CHAPTER 11

Configuring Wide Area File Services

This chapter describes how to configure Wide Area File Services (WAFS), which allows branch office users to more efficiently access data stored at centralized data centers. The WAFS feature overcomes the WAN latency and bandwidth limitations by caching data on Edge WAEs near branch office users.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances and WAE Network Modules (the NME-WAE family of devices).

This chapter contains the following sections:

About File Services

Enterprises today have remote offices in different parts of the country and around the world. Typically, these remote offices have their own file servers to store and manage the data needed by their local users.

The problem with this method of operation is that it is costly to purchase, manage, and upgrade file servers at each remote office. A great deal of resources and manpower must be dedicated to maintaining these file servers, and especially to protect the data in case of server failure. To achieve the required level of data assurance, the remote office must devote resources to back up the data at the remote site and physically move it to a secure location, often at a considerable distance from the site. If you multiply this scenario by tens, hundreds, and thousands of remote offices, and you can see that this approach to enterprise data management not only raises costs exponentially, it also greatly increases the risks to critical data.

The logical solution in this scenario is to move all of the enterprise's important data to a central location containing the facilities, trained personnel, and storage mass required to manage the data properly. By having a data center provide backup and other storage management facilities, the enterprise can achieve better utilization of both personnel and storage, as well as a higher level of data assurance and security.

The WAN between the enterprise's data center and its remote offices tends to be unreliable and slow, with limited bandwidth and high latency. In addition, the WAN creates other obstacles to the implementation of the data center solution.

One obstacle is created by the file server protocols that operate over the WAN. CIFS, which is the file server protocol for Windows was designed to operate over a LAN. Every file operation generates several exchanges of protocol messages between the client and the file server. This situation is usually not noticeable on the LAN, but quickly causes high latency over the WAN. Occasionally, this high latency breaks the file server protocol altogether.

Even in cases where the file server protocol is managing to function correctly over the WAN, there are typically long delays between each transaction. These delays can often cause timeouts in user applications such as word processing programs, image editing programs, and design tools, which stops them from functioning correctly.

All of these problems—unreliable WANs, file system protocol compatibility, and user application compatibility—contribute to an unfriendly work environment that negatively affects the user experience and diminishes productivity.

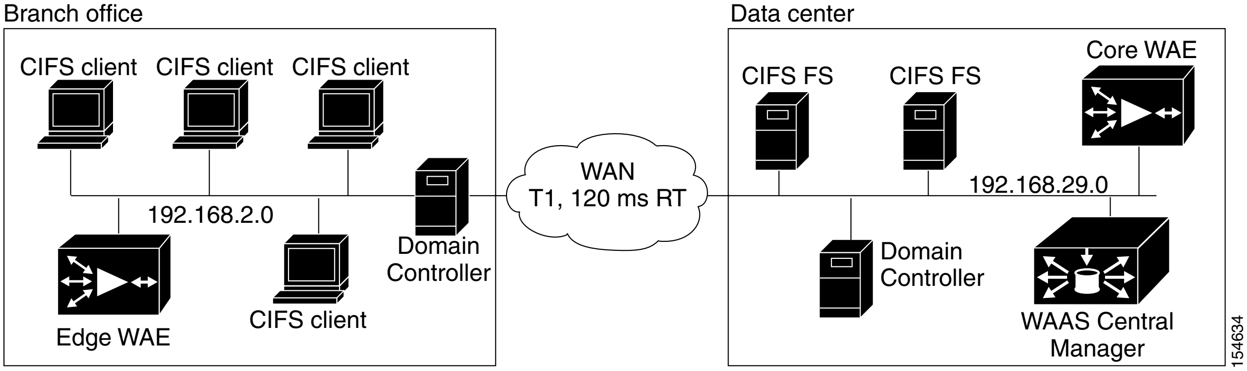
File Services Solution

The WAAS file services feature overcomes the WAN latency and bandwidth limitations by caching data on Edge WAEs near the user. This data caching method allows branch office users to access centralized data at LAN-like speeds over the WAN. The solution is based on several key concepts:

- **Use the WAN as little as possible**—By minimizing the number of operations that need to traverse the WAN, WAAS effectively shields users from many of the obstacles that WANs create.
- **Use the WAN optimally**—The file services feature uses sophisticated caching, compression, and network optimization technologies, which enable the system to use the WAN optimally.
- **Preserve file system protocol semantics**—Although Cisco WAAS uses its own proprietary protocol over the WAN, it leaves the complete semantics of the standard file system protocol commands intact. This is essential to preserve the correctness and coherency of the data in the network.
- **Make the solution transparent to users**—The best solutions are the ones that do their jobs unnoticed, without interfering with end users' operations or forcing users to change their ways of doing business. The WAAS file services solution does not require any software installations, either on the server side or at the client, and does not require the user to learn anything new. Users derive all the benefits of having a secure data center without needing to change any of their work habits.

By using the WAAS file services feature, enterprises can consolidate their file servers to a data center that provides the facilities, IT personnel, and storage devices required to manage the data properly. Figure 11-1 shows a typical deployment scenario after WAAS file services have been set up.

Figure 11-1 WAAS File Services Solution



Overview of File Services Features

The WAAS file services features are described in the following sections:

- Automatic Discovery, page 11-3
- Prepositioning, page 11-4
- Data Coherency, page 11-4
- Data Concurrency, page 11-5
- File Blocking, page 11-6
- Microsoft Interoperability, page 11-6

Automatic Discovery

The automatic discovery feature allows you to enable WAFS without having to register individual file servers in the WAAS Central Manager as described in the "Setting Up File Servers to Export to the Edge WAE Cache" section on page 11-15. With the automatic discovery feature, WAAS will attempt to automatically discover and connect to a new file server when a transparent mode CIFS request is received. If there are multiple paths to the file server, WAAS chooses the path with the lowest latency.

If the latency between the core WAE and the discovered server is more than 25 milliseconds, the server is considered to be too far away, and the connection will not be optimized. Additionally, if the latency between the edge WAE and the server is less than 2 milliseconds, the server is considered to be local, and the connection will not be optimized.

The automatic discovery feature operates by default for CIFS requests to unregistered file servers. You may still want to register file servers, however, because WAFS functions are limited when interacting with automatically discovered file servers. With automatically discovered file servers, the following WAFS features are not available: prepositioning, dynamic shares, file blocking, and disconnected mode. Additionally, if the file server requires a digital signature, WAFS cannot cache its data.

As new file servers are added to the policy engine dynamic map, you can see them by using the **show policy-engine application dynamic** EXEC command. A file server remains in the dynamic map for three minutes after the last connection to it is closed.

Prepositioning

The prepositioning feature allows system administrators to proactively “push” frequently used files from the central storage into the cache of selected Edge WAEs. This operation provides users with faster first-time file access, and makes more efficient use of available bandwidth. You create preposition directives from the WAAS Central Manager GUI.

