

Deploying Cisco Wide Area Application Services and Digital Media System for Video Acceleration

Most enterprises understand the power of video-based information delivered at precisely the time when that information can be most effectively absorbed and used. They also understand that the technical quality of that video presentation, in addition to content quality, has a significant effect on the video's ability to engage the viewer and impart the message. Previous efforts to deliver high-quality video messaging, either live or on video tape or DVD, have been expensive, time consuming, difficult to control, and difficult to maintain. Network-based delivery of live video and video on demand (VoD) require significant bandwidth and dedicated content distribution networks.

Cisco® Wide Area Application Services (WAAS) and Cisco Digital Media System (DMS) provide a simple and efficient solution for delivering high-quality live video and VoD throughout the enterprise while also providing state-of-the-art WAN acceleration for other TCP-based applications.

This document shows how to combine the flexibility and management capability of Cisco DMS with the efficiencies and acceleration capabilities of Cisco WAAS.

The Value of Business Video

Few would argue that video is the next-best thing to being there, and often video can be even better. "Being there" involves a significant cost in travel and lost productivity and does not guarantee that the information being offered will be received, digested, and absorbed by the listener. Live video streaming can provide a sense of immediacy and personal involvement. If that information is not immediately useful and applied, however, it can be lost as other, more pertinent information is acquired and applied. The concept of video on demand, or VoD, has been implemented in various forms over the years in an attempt to mitigate this problem and provide precise information at just the right time when the viewer is ready and willing to receive the material and able to apply it immediately.

Live video and VoD can also help unify an organization as each viewer in the organization receives the same message whether it is delivered today or next year. Live video and VoD can uniformly educate employees about corporate goals and priorities, new products and procedures, regulatory compliance mandates, or any other information that needs to be communicated, providing a sense of intimacy and immediacy between the speaker and viewer, difficult to achieve in any medium other than a live interaction. This intimacy makes video especially useful for:

- **Executive communications about corporate goals, achievements, changes in direction, and new campaigns:** Employees appreciate getting a sense of the person making the announcement, and the executive's urgency, pride, and priorities come across naturally.

- **Sales force and product training:** Viewers can return to parts of the video they need to watch again, training can be delivered no matter where the employee is, and the content can be updated frequently. This feature is especially valuable for technology, pharmaceutical, financial, and other industries where products change frequently.
- **Employee regulatory compliance training:** Viewers can repeat certain sections to make sure they understand them, and the video can display documents along with a person talking to clarify the information. In addition, the delivery system can monitor which employees have seen the material.

The Problem with Business Video

The appeal of video is widely recognized, but its immediacy is not, and immediacy is a crucial part of its usefulness. Live streaming broadcasts can satisfy this requirement, and recordings can be saved for future playback. The material must be delivered in a timely way so it is fresh and accurate: Yesterday's news loses its value. When it is not live, it is usually best delivered at the viewer's convenience: when it fits into the viewer's schedule and preferably at the viewer's workspace. With any more than a few video assets, managing the timeliness of business video becomes problematic.

Cost becomes a concern when large numbers of viewers in geographically disbursed locations are involved. Each time the content changes, new video must be prepared and distributed. With physical media such as video tape or DVD, managing the creation, distribution, version control, and assets in the local office becomes a burdensome and cost-prohibitive task.

To reduce these costs, an alternative is to deliver the video directly to the viewer over the network. This method requires substantial network bandwidth for even low-bit-rate (relatively small size and low quality) video. High-quality and thus more engaging video is not possible with this method without significant network infrastructure and investment.

For live video streaming, without a full multicast environment, all viewers must receive individual streams at their desktop players. Without some form of optimization, each individual stream will originate at the source origin media server and be streamed across the entire network. This transmission can quickly overwhelm even the most robust network.

For VoD, one way to mitigate the network bandwidth problem is to preposition video content on a device close to the viewer, reducing the distance between the viewer and the video source. Electronic content distribution networks (eCDNs) provide capabilities that address the bandwidth problem, but require deployment and management of a relatively complex network. eCDNs work well for providing a wide range of features and functions for acquiring and distributing digital media assets throughout the enterprise, but at a significant cost for features seldom, if ever, used.

Clearly, an alternative solution is needed that treats high-quality video, both live and VoD, as just another application requiring acceleration and optimization in its delivery from a centrally managed data repository to the requesting user at the edges of the enterprise network.

A Simple Solution

Addressing the VoD problem requires addressing both the management of the video assets (that is, the creation, cataloging, advertising, updating, etc.) and the delivery of the video asset to the viewer. A number of vendors address one or the other of these problems, but only Cisco offers a simple end-to-end solution by combining the digital media management capabilities of Cisco

Digital Media Manager (DMM) and Cisco Video Portal with the file distribution and HTTP application optimization capabilities of Cisco WAAS.

A typical implementation of a Cisco DMS for a single site or campus uses a web server to host and deliver the content to the requesting user's desktop Cisco Video Portal. For efficient delivery over a WAN, a more efficient distribution mechanism involving staging, or prepositioning, of large-file-size video content is required. Until now, the distribution technology of choice has been an eCDN. With the growing demand for WAN optimization in general, Cisco WAAS can now be employed to provide similar distribution and prepositioning capabilities.

For live video events, Cisco WAAS Software Version 4.1 provides a simple solution with automatic and transparent video stream splitting at the edge of the network. No configuration is required for Windows Media live streams. When multiple users make identical requests to join a live streaming event, the edge Cisco Wide Area Application Engine (WAE) Appliance using Cisco WAAS detects the request and automatically splits the single incoming stream into as many outgoing streams as are requested.

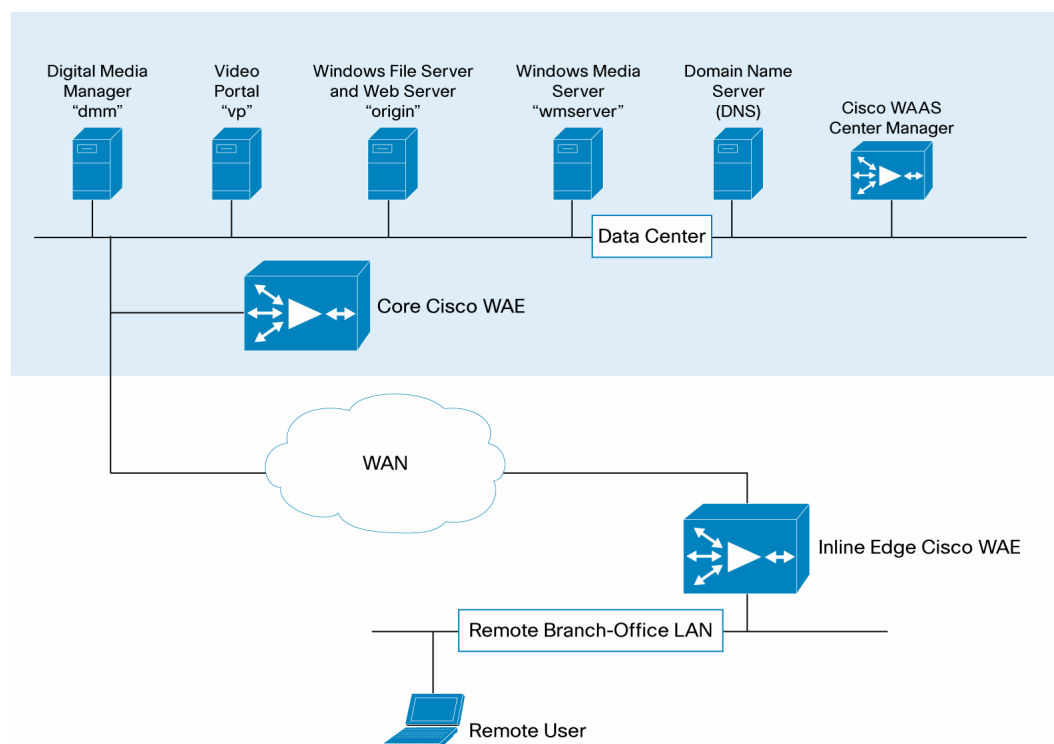
While typical video on demand prepositioning capability encompasses web objects or files using the HTTP protocol, Cisco WAAS prepositioning is file based, using the Microsoft Common Internet File System (CIFS) protocol. The capability to serve file-based objects from a local cache can currently be employed only for protocols, such as Windows Media, that can accommodate file-based access. In a typical enterprise deployment of Cisco Video Portal over a WAN, in addition to standard HTTP web content, two types of video content are involved: Adobe Flash and Windows Media. The Cisco WAAS standard WAN acceleration techniques, including data redundancy elimination (DRE), Lempel-Ziv (LZ) compression, transport flow optimization (TFO), and with the upcoming new release of Cisco WAAS, the HTTP application optimizer with its TCP connection reuse capability, the Cisco Video Portal HTTP and Adobe Flash content delivery will be optimized with TFO, DRE, and LZ compression and delivered directly from the origin server. The high-bandwidth, large-file-based Windows Media video content, comprising the vast majority of the potential WAN traffic, can be fully prepositioned from the origin server and served locally from the edge Cisco WAAS WAE devices, thereby removing most of the Cisco Video Portal traffic that would otherwise traverse the network. The remaining non-file-based content, the HTTP and Adobe Flash content, should still be prepositioned to the edge using CIFS prepositioning to take advantage of prepopulation of the DRE cache for best compression when the content is actually requested, but the content is ultimately served from the origin server. Prepositioning this content allows the DRE cache to be preloaded so that any subsequent requests for this content can be re-created from the DRE cache, reducing the total access time.

