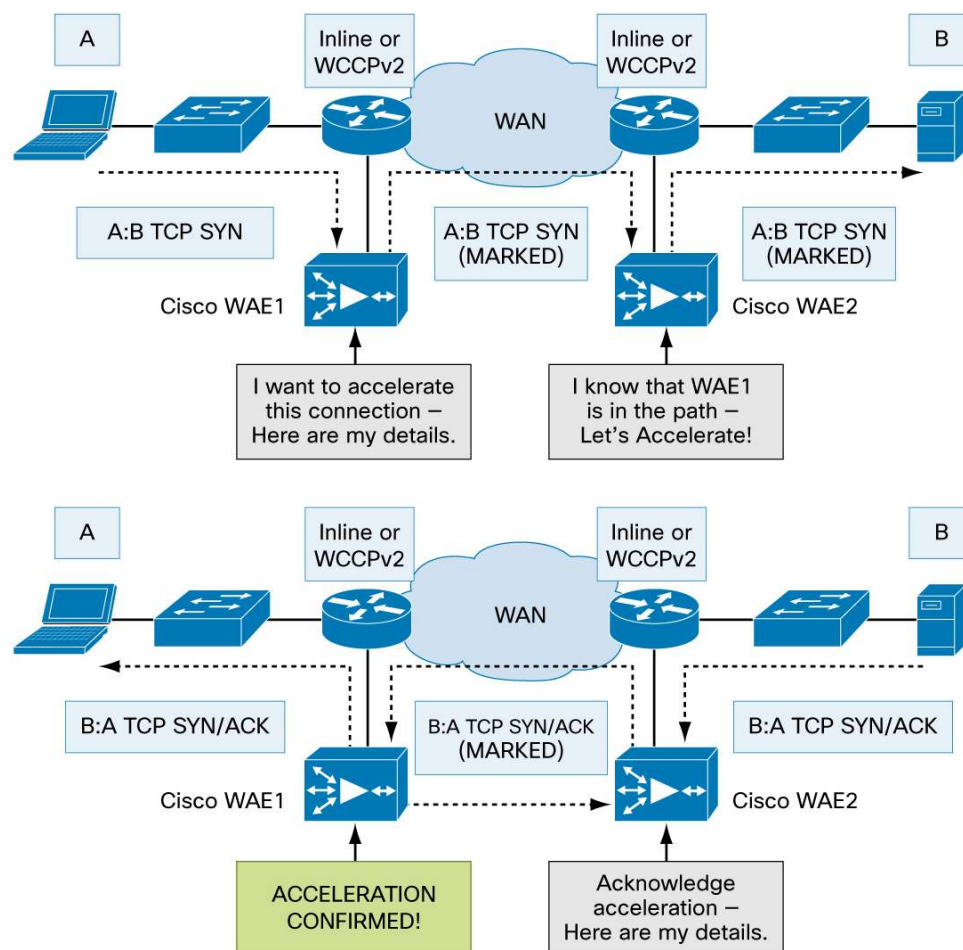
The Cisco WAAS Central Manager is a central component in automatic Cisco WAAS device registration. This capability allows customers to widely deploy Cisco WAAS in their enterprises with little or no initial device configuration required. Automatic registration allows Cisco WAAS devices to automatically obtain an IP address and automatically attach to the Cisco WAAS Central Manager. This deployment model gives customers the flexibility to manage and rapidly deploy thousands of branch-office Cisco WAAS devices while maintaining configuration and control from a single, central interface.

## Automatic Discovery

Cisco WAAS provides an automatic discovery feature for transparent integration, simplified deployment, and ease of management. Cisco WAAS automatic discovery provides automatic discovery of accelerators, mitigating the need for complex overlay networks and helping network infrastructure teams get the most from their investment in network design. Without automatic discovery, an administrator would have to manually define optimization tunnels, defining a peer-to-peer relationship, which is not scalable in large environments.

With automatic discovery, as shown in Figure 8, accelerators first check whether a peer accelerator exists in the path of the packet flow between the source and the destination. If a pair of accelerators exists, an optimization policy is transparently negotiated and then applied to the application flow. If a peer accelerator does not exist, the application flow remains unoptimized and passes through without modification. By using automatic discovery, network infrastructure teams can deploy services to improve application performance over the WAN without having to implement complex overlay networks that require as much, or more, administration than the routed network.

**Figure 8.** Cisco WAAS Automatic Discovery



## Cisco WAAS Central Manager Scalability and High-Availability Configurations

The Cisco WAAS Central Manager is designed for enterprise scalability, and it can be deployed in highly available and redundant configurations.

For scalability, customers can deploy multiple Cisco WAAS Central Managers to scale to any number of deployed Cisco WAAS devices. Because of the unique Cisco WAAS autodiscovery protocol, Cisco WAAS devices can easily be configured to detect, optimize, and interoperate with other Cisco WAAS devices managed by any Cisco WAAS Central Manager. This unique feature enables optimization between domains, cross-functional units, and even different companies while still maintaining separation of management and security.