When an end user attempts to open a file that is not found in the Edge WAE cache, the Edge WAE retrieves it across the WAN from the file server where it is stored. Prepositioning is a feature that allows administrators to push large, frequently accessed files from file servers to selected Edge WAE caches according to a predefined schedule. Through the proper use of prepositioning, administrators can allow users to benefit from cache-level performance even during first-time access of these files. Prepositioning improves WAN bandwidth utilization by transferring heavy content when the network is otherwise idle (for example, at night), which frees up bandwidth for other applications during the day.

The WAAS Central Manager GUI allows administrators to create multiple, overlapping preposition policies (each with its own schedule), a list of target Edge WAEs, and defined time and size constraints.

Note Prepositioning includes the ability to configure multiple roots. See the “Creating a New Preposition Directive” section on page 11-27.

Data Coherency

Cisco WAAS ensures data integrity across the system by using two interrelated features – *coherency*, which manages the freshness of the data, and *concurrency*, which controls the access to the data by multiple clients.

Maintaining multiple copies of data files in multiple locations increases the likelihood that one or more of these copies will be changed, causing it to lose consistency or coherency with the others. Coherency semantics are used to provide guarantees of freshness (whether the copy is up-to-date or not) and the propagation of updates to and from the origin file server.

Cisco WAAS applies the following coherency semantics to its built-in coherency policies:

- **Strict CIFS behavior for intra-site—**Users of the same cache are always guaranteed standard, strict CIFS coherency semantics.
- **Cache validation on CIFS open—**In CIFS, the **File Open** operation is passed through to the file server. For coherency purposes, Cisco WAAS validates the freshness of the file on every file open, and invalidates the cached file if a new version exists on the file server.

  Cisco WAAS validates data by comparing the time stamp of a file in the cache to the time stamp of the file on the file server. If the time stamps are identical, the cached copy on the Edge WAE is considered valid and the user is permitted to open the file from the Edge WAE cache.

  If the time stamps are different, the Edge WAE removes the file from its cache and requests a fresh copy from the file server.
- **Proactive cache updating**—Cisco WAAS supports the use of change notifications in CIFS environments as a way to keep cached data on the Edge WAEs up-to-date.

  When a client makes a change to a directory or file, the Edge WAE sends a change notification to the file server. The file server then sends to all the Edge WAEs a change notification that includes a list of the modified directories and files. Upon receiving the change notification, each Edge WAE checks its cache and invalidates the directories and files listed in the notification, and then updates its cache with the latest versions.

For example, if a user edits an existing Word document and saves the changes to the Edge WAE cache, the Edge WAE sends a change notification to the file server so it knows that the file has been modified. The Edge WAE then sends the changed sections to the file server, and the file server proactively sends change notifications to the other Edge WAEs in the network. These Edge WAEs then update their cache so the file is consistent across all access points.

This process also applies when you rename a directory, add a new subdirectory, rename a file, or create a new file in a cached directory.

- **Flush on CIFS close—**In CIFS, the **File Close** operation forces all write buffers to be flushed to the file server, and the **Close** request is only granted after all updates have been propagated to the file server. From a coherency standpoint, the combination of validate on file open and flush on file close ensures that well-behaved applications, such as Microsoft Office, operate in session semantics. The Open, Lock, Edit, Unlock, and Close commands are guaranteed to work correctly on the Cisco WAAS network.
- **Age-based validation on directories (CIFS)—**Directories are associated with a preconfigured age. When the age expires, the Edge WAE cache revalidates the directory.

  When a user first attempts to view the contents of a directory, the Edge WAE enables the file server to perform the authorization check using the directory's access control list (ACL), which contains the user and group permissions. The Edge WAE monitors which directories the user has accessed and whether the file server permitted that access. If the user tries to access the same directory again during a short period of time (aging period), the Edge WAE does not contact the file server and instead uses the cached permissions to determine if the user should be provided access. After the aging period expires, the Edge WAE contacts the file server to refresh the cached permission of the user.

  This authorization process prevents users from accessing directories and files in the cache that they do not have permission to access on the file server.

Data Concurrency

Concurrency control is important when multiple users access the same cached data to read, or write, or both. Concurrency control synchronizes this access by establishing and removing file system locks. This file-locking feature ensures data integrity and provides the following benefits:

- Enables a client to aggressively cache file data so it does not have to rely on retrieving data from the remote file server.
- Provides a performance boost in many applications running on existing CIFS client implementations.
- Preserves data integrity because only one user at a time can make changes to a section of a file.

Cisco WAAS supports the CIFS oplocks feature, which allows a user to lock a file so the user can safely read and write data to its local cache instead of using network bandwidth to perform these functions over the WAN on the file server. By using oplocks, a user can proactively cache read-ahead data because it knows that no other user is accessing the file so there is no chance the cached data can become stale. The user can also write data to its local cache and does not need to update the file server until it closes the file or until another user requests to open the same file.

Oplocks only applies to files. The file server does not grant oplock requests on directories and named pipes.

File-Locking Process

When a user opens a file, it sends a lock request to the file server. The Edge WAE intercepts and forwards all lock requests from the user to the file server as well as all responses from the file server to the user. If no other user has a lock on the file, the file server grants an exclusive lock request so that the user can safely cache the file.

If a second user requests to open the same file, the following actions occur:

1. The file server revokes the exclusive file lock obtained by the first user.
2. The first user performs the following actions:
   - Flushes any file changes stored in its cache to the file server. This action ensures that the second user opening the file receives the latest information from the file server.
   - Deletes any of its read-ahead buffers for the file because that data is no longer guaranteed to remain up-to-date now that a second user will open the file.
3. The file server allows the second user to open the file.

File Blocking

The file-blocking option allows you to define one or more file-blocking directives that prevent users from opening, creating, or copying files that match a defined file pattern. These directives, which apply to all Edge WAEs enabled with file services, prevent limited bandwidth, as well as file server and cache space, from being wasted on files that you decide to block.

Microsoft Interoperability

The WAAS file services feature interoperates with these Microsoft CIFS features:

- Active Directory for user authentication and authorization
- Offline folders in Microsoft CIFS
- Microsoft DFS infrastructure
- Windows shadow copy for shared folders, as described in the "Windows Shadow Copy for Shared Folders" section on page 11-6)

Windows Shadow Copy for Shared Folders

WAAS file services support the Shadow Copy for Shared Folders feature that is part of the Windows Server 2003 operating system. This feature uses the Microsoft Volume Shadow Copy Service to create snapshots of file systems so that users can easily view previous versions of folders and files.

In a WAAS environment, users view shadow copies in the same way they would in a native Windows environment by right-clicking a folder or file from the Edge WAE cache and choosing **Properties > Previous Version**.

For more information about Shadow Copy for Shared Folders, including the limitations of the feature, refer to your Microsoft Windows Server 2003 documentation.