Using Cisco Video Portal with Cisco WAAS as the distribution technology involves:

- Creating a file server file share to store Windows Media video content
- Creating a web server to serve web content other than Windows Media video content
- Creating an FTP server to upload content to the web and file server
- Setting the Windows Media access mechanism specified in Cisco DMS to a file-based URL
- Setting up Cisco WAAS prepositioning policy directives
- Managing file server access authorization

Figure 1 shows a conceptual diagram of a Cisco WAAS content network domain called `waaslab.local`. Note that while the diagram shows an inline deployment of Cisco WAAS at the remote branch office, this is not a requirement. The deployment would work just as well with Web Cache Communication Protocol (WCCP) redirection to a Cisco WAAS appliance as shown in the data center.

Figure 1. Conceptual Network Diagram for `waaslab.local`

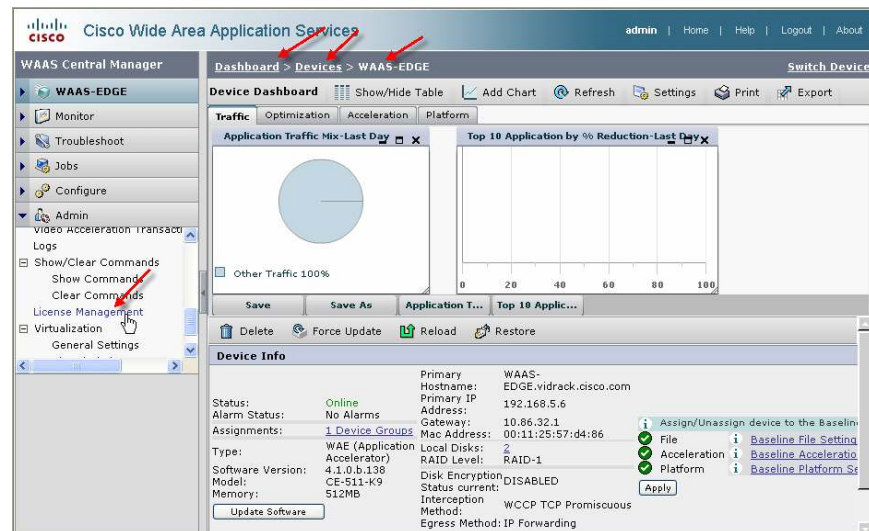


The procedures in the following sections document the steps required to configure and implement Cisco Video Portal using Cisco WAAS as the distribution technology.

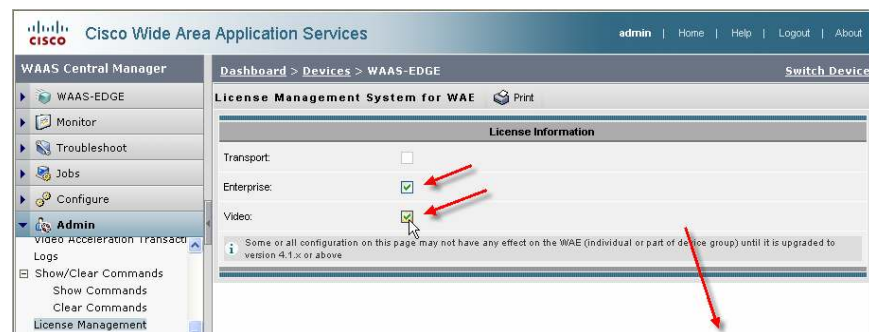
Configuring Live Events with Cisco WAAS and Cisco DMS

Configuring Cisco WAAS and Cisco DMS for Windows Media live streaming events requires setting up a standard live event in Cisco DMS using a Windows Media Server as a publishing point and then licensing and enabling the video application optimizer on the edge Cisco WAAS WAE device.

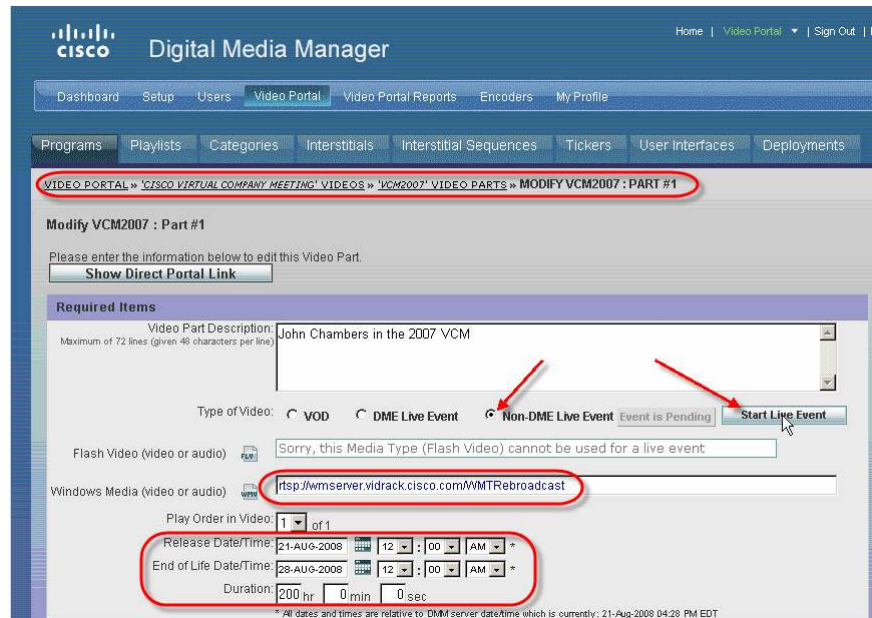
1. From the Cisco WAAS Central Manager GUI, select the edge device that will perform the stream split to serve the requesting users and, under the Admin group, click License Management.



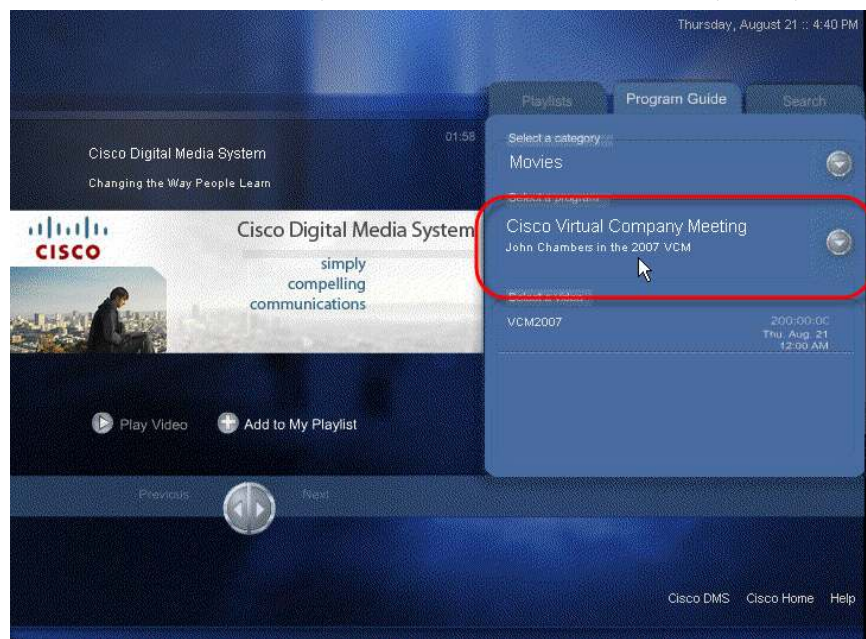
2. Verify that the Enterprise and Video licenses have been enabled. Click Submit (button not shown) to complete the transaction.



- Configure Cisco DMS for a live event in the standard way using a Windows Media Server as the live publishing point. The screen shot shown here and the following discussion and illustrations assume that the publishing point is `rtsp://wmserver.vidrack.cisco.com/WMTRebroadcast`. This particular publishing point is a rebroadcast of a previous live event. Define the type of this video part in Cisco DMM as Non-DME Live Event. Then start the live event and deploy the program to the Cisco Video Portal.



- On the Video Portal tab, verify that the live event has been properly deployed.



5. Open a Telnet session for the edge Cisco WAE and clear the video counters:

```
WAAS-EDGE#clear stat accelerator video
WAAS-EDGE#sho statistics accelerator video
```

VIDEO:

Global Statistics

Time elapsed since "clear statistics": 0days 0hr 0min 5sec

Video Connections

=====

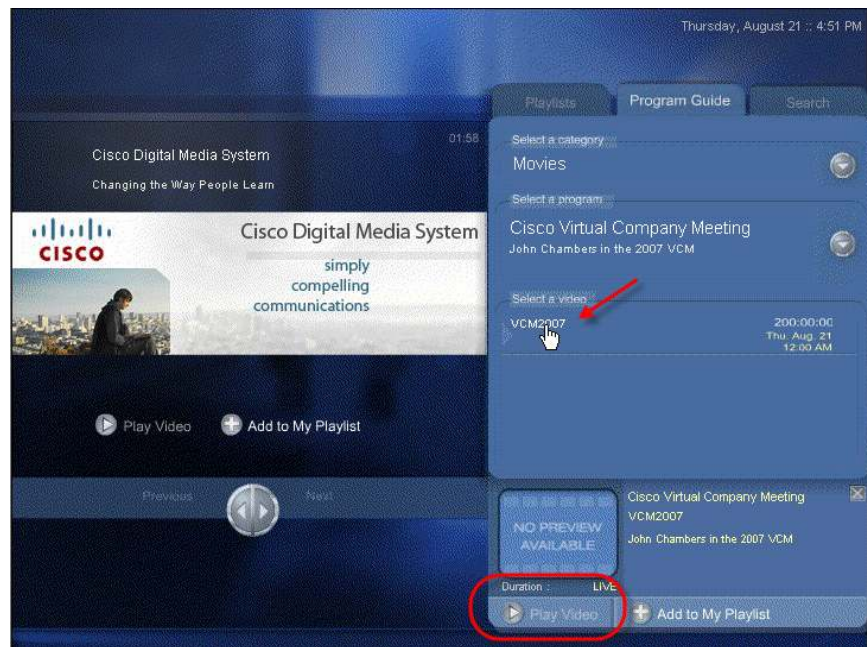
Connections handled	num	%
Total handled	0	0.00
Windows-media live accelerated	0	0.00
Un-accelerated pipethru	0	0.00
Un-accelerated dropped due to config	0	0.00
Error dropped connections	0	0.00