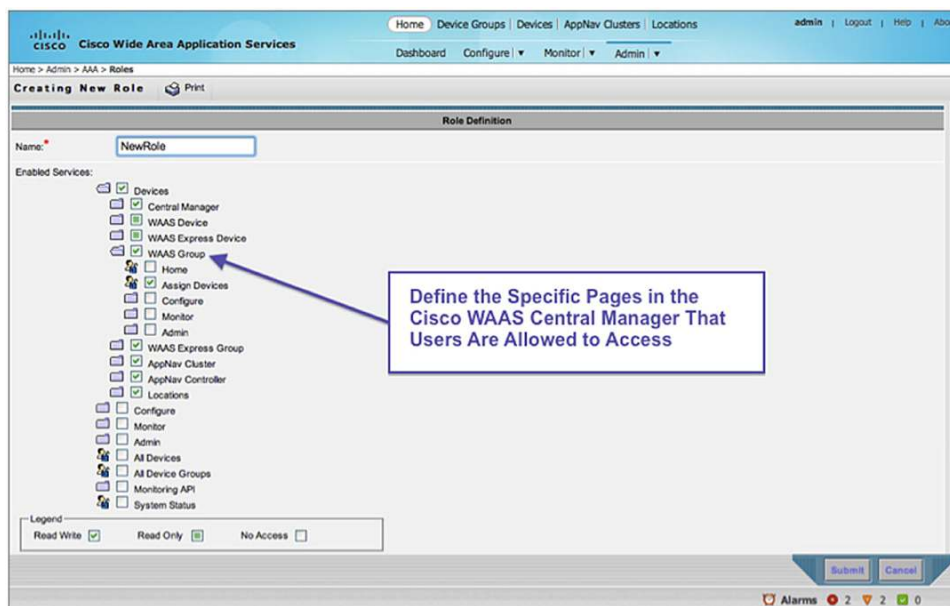
For high availability, the Cisco WAAS Central Manager can also be deployed in an active-standby configuration. One Cisco WAAS device will act as the primary Cisco WAAS Central Manager, and the second device will act as a backup Cisco WAAS Central Manager. In this mode, the Cisco WAAS device serving as the backup Cisco WAAS Central Manager automatically receives configuration changes and monitoring data from the primary Cisco WAAS Central Manager, just like any other Cisco WAAS device in the Cisco WAAS topology. If the primary Cisco WAAS Central Manager fails, the Cisco WAAS devices in the topology automatically redirect themselves to the secondary Cisco WAAS Central Manager. The monitoring data collected on the primary Cisco WAAS Central Manager will be available on the secondary Cisco WAAS Central Manager device automatically.

## Role-Based Access Control

The Cisco WAAS Central Manager allows the central management system to be provisioned so that administrative groups have control over only the portions of the Cisco WAAS topology that they need. By using role-based access control (RBAC), a Cisco WAAS administrator can define administrative users, roles, and domains to specify the areas of the Cisco WAAS Central Manager that users can view and control. User accounts and credentials can be either stored locally on each Cisco WAAS device, or authenticated using a third-party authentication service such as TACACS, RADIUS, or Microsoft Active Directory.

Figure 9 shows that roles can be defined to provide very detailed control over the pages of the Cisco WAAS Central Manager for which a user assigned to the role has read and write privileges.

**Figure 9.** Cisco WAAS Central Manager Role Definition Allows Detailed Control of Administrative Access



Domains can be configured to specify the devices or device groups for which a user assigned to the domain has privileges to perform operations. For example, a Cisco WAAS Central Manager administrator can assign a user to a role and a domain that allow the user to create and modify application policies on a specific group of devices but do not allow the user to make any other changes to the system.

Figure 10 shows the assignment of a user to a management domain; here, the specific user is assigned to manage a group of devices based on the geographical location of the devices.

**Figure 10.** Cisco WAAS Central Manager Management: Assigning a User to a Management Domain

Domains Easily Assigned Through Tab on the Account Management Page

Assigned as Administrator for North America Management Domain

This Domain Includes Devices in North America

Name	Entity Type	Comments
APAC Domain	Device Group	Domain for devices in APAC
EMEA Domain	Device Group	Domain for devices in EMEA
NA Domain	Device Group	Domain for devices in North America

## Centralized Software Upgrades Using Cisco WAAS Central Manager

Every Cisco WAAS device within the Cisco WAAS topology should be configured to use the same version of software. Many functions are available to control the installed software version on a Cisco WAAS device, including the software installation and management system in the Cisco WAAS Central Manager. The Cisco WAAS Central Manager enables centralized software management across an entire network of Cisco WAAS devices. Using the Cisco WAAS Central Manager, an administrator can define up to 10 individual software versions, which can be selectively and individually assigned to a Cisco WAAS devices or to a device group containing multiple Cisco WAAS devices, as shown in Figure 11. After a software version has been defined, it can be distributed to a group of Cisco WAAS devices and either installed automatically or installed manually at a later reboot.