Users can perform the same tasks when accessing a shadow copy folder on the Edge WAE as they can in the native environment on the file server. These tasks include the following:

- Browsing the shadow copy folder
- Copying or restoring the contents of the shadow copy folder
- Viewing and copying files in the shadow copy folder

The Shadow Copy for Shared Folders feature does not support the following tasks:

- Renaming or deleting a shadow copy directory
- Renaming, creating, or deleting files in a shadow copy directory

Supported Servers and Clients

WAAS supports Shadow Copy for Shared Folders on the following file servers:

- Windows 2003 (with and without SP1)
- NetApp Data OPTap versions 6.5.2, 6.5.4 and 7.0
- EMC Celerra versions 5.3 and 5.4

WAAS supports Shadow Copy for Shared Folders for the following clients:

- Windows XP Professional
- Windows 2000 (with SP3 or later)
- Windows 2003

Note Windows 2000 and Windows XP (without SP2) clients require the Previous Versions Client to be installed to support Shadow Copy for Shared Folders. For more information, refer to the following Microsoft article:

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/22a0add1-d224-47ee-8f6e-65103fb63e23.mspx

Preparing for File Services

Before enabling file services on your WAEs, make sure that you complete the following tasks:

- If you want to configure multiple devices with the same settings, make sure that you have created a device group that contains all the edge devices you want to enable with file services. For information on creating device groups, see Chapter 3, "Using Device Groups and Device Locations."
- Identify the edge devices on which you want to enable file services. An edge device may also serve as a core device if it also exports local file servers to other edge devices.
- Identify the file servers that you want to export, and refer to Table 11-1 to verify that these file servers are supported by Cisco WAAS.

Table 11-1 Supported File Servers

Vendor	Product	Version
Dell	PowerVault	715N
Network Appliance	FAS270 FAS250 F760 F85	ONTAP 7.0.1R.1 ONTAP 7.0.1R.1 6.5.2R1P16 6.4.5
Spinnaker	SpinServer 3300	2.5.5p2 (Kernel 2.4.18spinos)
EMC	Celerra NS702 Celerra NS702 Celerra NS501	5.4.17.5 5.4.14-3 5.3.12-3
Microsoft	Windows NT 4.0 Windows Server 2000 Windows Server 2003	 No service pack, SP1, SP3, and SP4 No service pack, SP1, and R2
Novell[1]	6.5	SP-3
RedHat	Samba	3.0.1.4a

[1] WAAS supports Novell 6.5 for CIFS optimization, server consolidation, and generic network acceleration for NCP, eDirectory/NDS, and iPrint. If your Novell file server uses the NFAP option, WAAS can optimize your Novell traffic at the transport layer as well as at the protocol layer using the WAAS CIFS adapter. NFAP is Novell's Native File Access Pack that uses the CIFS protocol on top of Novell's NCP (Novell Core Protocol).

Using File Services on the NME-WAE

If you are running WAAS on a network module that is installed in a Cisco access router, there are specific memory requirements for supporting edge and core file services. To enable edge file services, the NME-WAE must contain at least 1 GB of memory. To enable core file services or both core and edge file services, the NME-WAE must contain at least 2 GB of memory. If you try to enable edge or core file services and the device does not contain enough memory, the WAAS Central Manager will display an error message.

You can check the amount of memory that a device contains in the Device Home window. For details, see the "Device Home Window" section on page 15-10.

Configuring File Services

Table 11-2 provides an overview of the steps you must complete to configure file services.

Table 11-2 Checklist for Configuring File Services

Task	Additional Information and Instructions
1. Prepare for file services.	Provides the tasks you need to complete before enabling and configuring file services on your WAAS devices. For more information, see the "Preparing for File Services" section on page 11-7.

Table 11-2 Checklist for Configuring File Services (continued)

Task	Additional Information and Instructions
2. Configure a WAFS core cluster.	WAFS core clusters are required to copy data from the exported file server to the cache of the Edge WAEs. For more information, see the "Configuring the Core Cluster" section on page 11-9.
3. Configure the edge devices.	By default, file services are not enabled on your WAAS devices. To enable and start file services on edge devices, see the "Configuring the Edge Devices" section on page 11-12.
4. Register a file server with the WAAS Central Manager (optional).	Identifies to the WAAS system which file servers to export. This step also creates a link between a core cluster and the registered file server. For more information, see the "Setting Up File Servers to Export to the Edge WAE Cache" section on page 11-15. This step is optional if you are using automatic discovery.
5. Identify dynamic shares (optional).	Identifies the dynamic shares on a exported file server. If your file server does not contain dynamic shares, you can skip this step. For more information, see the "Creating Dynamic Shares for Registered File Servers" section on page 11-19.
6. Create a connection between a core cluster and your edge devices.	Enables a core cluster to copy data to the Edge WAE cache. For more information, see the "Creating a Connection Between a Core Cluster and Edge WAEs" section on page 11-21.
7. Create a file blocking directive (optional).	Defines the type of files that cannot be opened, created, or copied by end users. For more information, see the "Creating a File-Blocking Directive" section on page 11-25.
8. Create a preposition directive (optional).	Defines which files are proactively copied from an exported file server to the Edge WAE cache. For more information, see the "Creating a Preposition Directive" section on page 11-26.

Configuring the Core Cluster

The first step in setting up file services is to enable Core services on a device and assign the device to a Core cluster. The Core cluster will be responsible for copying data from the exported file server (or multiple file servers) to the cache of the Edge WAEs. In later sections you will assign edge devices and, optionally, file servers to this core cluster, so the cluster knows which file servers to export and which edge devices to populate with cached data.

In Steps 1 through 7 you enable core server services and assign the device to a Core cluster. In Steps 8 through 12 you configure the new core cluster. The last step in this procedure describes how to reload the device, which is required for the device to function as a Core WAE.

To create a WAFS core cluster, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices**.

The Devices window displays a list of devices created on your WAAS system.

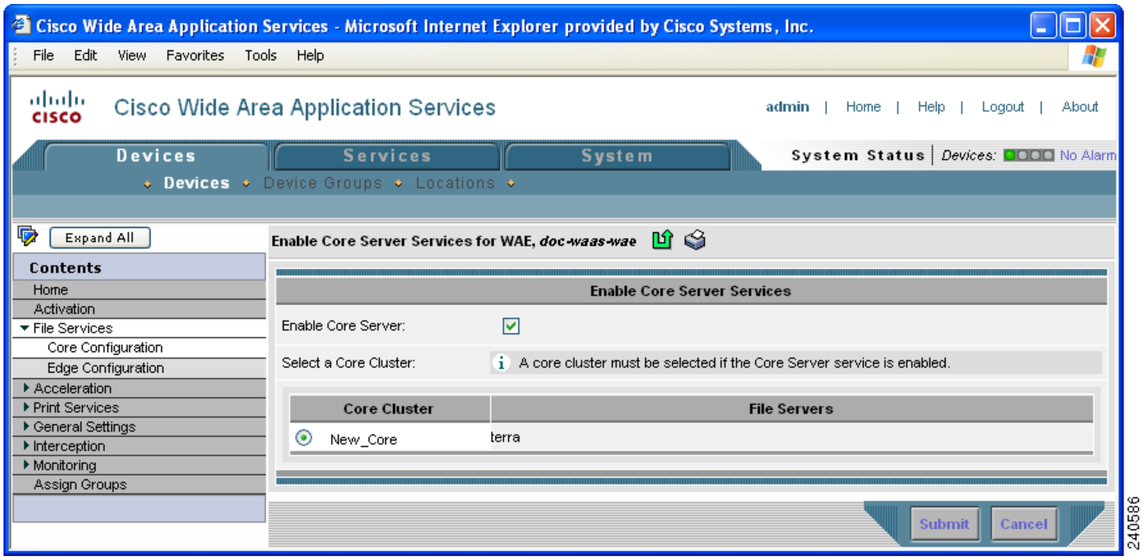
Step 2 Click the **Edit** button next to the device that you want to be a member of the new core cluster.