Windows-media active sessions	current	max
Outgoing (client) sessions	0	0
Incoming (server) sessions	0	0

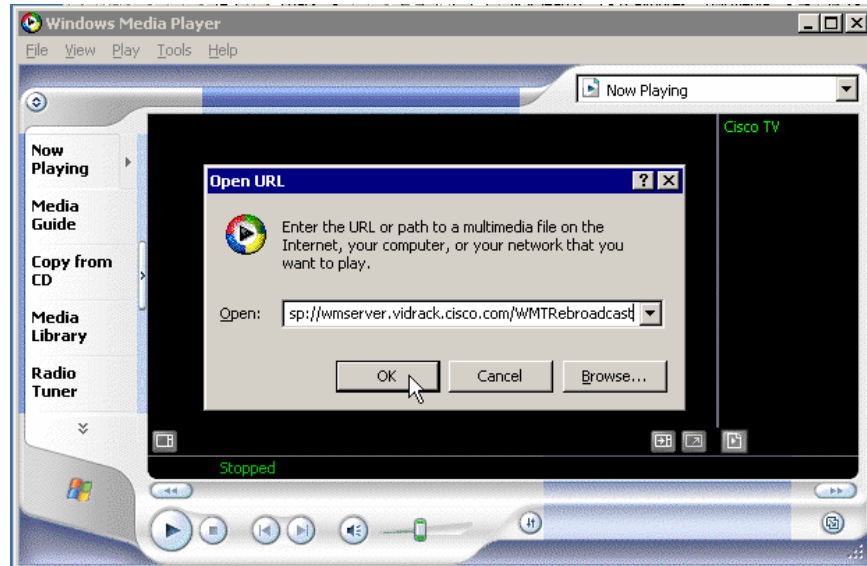
Windows-media byte savings		
% Bytes saved	Incoming(server) bytes	Outgoing(client) bytes
0.00	0 B	0 B

WAAS-EDGE#

6. On the Video Portal tab, click the video link and then click Play Video.



7. Open Windows Media Player and enter the URL specified during program setup in the Cisco DMM: in this case, `rtsp://wmserver.vidrack.cisco.com/WMTRebroadcast`. When you click OK, two requests for the same live video stream will be sent to the origin Windows Media Server at `wmserver.vidrack.cisco.com`.



8. In the edge Cisco WAE telnet session, again show the video statistics:

```

WAAS-EDGE#show statistics accelerator video
VIDEO:
    Global Statistics
    -----
Time elapsed since "clear statistics": 0days 0hr 7min 18sec

Video Connections
=====
Connections handled                                num      %
-----
Total handled                                     2         100.00
Windows-media live accelerated                   2         100.00
Un-accelerated pipethru                         0          0.00
Un-accelerated dropped due to config            0          0.00
Error dropped connections                       0          0.00

Windows-media active sessions                    current   max
-----
Outgoing (client) sessions                      2         2
Incoming (server) sessions                     1         2

Windows-media byte savings
=====
% Bytes saved      Incoming(server) bytes    Outgoing(client) bytes
29.04              2.99 MB                      4.21 MB
WAAS-EDGE#

```

Note: The Windows Media live accelerated count and the number of incoming and outgoing sessions. One stream is incoming from the origin server, and two streams are outgoing from the Cisco WAAS WAE to the requesting clients. In fact, any number of Cisco Video Portal clients can view the live event without incurring additional overhead on the WAN connection to the origin server.

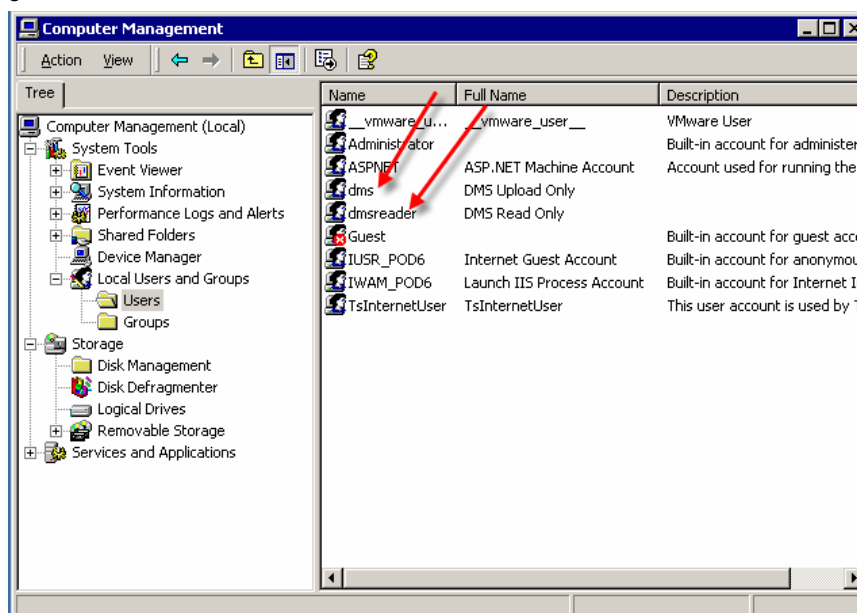
Configuring Video On Demand with Cisco WAAS and Cisco DMS

Configuring Cisco WAAS and Cisco DMS for Windows Media VoD requires setting up a Windows file and web server, configuring Cisco DMM to use the Windows file server, and then configuring Cisco WAAS to preposition the published files to the edge Cisco WAE devices.

Configuring the Windows File and Web Server

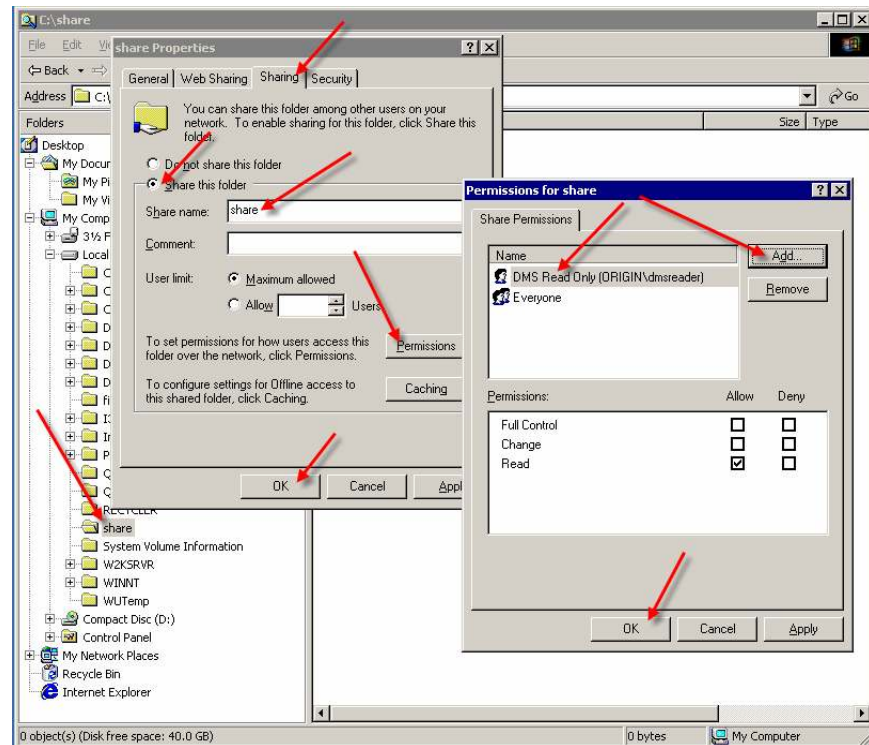
Configuring the Windows file server, origin.waaslab.local, involves setting up an FTP server to allow Cisco DMS to deploy the content to the server and setting up a file share to allow users to access the deployed video content.

1. Create a local username on the origin server specifically for uploading content from Cisco DMM to the file server and create a local username for read-only access to the uploaded content. In the screenshot here, local usernames dms and dmsreader have been created, both have passwords that do not expire, and both have been removed from all groups, including the User group, so that access to any resource on the file server must be explicitly granted.