**Figure 11.** Cisco WAAS Central Manager Provides Centralized Software Update Services for Cisco WAAS Devices

Software Version

Enable or Disable Auto Reload After an Upgrade

Software Download Location (HTTP or FTP URL)

Use a Full or Lightweight Image for Low-Bandwidth Sites

Software File URL	Software Version	Image Type	Auto Reload
ftp://2.8.4.200/share/code/waas-universal-4.4.5-49 bin	4.4.5	Universal	Disabled
ftp://2.8.4.200/share/code/waas-universal-5.0.0.168-49 bin	5.0.0	Universal	Enabled

## Cisco WAAS CLI

The Cisco WAAS CLI, similar to the Cisco IOS Software CLI, allows administrators to configure, manage, and monitor Cisco WAAS devices through a console connection or a terminal emulation program. This powerful CLI enables simple, quick troubleshooting access on an individual device basis. However, the Cisco WAAS Central Manager is the primary tool for configuring, managing, and monitoring Cisco WAAS devices, providing scalability and management in groups rather than just for individual devices. Wherever possible, you should use the Cisco WAAS Central Manager GUI instead of the CLI.

Figure 12 shows the CLI, which gives the administrator a familiar Cisco IOS Software type of interface for viewing and modifying basic network configuration settings.

**Figure 12.** Cisco WAAS CLI

```
datacenter#show run
! waas-universal-k9 version 5.0.0 (build b137 Feb 29 2012)
device mode application-accelerator
interception-method vn-service vpath
!
hostname datacenter
!
ip domain-name waas.local
!
primary-interface Virtual 1/0
interface Virtual 1/0
ip address 172.30.100.202 255.255.255.0
exit
interface Virtual 2/0
ip address 172.30.125.1 255.255.255.252
exit
!
ip default-gateway 172.30.100.254
!
no auto-register enable
!
datacenter#
```

## System Logging and Notification

Cisco WAAS devices support remote notification capabilities, including Simple Network Management Protocol (SNMP) traps, SMTP notifications, and system logging (syslog) notifications. Cisco WAAS devices can be configured to use up to four syslog servers.

## SNMP Management

Cisco WAAS supports SNMP Versions 1, 2c, and 3. Cisco WAAS can send informational alerts or alarms to any SNMP-compliant manager, including the most commonly used managers such as HP OpenView and IBM Tivoli NetView. Cisco WAAS supports several MIBs that allow administrators to monitor and troubleshoot nearly every aspect of the Cisco WAAS topology.

Cisco WAAS exports parameters for monitoring the state and performance of the deployment to both private and standard MIBs.



---

The private MIBs provide information specific to Cisco WAAS and include the following:

- ACTONA-ACTASTOR-MIB: Provides transparent CIFS statistics
- CISCO-CDP-MIB: Provides information about interfaces displayed with Cisco Discovery Protocol
- CISCO-CONFIG-MAN-MIB: Provides a method for accessing the configuration of the Cisco WAAS device
- CISCO-CONTENT-ENGINE-MIB: Provides alarms and other notification events
- CISCO-ENTITY-ASSET-MIB: Provides more detailed information about the items in ENTITY-MIB, such as serial number, orderable part number, firmware version, and revision ID
- CISCO-WAN-OPTIMIZATION-MIB: Contains detailed WAN optimization-specific statistics, such as connection count, application liveliness, application statistics, and capacity

The standard MIBs are used to obtain general liveliness and platform information and include the following:

- MIB-2 General Network Statistics (RFCs 1213 and 1157): Contains essential parameters for the basic management of TCP/IP-based networks
- Host Resources (RFC 1514): Contains a uniform set of objects useful for managing host computers
- ENTITY-MIB (RFC 2737): Provides information about the physical and logical entities in the device
- EVENT-MIB (RFC 2981): Provides the capability to monitor MIB objects on the local system or on a remote system and take simple action when a trigger condition is met
- SNMPv3 MIBs (RFCs 2571 through 2576)

## XML API

Cisco WAAS Central Manager provides an API to allow applications to interact directly with data and information collected by Cisco WAAS. This API provides a programmable interface for system developers to integrate with customized or third-party monitoring and management applications.

The Central Manager monitoring API is a web service implementation. The client and server communication follows the Simple Object Access Protocol (SOAP) or Service-Oriented Architecture (SOA) standard. This communication, which exchanges XML-based messages over the network using HTTP or HTTPS, allows comprehensive monitoring and data exchange between Cisco WAAS Central Manager and other third-party or custom applications.

## Conclusion

IT departments considering infrastructure consolidation and application acceleration solutions should explore solutions that provide secure, scalable, and simplified central management. The goal of such solutions should not be solely cost reduction and performance improvement, but also simplification of the overall application delivery management process. Cisco WAAS provides such a framework through a secure, scalable, and simplified central management system that allows IT departments to easily manage a consolidated infrastructure.

## For More Information

Visit <http://www.cisco.com/go/waas>




Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)