The Device Home window appears.

Step 3 From the Contents pane, select **File Services > Core Configuration**.

The Enable Core Server Services window appears. (See Figure 11-2.)

Figure 11-2 Enabling Core Server Services


Cisco Wide Area Application Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
Devices Services System
System Status | Devices: No Alarm
Devices Device Groups Locations
Expand All
Contents
Home
Activation
File Services
Core Configuration
Edge Configuration
Acceleration
Print Services
General Settings
Interception
Monitoring
Assign Groups
Submit
Cancel
240586

Enable Core Server Services for WAE, *doc-waas-wae*

Enable Core Server Services

Enable Core Server: ☑

Select a Core Cluster: A core cluster must be selected if the Core Server service is enabled.

	Core Cluster	File Servers
●	New_Core	terra

Step 4 Check the **Enable Core Server** check box.

Step 5 Use one of the following methods to assign this device to a core cluster:

- To create a new core cluster for this device, select the radio button next to the empty Core Cluster field, and enter a name for the new core cluster in this empty field. This name cannot contain spaces or special characters.
- To have this device join an existing core cluster, select the radio button next to that core cluster. If you do not have any existing core clusters, your only option is to create a new core cluster for this device.

Step 6 Click **Submit**.

A pop-up message is displayed that the device must be manually rebooted for the device to function as a Core server.

Step 7 Click **OK** after reading the pop-up message.

Core Server services are enabled on the device and the device joins the specified Core cluster. The last step in this section describes how to reboot the device, which is required for the Core services to be activated.

If you click **Cancel** on the pop-up message you are returned to the Enable Core Server window and your changes are not submitted.

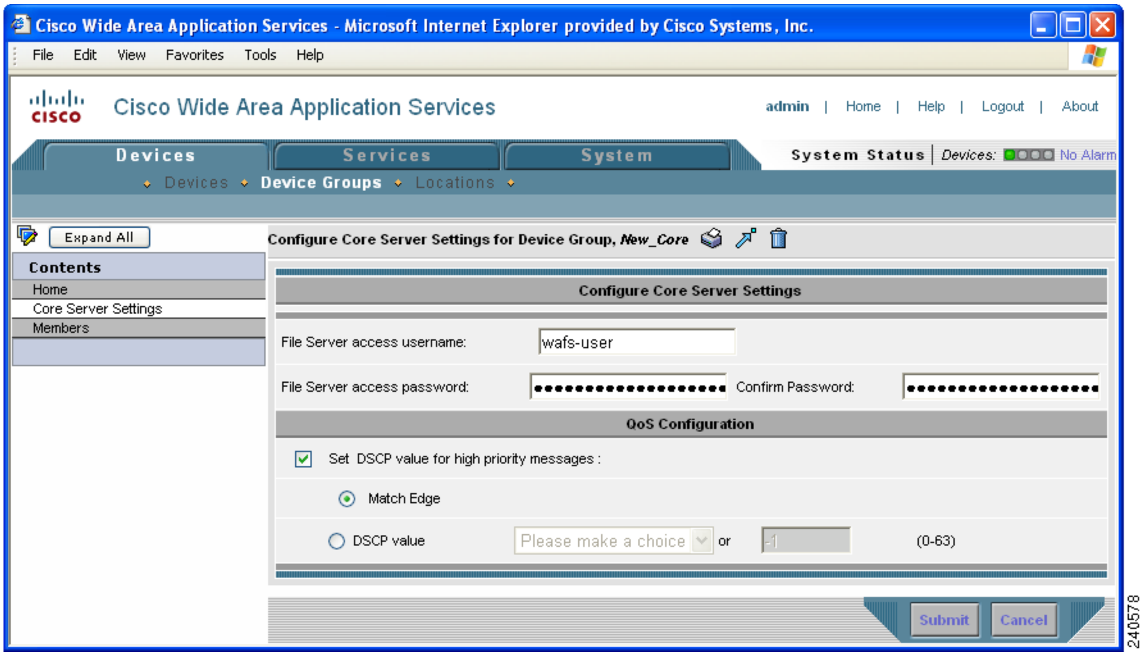
If you are relying on the automatic discovery feature instead of explicitly registering file servers, and you do not need to configure an optional differentiated services code point (DSCP) setting, you can skip to Step 14.

Step 8 From the WAAS Central Manager GUI, choose **Devices > Device Groups**.

Step 9 Click the **Edit** icon next to the new core cluster.

Step 10 From the Contents pane, select **Core Server Settings**. The Configure Core Server Settings window appears. (See Figure 11-3.)

Figure 11-3 Configuring a Core Cluster Example


Cisco Wide Area Application Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
Devices
Services
System
System Status | Devices: No Alarm
Devices
Device Groups
Locations
Expand All
Contents
Home
Core Server Settings
Members
Submit
Cancel
240578

Configure Core Server Settings for Device Group, *New_Core*

Configure Core Server Settings

File Server access username: wafs-user

File Server access password: ••••••••••••••••••••• Confirm Password: •••••••••••••••••••••

QoS Configuration

☑ Set DSCP value for high priority messages :

● Match Edge

○ DSCP value Please make a choice or -1 (0-63)

Step 11 In the **File Server access username**, **File Server access password**, and **Confirm password** fields, enter the access information that will be used for all of the CIFS file servers that are configured as part of this Core cluster. If you are relying on the automatic discovery feature instead of explicitly registering file servers, these fields are unnecessary.

You will specify which file servers this core cluster will export in the "Setting Up File Servers to Export to the Edge WAE Cache" section on page 11-15.

Step 12 Optionally configure a differentiated services code point (DSCP) value for high-priority messages, by following these steps:

a. Place a check in the **Set DSCP value for high priority messages** check box.

b. Select one of the following options:

- **Match Edge**—Matches the DSCP value of the Edge WAEs connected to this core cluster. This matching takes place when you create a connection between edge and core devices, as described in the "Creating a Connection Between a Core Cluster and Edge WAEs" section on page 11-21.
- **DSCP Value**—Allows you to specify a DSCP value for this core cluster.