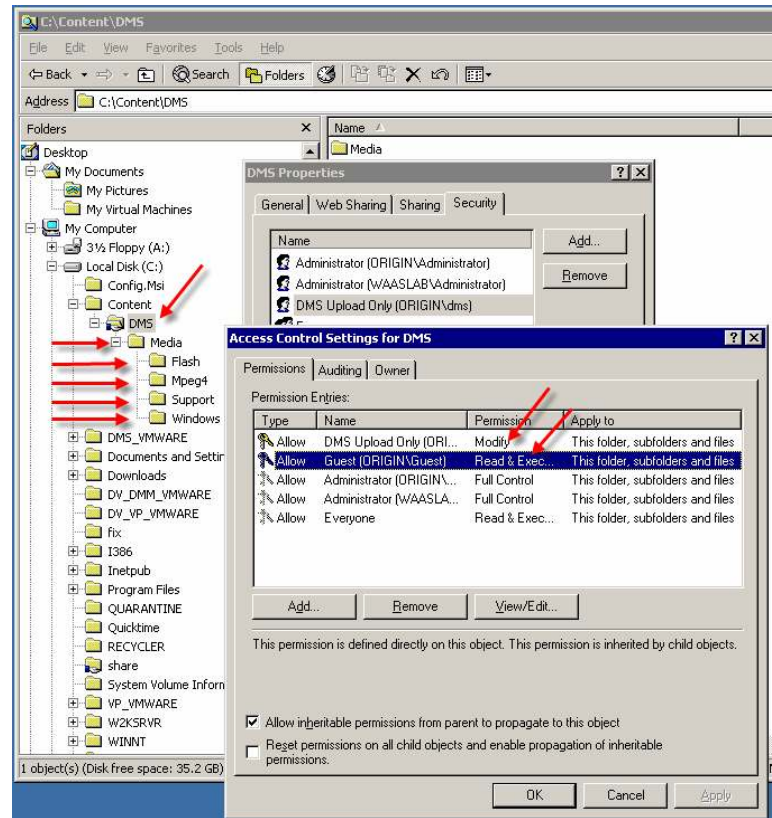


2. To allow users to view content stored on the file server, each user must be given read access to certain shares on the file server and be authenticated to the file server prior to accessing content using the Cisco Video Portal. To do this without compromising the security of the file server or its content, we will create an empty shared file folder called share on the server. In a Microsoft Active Directory environment typical of most enterprises, read-only access to the share can be assigned to one or more Active Directory groups. For this lab setup, we will grant read-only access to the local machine (dmsreader) user. Each user who will use the Cisco Video Portal must mount this share and authenticate with the server prior to accessing the Cisco Video Portal.

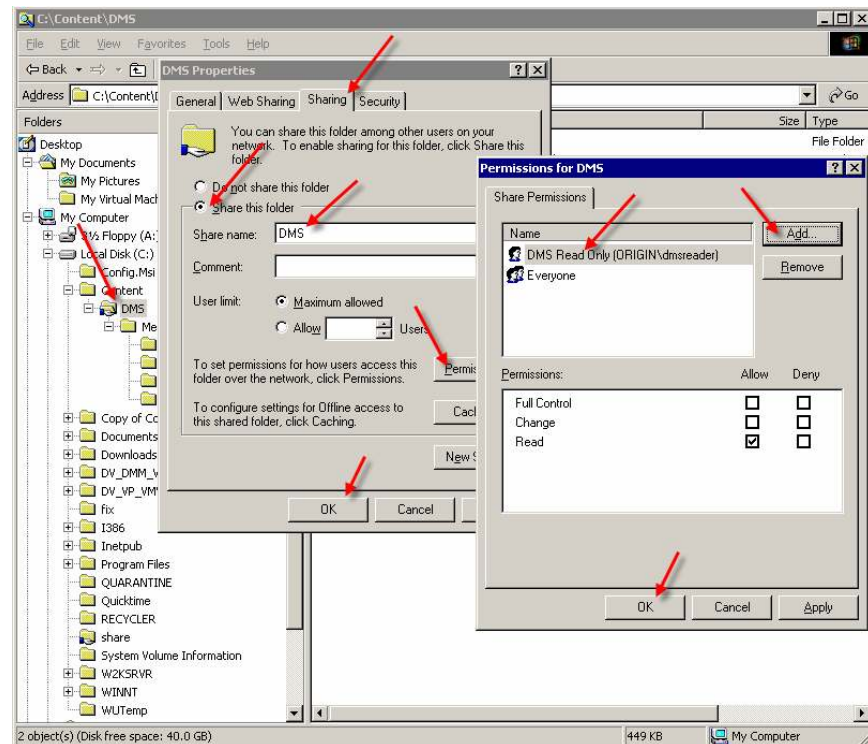
Create a folder named share, right-click the folder and choose Properties. In the “share Properties” dialog box, select the Sharing tab. Click the “Share this folder” radio button and name the share. Click Permissions. In the “Permissions for share” dialog box, click the Add button. A Select Users, Computers, or Groups dialog box will appear (not shown). In the “Look in” drop-down menu, select the origin server. Under Name, find and select the dmsreader username, click Add, and then click OK. Click OK to close the “Permissions for share” dialog box and click OK again to create the share.



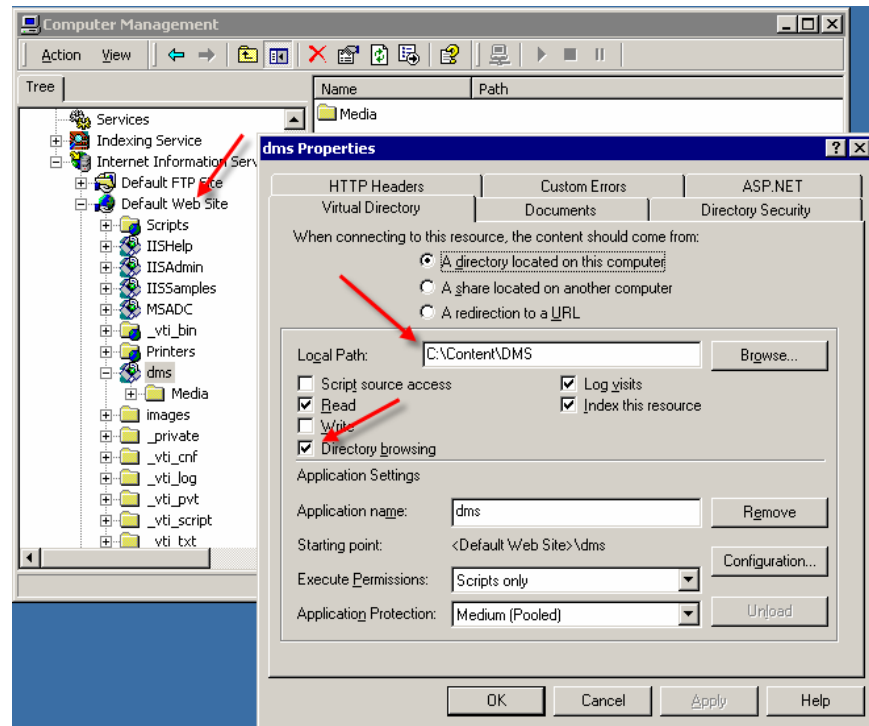
3. Create a folder hierarchy to contain the published media content and share the high-level folder. The screenshot here shows a shared folder called DMS within the Content folder. Inside is a Media folder with subfolders of Flash, Mpeg4, Windows, and Support. Each of these subfolders will contain the corresponding media content type published by the Cisco DMM. The content of each folder will be prepositioned by Cisco WAAS. The Windows Media content in the Windows folder will be served by the Cisco WAAS WAE at the edge. Security for the shared DMS folder is set so that the dms username, used by the Cisco Video Portal deployment facility, can update the folder contents. Each subfolders inherits permissions from the DMS folder.



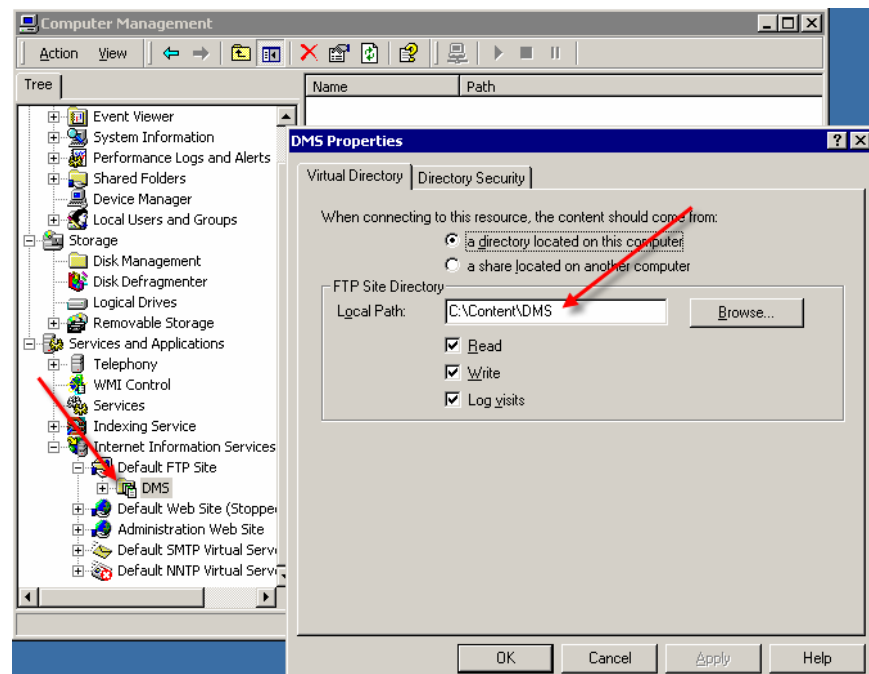
4. Create the DMS folder similar to the way you did the share folder in Step 2. Like the share folder, the DMS folder is shared. Set security for the shared DMS folder so that the dmsreader user can (only) read the folder content.