  Select a value from the drop-down list and refer to Table 11-3 on page 11-14 for a description of the supported values. If you choose **Please Make a Choice** from the drop-down list, enter a value from 0 to 63 in the corresponding field.

DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. Levels of service are assigned by marking each packet on the network with a DSCP code (shown in Table 11-3) and appropriating it to the corresponding level of service. DSCP is the combination of IP Precedence and Type of Service (ToS) fields. For more information, see RFC 2474.

We recommend setting a DSCP value for WAFS control traffic to improve system performance. This requires your routers to be configured to enforce the QoS markings accordingly.

Step 13 Click **Submit**.

Step 14 Reload the device by clicking the **Reload WAE** icon in the taskbar, or by completing the following steps:

a. From the WAAS Central Manager GUI, choose **Devices > Devices**.

b. Click the **Edit** icon next the device on which you enabled Core services. The Device Home window is displayed.

c. Click the **Reload WAE** icon in the taskbar. The device is rebooted and Core services are activated on the device.

Configuring the Edge Devices

After you create and configure the core cluster, the next step is to configure the edge devices that will contain the exported file server data in their cache.

To enable the edge server on a device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Note We recommend enabling file services on an edge device group if WCCP is enabled on your network. If WCCP is disabled, you should enable file services on individual edge devices to prevent name conflicts.

Step 2 Click the **Edit** icon next to the edge device or device group on which you want to enable file services.

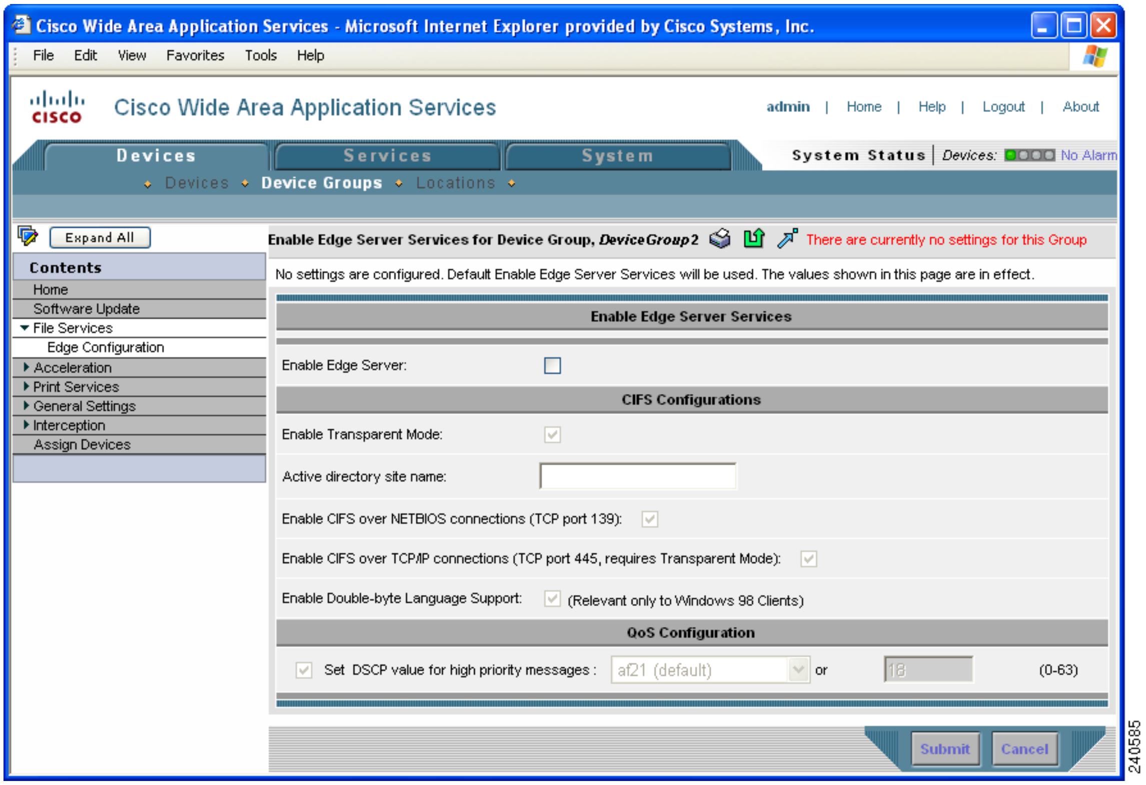
The Device Home window or the Modifying Device Group window appears depending on the selected option.

You cannot enable edge services on the WAAS Central Manager device.

Step 3 From the Contents pane, choose **File Services > Edge Configuration**.

The Enable Edge Server Services window appears. (See Figure 11-4.)

Figure 11-4 Enabling File Services on Edge Devices


Cisco Wide Area Application Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
Devices Services System
System Status | Devices: No Alarm
Devices Device Groups Locations
Expand All
Contents
Home
Software Update
File Services
Edge Configuration
Acceleration
Print Services
General Settings
Interception
Assign Devices
Submit
Cancel
240585

Enable Edge Server Services for Device Group, *DeviceGroup2* There are currently no settings for this Group

No settings are configured. Default Enable Edge Server Services will be used. The values shown in this page are in effect.

Enable Edge Server Services

Enable Edge Server: □

CIFS Configurations

Enable Transparent Mode: ☑

Active directory site name:

Enable CIFS over NETBIOS connections (TCP port 139): ☑

Enable CIFS over TCP/IP connections (TCP port 445, requires Transparent Mode): ☑

Enable Double-byte Language Support: ☑ (Relevant only to Windows 98 Clients)

QoS Configuration

☑ Set DSCP value for high priority messages : af21 (default) or 18 (0-63)

Step 4 Check the **Enable Edge Server** check box.

The other fields in the window are enabled.

Step 5 Check the **Enable Transparent Mode** check box if WCCP or PBR is enabled on your network, or if you are using inline mode.

The options for enabling TCP ports 139 and 445 are automatically updated based on whether transparent mode has been enabled.

If you enable transparent mode, the options for enabling TCP port 139 and port 445 are automatically selected. If you disable transparent mode (Enable Transparent Mode is not checked), the option for enabling TCP port 139 is selected and the option for enabling TCP port 445 is not selected, because port 445 is used only in transparent mode.

Step 6 Enter the name of the active directory site in the provided field.

Step 7 Enable the relevant ports on the Edge WAE by checking the following options (at least one must be checked):

- **Enable CIFS over NETBIOS connections (tcp port 139)**—Check this option if port 139 is open between your clients and the Edge WAEs, as well as between your core cluster and your file servers.

  If port 139 is not open on your network for security reasons, uncheck this option, and then complete the following tasks:

  - Enable WCCP on your routers and Edge WAEs, or enable inline mode on the Edge WAEs. For more information, see Chapter 4, “Configuring Traffic Interception.”
  - Enable port 445 on the Edge WAE by checking the **Enable CIFS Over TCP/IP Connections** check box.

- **Enable CIFS over TCP/IP connections (tcp port 445, requires Transparent Mode)**—Check this option if port 445 is open on your network.

  If port 445 is closed on your network, uncheck this option so that your Edge WAE does not try to establish a connection on this port, and then check the **Enable CIFS over NETBIOS connections** check box.

  When you disable port 445 all clients connect directly to port 139 on the Edge WAE, then the core cluster connects to port 139 on the file server.

  Note If you enable or disable connections on port 139 and port 445, existing clients will not lose their connection to the Edge WAEs.

Step 8 Check the **Enable Double-byte Language Support** check box if you have Windows 98 clients that need to support two-byte languages such as Japanese.

Leave this option unchecked in the following situations:

- You do not have any Windows 98 clients in your environment.
- You have Windows 98 clients in your environment, but they only need to support one-byte languages.

English will always be supported regardless of how this option is configured.

Step 9 Optionally configure a differentiated services code point (DSCP) value for high-priority messages, by following these steps:

a. Place a check in the **Set DSCP value for high priority messages** check box.

b. Select a value in the drop-down list. Refer to Table 11-3 for a description of the supported values.

   If you choose **Please Make a Choice** from the drop-down list, enter a value from 0 to 63 in the corresponding field.

DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. Each packet on the network is marked with a DSCP code (shown in Table 11-3) and is assigned to the corresponding level of service. DSCP is the combination of IP Precedence and Type of Service (ToS) fields. For more information, see RFC 2474.

We recommend setting a DSCP value for WAFS control traffic to improve system performance. This requires your routers to be configured to enforce the QoS markings accordingly.

Table 11-3 DSCP Codes

DSCP Code	Description
af11	Sets packets with AF11 dscp (001010).
af12	Sets packets with AF11 dscp (001100).
af13	Sets packets with AF13 dscp (001110).
af21	Sets packets with AF21 dscp (010010).
af22	Sets packets with AF22 dscp (010100).
af23	Sets packets with AF23 dscp (010110).
af31	Sets packets with AF31 dscp (011010).
af32	Sets packets with AF32 dscp (011100).
af33	Sets packets with AF33 dscp (011110).
af41	Sets packets with AF41 dscp (100010).

Table 11-3 DSCP Codes (continued)

DSCP Code	Description
af42	Sets packets with AF42 dscp (100100).
af43	Sets packets with AF43 dscp (100110).
cs1	Sets packets with CS1 (precedence 1) dscp (001000).
cs2	Sets packets with CS2 (precedence 2) dscp (010000).
cs3	Sets packets with CS3 (precedence 3) dscp (011000).
cs4	Sets packets with CS4 (precedence 4) dscp (100000).
cs5	Sets packets with CS5 (precedence 5) dscp (101000).
cs6	Sets packets with CS6 (precedence 6) dscp (110000).
cs7	Sets packets with CS7 (precedence 7) dscp (111000).
default	Sets packets with default dscp (000000).
ef	Sets packets with EF dscp (101110).

Step 10 Click **Submit**. A pop-up message is displayed that the device must be manually rebooted for the device to function as an Edge server.

Step 11 Click **OK** after reading the pop-up message. Edge Server services are enabled on the device.

If you click **Cancel** on the pop-up message, you are returned to the Edge Configuration window and your changes are not submitted.

Step 12 Reload the device by clicking the **Reload WAE** icon in the taskbar, or by completing the following steps:

a. From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

b. Click the **Edit** icon next the device or device group on which you enabled Edge services.

c. Click the **Reload WAE** or the **Reboot All Devices** icon in the taskbar. The device(s) are rebooted and Edge services are activated on the device(s).

Setting Up File Servers to Export to the Edge WAE Cache

After you enable file services on a core cluster and Edge WAEs, you can optionally use the WAAS Central Manager GUI to set up the file servers that you want to export. If your network has many file servers that you need to define on the WAAS network (10 or more, for example), you can create and import a comma-separated values (CSV) file to speed up the process.

If you do not want to set up file servers, you can rely on the automatic discovery feature to allow WAFS to automatically discover file servers when they are accessed by users. If you are not explicitly registering file servers, you can skip this section.

This section contains the following topics on setting up a file server in the WAAS Central Manager GUI:

- Registering a File Server with the WAAS Central Manager, page 11-16
- Importing File Server Definitions Using a CSV File, page 11-17
- Assigning a Core Cluster to a Registered File Server, page 11-19
- Creating Dynamic Shares for Registered File Servers, page 11-19

Registering a File Server with the WAAS Central Manager

To register a file server with the WAAS Central Manager, follow these steps:

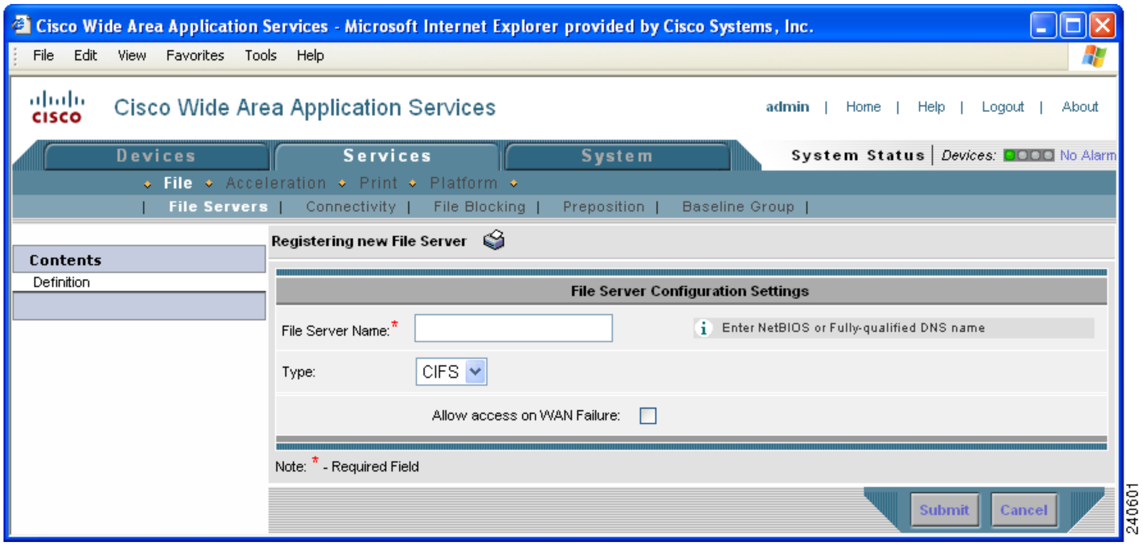
Step 1 From the WAAS Central Manager GUI, choose **Services > File > File Servers**. The File Servers window appears.