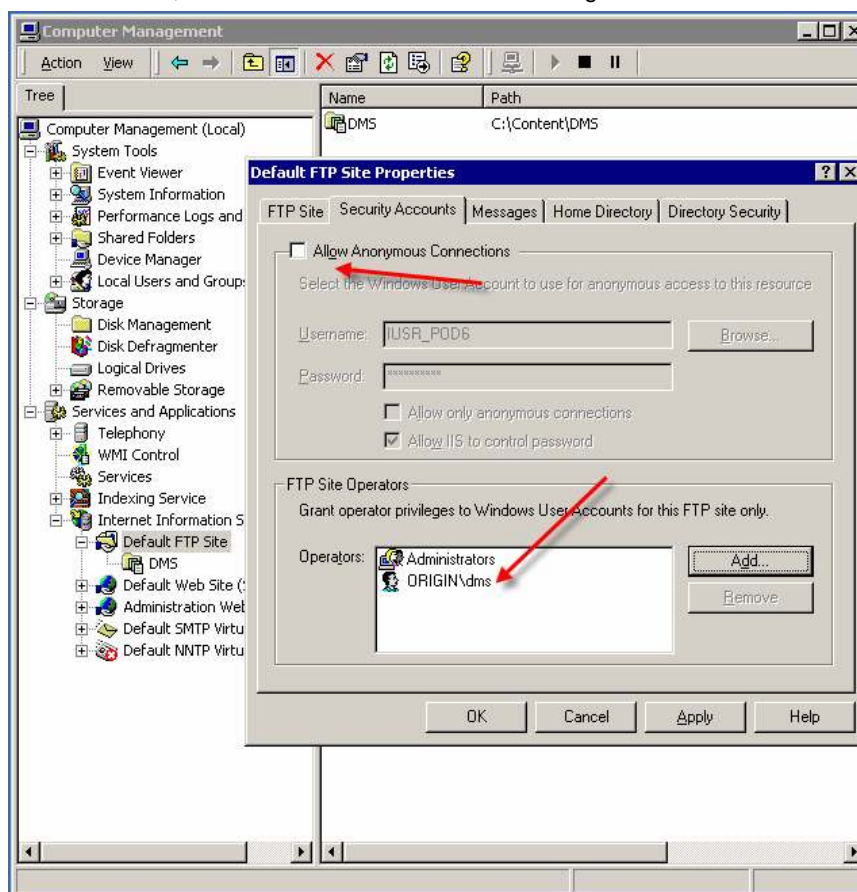
5. From the Computer Management Internet Information Services console, right-click Default Web Site and create a new virtual directory with an alias name of dms. Enter the directory path to the DMS file share created in Step 4 as the website content directory. Enable the Directory Browsing access permission for the new virtual directory.



6. From the Computer Management Internet Information Services console, right-click Default FTP Site and create a new FTP virtual directory called DMS with a local path of the shared DMS folder just created. Give the DMS virtual directory read and write permissions. This FTP site will be used by the Cisco DMM to publish content.



7. In most production environments, anonymous connection to an FTP server is prohibited. If this will be the case, make sure that the dms username is granted access to the FTP server.



Configuring the Cisco DMM Video Portal Module

- In the Cisco DMM Video Portal module, choose Setup > Deployment Locations. Here, we will connect the FTP deployment location with the root URL path. For each file type, Flash, Windows Media Video, Mpeg-4/H.264, and Support, do the following:
 - Choose FTP as the connection type.
 - Enter the root file directory path to the folder created for that specific content type.
 - Enter the host address of the FTP server.
 - Enter the FTP login name and login password created for Cisco DMS to access the FTP server.
 - Enter the root URL path expressed as an HTTP reference for the Flash, Mpeg4, and Support video root URL path, and as a file reference for the Windows Media video root URL path.

Note: Cisco DMS will not be able to check the validity of your Windows Media video root URL path when it is specified as a file path URL. However, you should be able to manually copy this root URL path into the address box of a browser, and it should resolve to the specified directory listing on the origin server.

Cisco Digital Media Manager

Home | Video Portal | Sign Out | Help

Dashboard | **Setup** | Users | Video Portal | Video Portal Reports | Encoders | My Profile

DMM | Video Portal | **Deployment Locations**

SETUP » DEPLOYMENT LOCATIONS

Deployment Locations
Please specify the Deployment Locations for each File type

- File Upload Protocol Type:
 - FTP: Passive FTP (port 21) to the directory using the login information provided. (creates directories as needed by the deploy process)
 - SFTP: Secure FTP (port 22) to the directory using the login information provided. (creates directories as needed by the deploy process)
 - SCP: SSH Secure Copy (port 22) to the directory using the login information provided. (Note: all destination directories must be pre-created when using SCP)
- Root File Directory: the location where all your binary files will be published.
- Root URL Path: the root path where the Video Portal will make HTTP requests for each type of file.

Successfully updated all data

Flash Video

Connection type: Root file directory: ☒ Check Root URL Path: ☒ Check

Host address: Login name: Login password:

Windows Media Video

Connection type: Root file directory: ☒ Check Root URL Path: ☒ Check

Host address: Login name: Login password:

MPEG4/H.264

Connection type: Root file directory: ☒ Check Root URL Path: ☒ Check

Host address: Login name: Login password:

Support
Images, logos, preview videos, sound clips

Connection type: Root file directory: ☒ Check Root URL Path: ☒ Check

Host address: Login name: Login password:

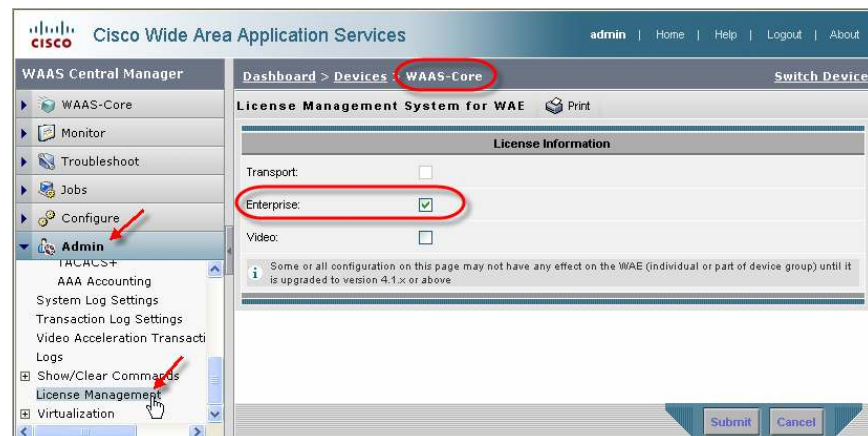
© 2002-2008, Cisco Systems, Inc. All rights reserved. [Warranty and End-User License Agreement](#)

- In the Cisco DMM Video Portal Module, deploy content in the normal way. The Cisco DMM should send the deployed video content through FTP to the respective folders on the origin file server. As shown in the screenshot here, a newly installed Cisco DMM and Cisco Video Portal will have at least one sample video for each content type. Verify that the content is correctly deployed to the origin server.

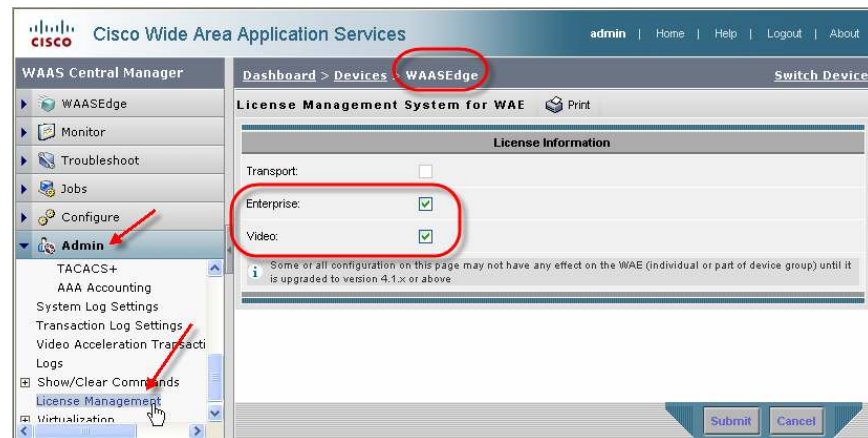
1. This document assumes that the Cisco WAAS deployment has been set up properly, that the standard default policies are in effect, and that traffic interception on the edge Cisco WAE has been set up and tested. For video-specific setup, in the Cisco WAAS Central Manager GUI (<https://<waas-cm-ip-or-fqdn>:8443>), verify the following:
 - a. Both a server-side and an edge Cisco WAAS WAE exist and both are online.

-
- The screenshot shows the Cisco Wide Area Application Services (WAAS) Central Manager interface. The left sidebar contains a navigation menu with the following items: Dashboard, Alerts, Manage Devices (highlighted with a red arrow), Manage Device Groups, Manage Locations, Monitor, Report, Jobs, Configure, and Admin. The main dashboard area is titled 'Dashboard' and includes a search bar, a table of devices, and a filter section. The table lists the following devices:
- | Device Name | Services | IP Address | CMS Status | Device Status | Location | Software Version |
|-------------|-------------------------|---------------|------------|---------------|--------------------|------------------|
| WAAS-CM | CM (Primary) | 192.168.100.2 | Online | | | 4.1.1 |
| WAAS-Core | Application Accelerator | 192.168.101.3 | Online | | WAAS-Core-location | 4.1.1 |
| WAAS-Edge | Application Accelerator | 192.168.202.3 | Online | | WAAS-Edge-location | 4.1.1 |
- The 'WAAS-Core' and 'WAAS-Edge' rows are circled in red. The 'CMS Status' for both is 'Online'. The 'Device Status' column shows a green icon with four dots for each device. The bottom right of the dashboard indicates 'Page 1 of 1'.