From this window, you can perform the following tasks:

- Edit the configuration of an existing file server by clicking the **Edit** icon next to the file server. You can then delete the file server configuration, or modify any of the file server settings.
- Import multiple file server definitions using a CSV file by clicking the **Import from CSV** icon in the task bar. (See the "Importing File Server Definitions Using a CSV File" section on page 11-17.)
- Identify a new file server to export, as described in the next steps.

Step 2 Click the **Create New File Server** icon in the taskbar to identify a new file server to export. The Registering New File Server window appears.

Figure 11-5 Registering New File Server Window


Cisco Wide Area Application Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
cisco
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
Devices
Services
System
System Status | Devices: No Alarm
File Acceleration Print Platform
File Servers | Connectivity | File Blocking | Preposition | Baseline Group |
Registering new File Server
Contents
Definition
File Server Configuration Settings
Submit
Cancel
240601

File Server Name:*
Enter NetBIOS or Fully-qualified DNS name

Type: CIFS

Allow access on WAN Failure: □

Note: * - Required Field

Step 3 In the **File Server Name** field, enter the hostname of the file server to export.

Note If a file server has multiple NetBIOS or DNS names, you must register the file server separately under each one of its names. Otherwise, a client using a NetBIOS name that is not registered will not be able to connect. (Clients using CIFS over TCP port 445 will work fine, however.) You cannot specify the file server's IP address as its name.

Step 4 Check the **Allow Access on WAN Failure** check box to provide CIFS clients with read-only access to the cached data on this Edge WAE in the event of a WAN failure.

When a WAN failure occurs, enabling this option allows CIFS clients to browse the cached directory structure and read fully cached files while authentication and authorization is maintained.

For more information, see the "Preparing Your WAAS Network for WAN Failures" section on page 11-33.

Step 5 Click **Submit**.

The file server is registered with the WAAS system, and the Contents pane refreshes with additional options.

Step 6 Proceed to the "Assigning a Core Cluster to a Registered File Server" section on page 11-19 to assign a core cluster to the registered file server.

Importing File Server Definitions Using a CSV File

If your network includes a high number (10 or more, for example) of file servers that you need to define on the WAAS network, you can create and import a comma-separated values (CSV) file to speed up the process. You can use Excel or another spreadsheet application to create the CSV file.

This section contains the following topics:

- CSV File Creation Requirements, page 11-17
- CSV File Considerations, page 11-17
- Importing the CSV File, page 11-18

CSV File Creation Requirements

Table 11-4 specifies the CSV file requirements.

Table 11-4 CSV File Requirements

Column Heading	Syntax/Semantics	Comments
Name	Specify the name of the file server. Corresponds to the **File Server Name** field in the Registering New File Server window (Figure 11-5).	Required. Same constraints as in Step 3 in Registering a File Server with the WAAS Central Manager.
AllowDisconnected	Corresponds to the Allow access on WAN Failure check box in the Registering New File Server window (Figure 11-5). Set to "true" to apply; set to "false" when not applicable.	Optional. If not specified, assumed to be "false."
Cluster	Specifies the name of an existing core cluster to which the file server is to be assigned.	Optional. If not specified, file server is not assigned to a core cluster. No error is reported if a cluster name is assigned to a file server more than one time.

CSV File Considerations

Keep the following in mind when creating CSV files:

- The first row must list the column headings that you are going to specify.
- At a minimum, the file must contain a "Name" column (other columns are optional).

- Column headings are not case sensitive and can be specified in any order.
- To assign a file server to multiple core clusters, you can specify multiple "Cluster" columns. The column headings row must contain multiple "Cluster" columns if you want to specify multiple clusters in the data rows.
- When you specify a row, it is not necessary to have a value for each column. However, you must specify the correct number of columns. That is, the number of columns must correspond to the number of objects defined in the headings row. The following example presents valid CSV file entries (assuming that core clusters c-1, c-2, and c-5 exist). The adjacent pairs of commas indicate that default values are to be used.

  Example:

  ```
  name,allowdisconnected,cluster,cluster
  s71,TRUE,c-1,
  s72,,c-2,c-5
  ```

Importing the CSV File

After you have created the CSV file, you use the WAAS Central Manager GUI to import the file.

To import the CSV file, follow these steps:

Step 1 From the WAAS Central Manager GUI, click the **Services** tab.

Step 2 In the taskbar, click the **Import from CSV** icon ( ).

The Importing File Server Definitions window appears.

Step 3 Click **Browse**.

The Choose File window opens.

Step 4 Navigate to and select the CSV file that you want to import, then click **Open**. The path and file server name appear in the Path to File Server Definitions field.

Step 5 In the Importing File Server Definitions window, click **Submit**.

The CSV file is imported and a "successfully imported" message is displayed.

The WAAS Central Manager checks the following:

- File headings are correct
- File server name appears on each row
- At least one file server is specified in the file
- All rows have the correct number of columns and each row is syntactically correct

If the file fails any of these checks, an error message appears in the WAAS Central Manager and no file servers are imported. Error messages may provide error explanations for up to 10 rows. However, if the error is related to the headings or the file cannot be read, no further checking occurs.

Assigning a Core Cluster to a Registered File Server

After you register a file server with the WAAS Central Manager, you need to assign at least one core cluster to the file server. The core cluster will be responsible for exporting the file server to the cache on the Edge WAEs. If you are relying on the automatic discovery feature rather than explicitly registering file servers, you do not need to perform this step.

To assign a core cluster to a registered file server, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > File > File Servers**.

The File Servers window appears.

Step 2 Click the **Edit** icon next to the file server that you want to assign to a core cluster.

Step 3 In the Contents pane, choose **Assign Core Clusters**. The Core Cluster Assignments window appears.

The Core Cluster Assignments window displays the device groups configured in your WAAS network. By default, the window displays 10 device groups.

Step 4 Assign a core cluster to the file server by doing either of the following:

- Click ☒ in the taskbar to assign all available core clusters to the file server.
- Click ✖ next to each core cluster that you want to assign to the file server. The icon changes to ☒ when selected.

> **Note** You can only assign core clusters to file servers. You cannot assign regular device groups (identified by ✖) to file servers.

Step 5 Click the **Resolve File Server Name** icon (🔍) for the WAFS Core Cluster you selected. This icon is located next to the Type column and verifies that the name you entered for the file server can be resolved to an IP address.

This icon is only available for WAFS Core Clusters. If the file server name does not resolve, an error message appears in the Comments column. If this occurs, make sure you entered the correct name for the file server.

Step 6 Click **Submit**.

The icon next to the Core Clusters you selected changes to ✓.

Step 7 (Optional) If the file server you just added contains a dynamic share, see the "Creating Dynamic Shares for Registered File Servers" section on page 11-19.

When a file server contains a dynamic share, you must specify the dynamic share in the WAAS Central Manager GUI.