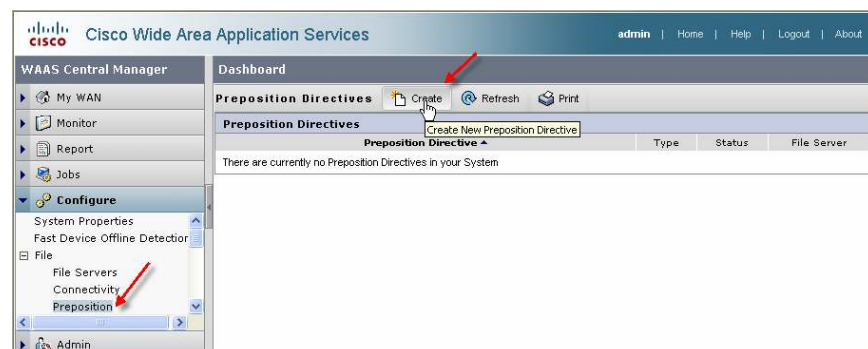
b. The server-side core Cisco WAE has an Enterprise license.



c. The edge Cisco WAE has an Enterprise and a Video license.



2. Create a new preposition directive. A preposition directive allows you to determine which files should be proactively copied from CIFS file servers to the cache of selected edge Cisco WAEs. Prepositioning enables you to take advantage of idle time on the WAN to transfer large or frequently accessed files to selected Cisco WAEs, so that users can benefit from cache-level performance even during first-time access of these files. From the menu list on the left, select Preposition. Then click the Create button.



- Enter a name for this preposition directive, the fully qualified domain name (FQDN) of the origin server, the Cisco WAE location that is closest to the origin server, and the dmsreader username and password that was set up on the origin server for read-only access. Click the Browse button. A browse window will appear below the Root Share and Directories list.

Cisco Wide Area Application Services

admin | Home | Help | Logout | About

WAAS Central Manager

Dashboard

Creating new Preposition Directive, *DMS*

Preposition Settings

Name:

CIFS - Use WAAS transport mode: ☐

Status:

File Server: Location:

User name:

Password: Confirm:

☐ DSCP value for high priority messages: Please make a choice or

Total Size as % of Cache Volume:

Max File Size: KB

Min File Size: KB

Duration: min

Type: min

Ignore Hidden Files and Directories: ☐

Content Settings

Root Share and Directories:

Include Sub Directories: ☒

File Name:

Submit Cancel

Configure the Location field with the CIFS AO device location closest to the file server to facilitate browsing.

- Click the folder next to the DMS/ directory. When the display refreshes, click the folder next to the Media/ directory.

Content Settings

Root Share and Directories:

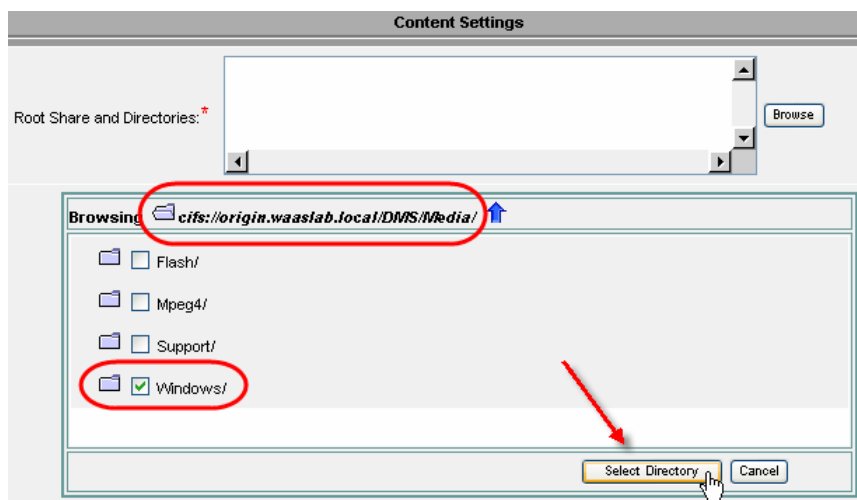
Browse

browsing cifs://origin.waaslab.local/




DMS/

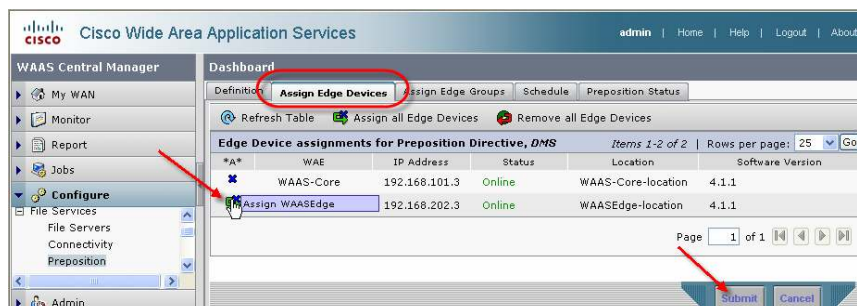
share/

5. Select Windows/ and then click the Select Directory button. /DMS/Media/Windows/ will be added to the Root Shares and Directories list. Click Submit.



Note: For this sample deployment, we are prepositioning only the Windows Media files in the Windows directory as that file type is the only one that can currently be played using a CIFS file-based URL. However, it is advantageous and a best practice to preposition all files in all subdirectories in the DMS/Media directory, subject to available cache disk space. Prepositioning causes the DRE cache to become prepopulated so that when Cisco Video Portal makes a subsequent request for the Adobe Flash, Mpeg4, or Support assets, the download time will be significantly reduced.

6. Four new tabs will appear next to the Definition tab. Select either Assign Edge Devices or Assign Edge Groups. Edge Cisco WAEs can be assigned to this preposition directive using either or both. Click the blue  next to the edge Cisco WAE or defined edge group. The blue  will change to . Click Submit.

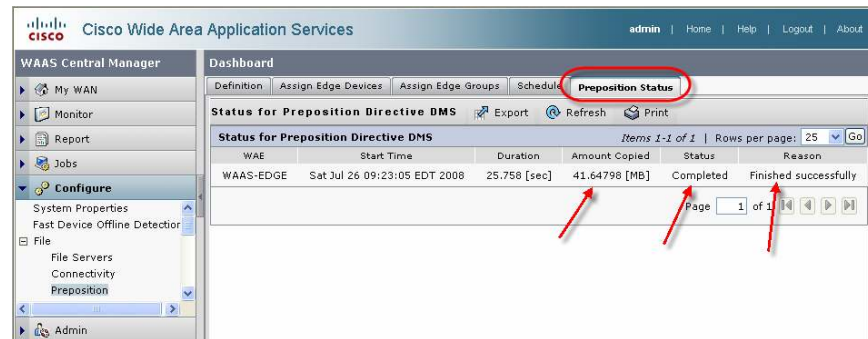


7. After create a preposition directive and assign Cisco WAEs to the directive, you should create a schedule that determines when and how often prepositioning occurs. Select the Schedule tab. This panel allows you to set up a regular schedule for prepositioning content to the edge Cisco WAEs. For this exercise and to immediately test the preposition directive, click Now and then click Submit. Your preposition directive will immediately begin to copy all files in the DMS/Media/Windows directory share.

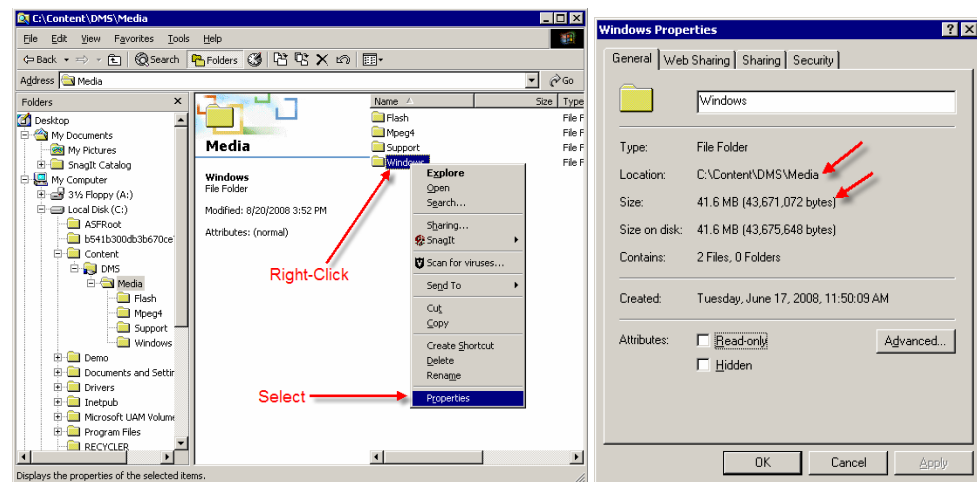
Configuring Setup Verification

Verifying Prepositioning

1. To monitor the preposition directive status, select the Preposition Status tab. Click the Refresh button until the Status column shows Completed.

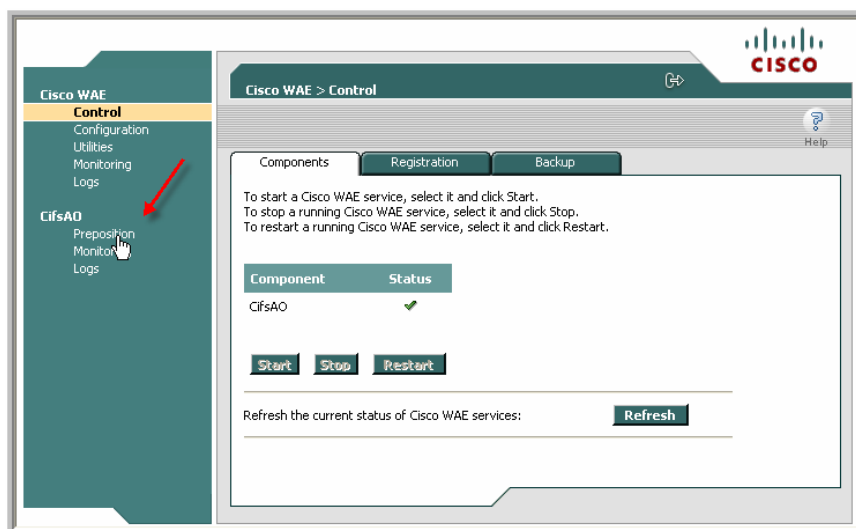


2. You can verify that the amount copied approximately equals the size of the prepositioned directory content. To do so, right-click on the folder name in Windows Explorer and select Properties.

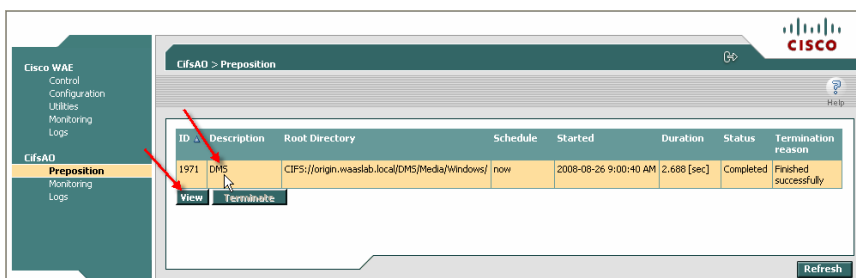


3. To monitor the preposition directive status on a particular edge Cisco WAE, from the Cisco WAAS Central Manager GUI, under My WAN, select Manage Devices and select the edge Cisco WAE that will be monitored. In the Device Info panel, click Device GUI. A new window will appear showing the edge Cisco WAE GUI.

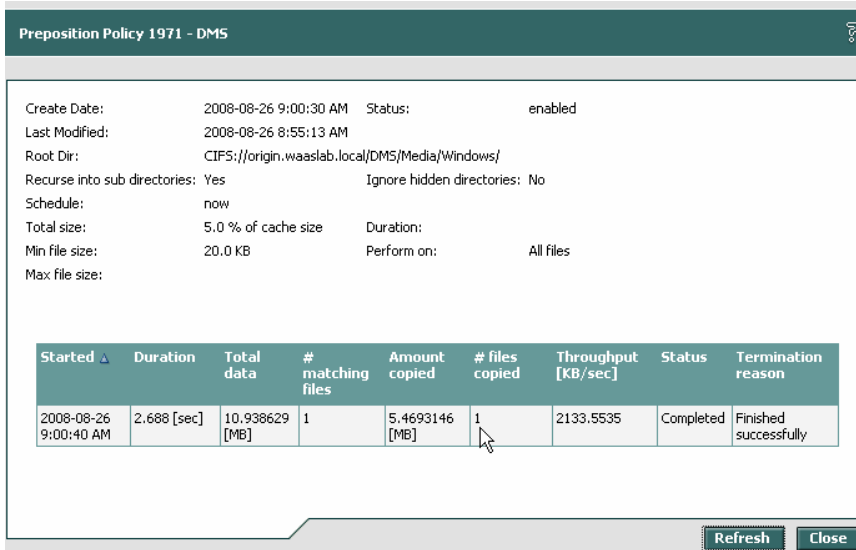
4. Under CifsAO, click Preposition.



5. A list of all preposition directives for this device will be displayed. Click the line of the DMS preposition directive and click View.



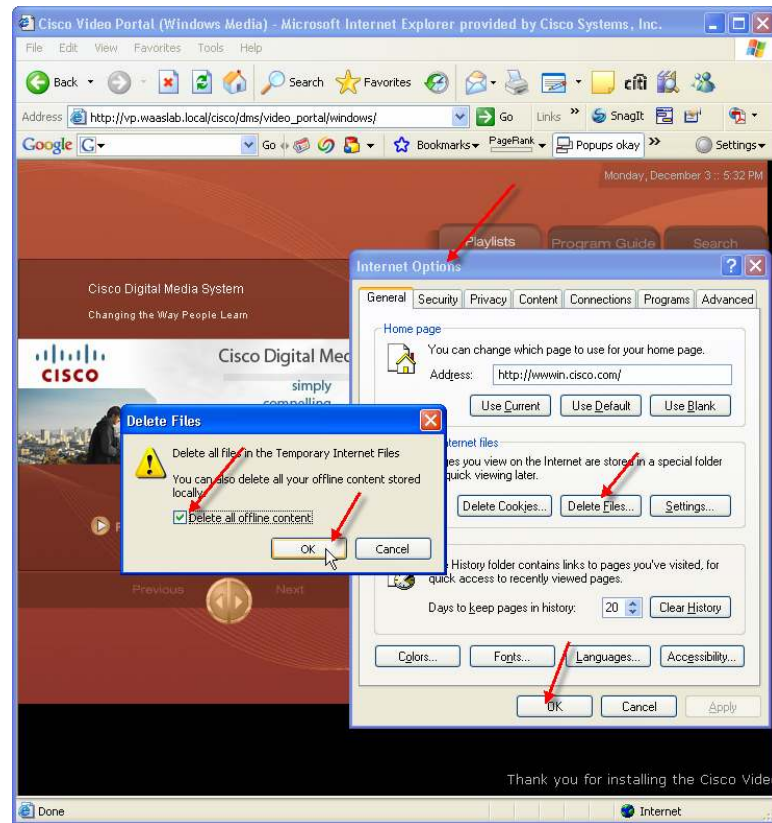
The current status of the directive will be displayed. In the screenshot here, the preposition directive has completed successfully.



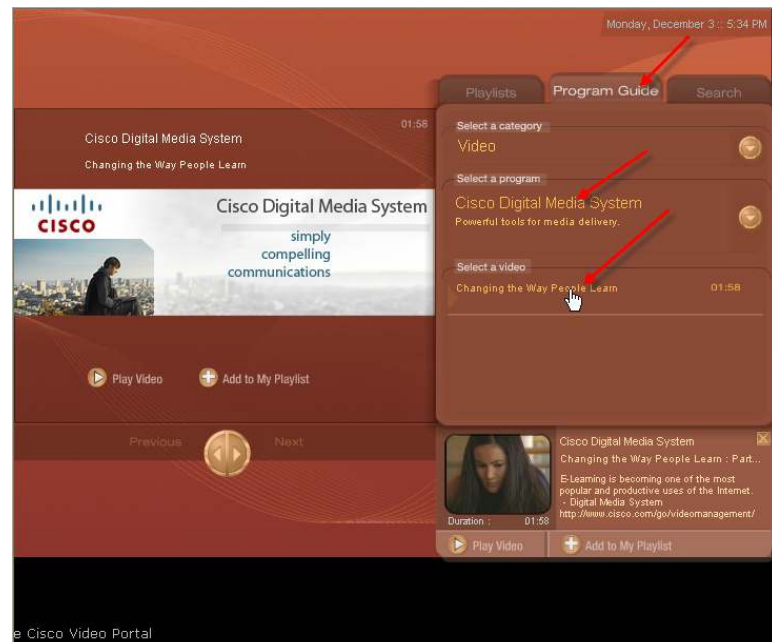
6. Close the Preposition Policy status window, but do not close the edge Cisco WAE GUI window. We will use it again in this document to verify the setup.

Verifying Cisco DMS Setup

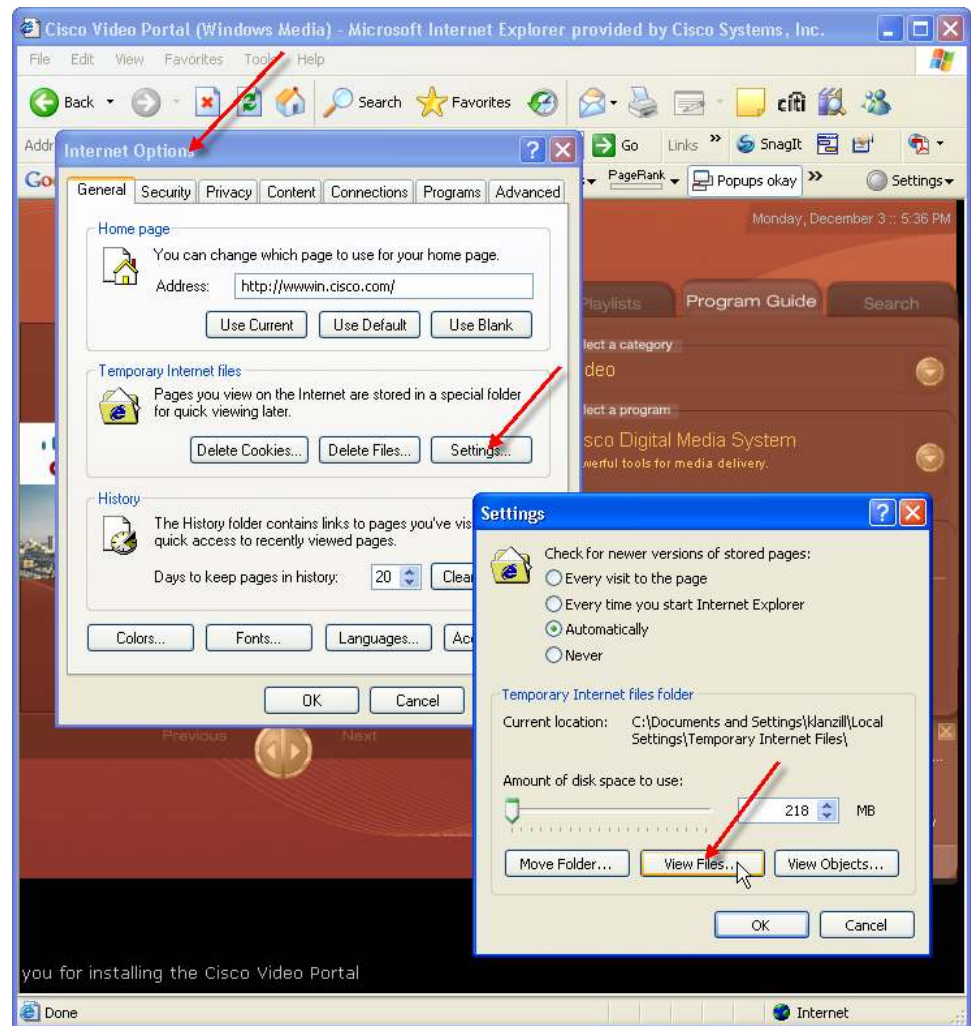
1. Open a browser window and enter the address to the installed Cisco Video Portal (<http://<vp-fqdn>>). Delete all temporary Internet files.



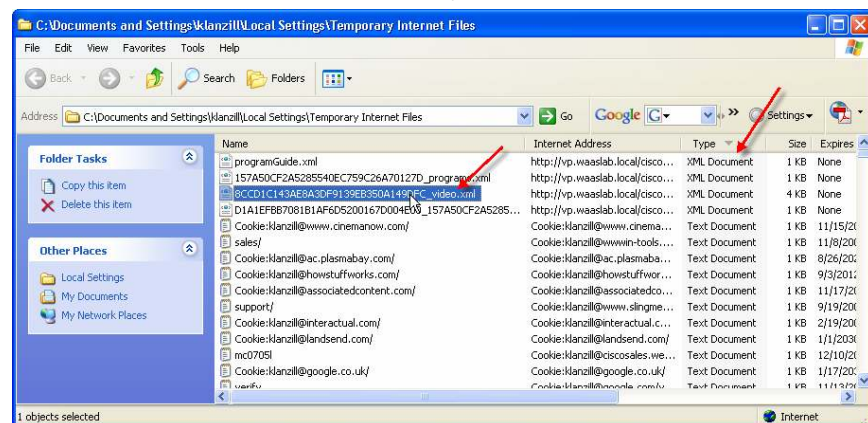
2. Click the Program Guide tab. Click the Cisco Digital Media System program and then select the video displayed. Do not play the video yet.



3. In the browser's Tools menu, choose Internet Options. In the Internet Options dialog Box, click Settings. In the Settings dialog box, click View Files. A new browser window will appear showing all temporary Internet files and cookies.

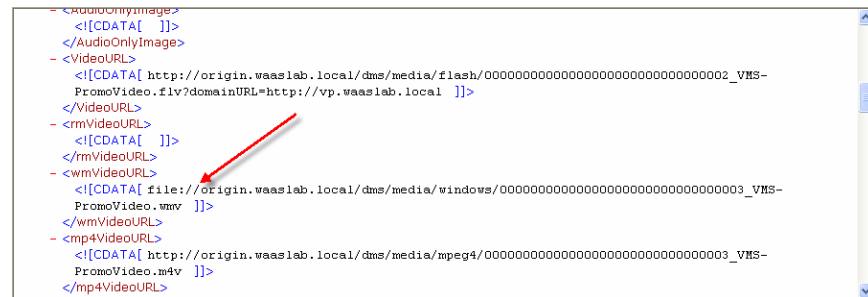


4. Perform a reverse sort on Type so that the XML files are at the top of the list. You are looking for the file that ends with “_video.xml.” This XML file contains the metadata for the selected video. Double-click the filename to display the file in a new browser window.



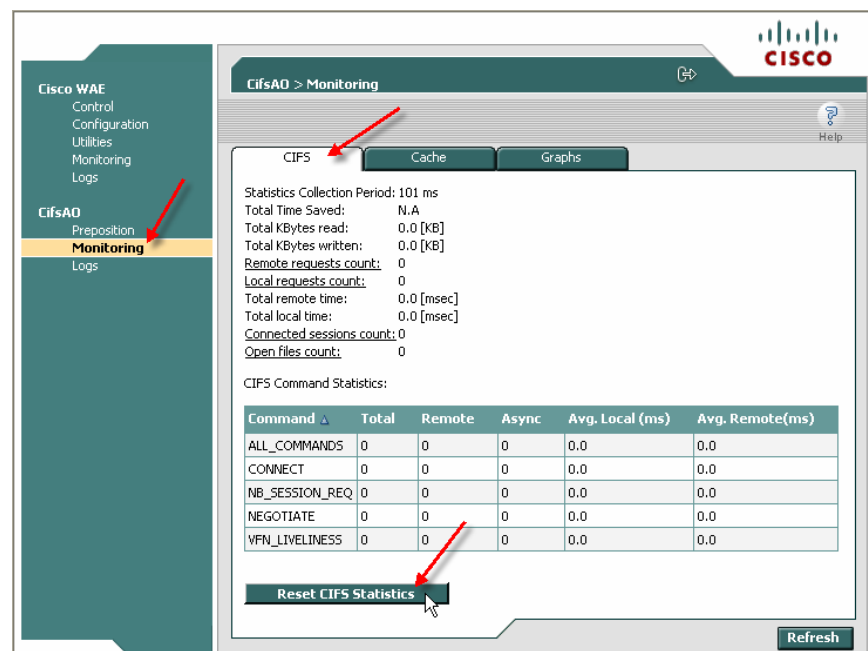
5. Scroll down the XML file display looking for the <wmVideoURL> XML tag. Note that the URL is a well-formed file-access URL. This URL can be copied and entered directly in Windows

Media Player (WMP) and will be used by the embedded WMP contained in the Cisco Video Portal.

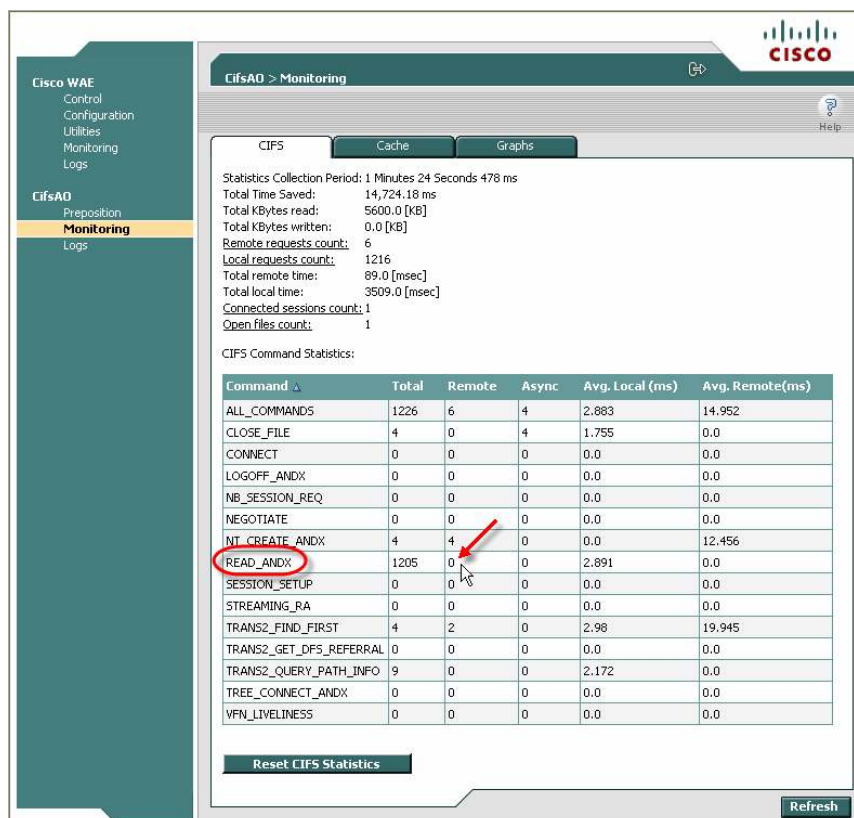


Verifying Playback of Prepositioned Video

1. Return to the edge Cisco WAAS WAE GUI browser window and, under CifsAO, select Monitoring. Select the CIFS tab and click Reset CIFS Statistics. Your display may not contain all the CIFS commands shown in the screenshot here.



2. Back in the Cisco Video Portal browser window, close the Settings and Internet Options dialog box. In the Cisco Video Portal browser window, click the Play Video button for the selected video. Play the video through to the end.
3. In the edge Cisco WAAS WAE GUI browser window, click Refresh. The CIFS command statistics will be displayed showing the total commands processed for each type and the number that were processed remotely. The difference will be the commands processed by the edge Cisco WAE. Note that the READ_ANDX command was processed completely on the local Cisco WAE, indicating that the played video file was served completely from the local Cisco WAAS WAE.



Conclusion

By combining the digital media management capabilities of Cisco DMM and Cisco Video Portal, with the file distribution and HTTP application optimization capabilities of Cisco WAAS, Cisco can offer a simple end-to-end solution to the problems associated with delivering high-quality, high-bandwidth VoD to today's global enterprises.

For More Information

For more information, please visit <http://www.cisco.com/go/waas> and <http://www.cisco.com/go/dms>.



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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCOVR, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)