Creating Dynamic Shares for Registered File Servers

Many file servers use dynamic shares, which allow multiple users to access the same share but then be automatically mapped to a different directory based on the user's credentials. Dynamic shares are most commonly used on file servers to set up user home directories.

For example, a directory named Home can be set up as a dynamic share on a file server so each user accessing that share is automatically redirected to their own personal directory.

If a registered file server contains a dynamic share, you must register that dynamic share with the WAAS Central Manager as described in this section.

Before adding a dynamic share, note the following limitations:

- Each dynamic share on a file server must be unique.
- You cannot add a dynamic share if that share has a preposition directive. You must remove the preposition policy before you can add the dynamic share.
- You can add two different dynamic shares with the same file server name and the same share name, but each one needs to be associated with a different core cluster. Each share will have a different ID.
- You can use the WAAS Central Manager GUI to define any directory as a dynamic share. However, if a directory is not set up as a dynamic share on the file server, all users will read or write the same content from the same directory and will not be redirected to different directories based on their credentials.
- You can add dynamic shares only for explicitly registered file servers. Dynamic shares are not supported on automatically discovered file servers.

To add a dynamic share, follow these steps:

Step 1 Before adding a dynamic share, verify the following:

- The dynamic share is already set up on the CIFS file server.
- You have set up the file server in the WAAS Central Manager GUI. For more information on identifying a file server, see the "Setting Up File Servers to Export to the Edge WAE Cache" section on page 11-15.

Step 2 From the WAAS Central Manager GUI, choose **Services > File > File Servers**.

A list of exported file servers appears.

Step 3 Click the **Edit** icon next to the CIFS file server that contains the dynamic share. The Modifying File Server window appears.

Step 4 From the Contents pane, choose **Dynamic Shares**.

The Dynamic Shares window shows all the dynamic shares defined for the selected file server. From this window you can perform the following tasks:

- Edit the configuration of an existing dynamic share by clicking the **Edit** icon next to the share. You can delete the dynamic share, or modify any of the dynamic share settings.
- Add a new dynamic share definition, as described in the next steps.

Step 5 Click the **Create New Dynamic Share** icon in the taskbar to add a new dynamic share. The Dynamic Share Configuration Settings window appears.

Step 6 Enter a name for the dynamic share. This name appears to users when they access the share on the Edge WAE cache.

The following characters are not supported in the dynamic share name: / \ : * ? " < > |

Step 7 In the **Share Name** field, specify the location of the dynamic share by doing one of the following tasks:

- Enter the name of the dynamic share on the file server. The following characters cannot be used in the share name: \ / : * ? " < > |
- Click **Browse** next to the **Share Name** field to navigate to the correct root directory.

Note For the **Browse** button to appear, the file server must be assigned to a Core Cluster and the cluster must contain at least one Core WAE. If these two conditions are not met, the **Browse** button is not displayed.

Step 8 Make sure the status of the share is set to enabled. If you change the status to disabled, the share will not be set up as a dynamic share in your WAAS environment.

Step 9 Click **Submit**.

The specified directory now functions as a dynamic share on the Edge WAE cache.

Creating a Connection Between a Core Cluster and Edge WAEs

After you have registered a file server with the WAAS system, you need to create a connection between a core cluster and your Edge WAEs. This connection enables the core cluster to copy files to the cache on your Edge WAEs.

Before you define a connection that includes multiple core clusters and Edge WAEs, it is important to confirm that each core cluster-to-Edge WAE link has the same connection parameters, such as allocated bandwidth and roundtrip delay, as well as identical aliasing. If this is not the case, you must define a separate connection for each link.

To create a connection between a core cluster and one or more Edge WAEs, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > File > Connectivity**.

The Connectivity window appears.

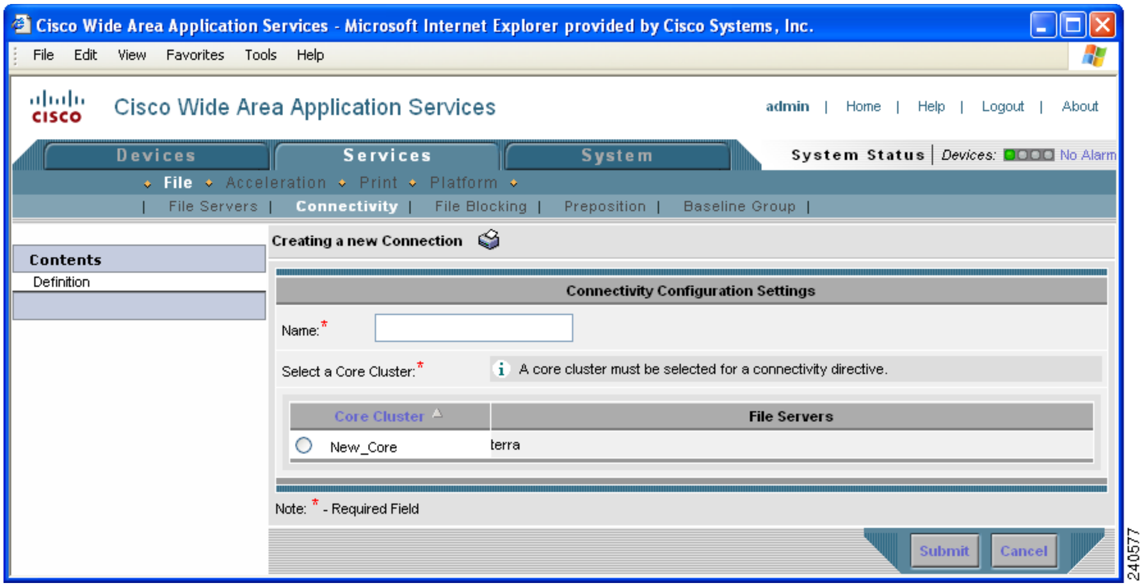
From this window you can perform the following tasks:

- Edit the configuration of an existing connection by clicking the **Edit** icon next to the connection. You can delete the connection, or modify any of the connection settings.
- Add a new connection, as described in the next steps.

Step 2 Click the **Create New Connection** icon in the taskbar to add a new connection.

The Creating a New Connection window appears. (See Figure 11-6.)

Figure 11-6 Creating a New Connectivity Directive Window



Cisco Wide Area Application Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
CISCO
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
Devices
Services
System
System Status | Devices: No Alarm
File Acceleration Print Platform
File Servers | Connectivity | File Blocking | Preposition | Baseline Group |
Contents
Definition
Submit
Cancel
240577

Creating a new Connection

Connectivity Configuration Settings

Name:*

Select a Core Cluster:* A core cluster must be selected for a connectivity directive.

	Core Cluster	File Servers
○	New_Core	terra

Note: * - Required Field

Step 3 Enter a name for the connection.

Step 4 Choose the radio button next to the core cluster that you want included in this connection.

Step 5 Click **Submit**.

A message appears explaining that if you do not want to export any file servers for this connection, you need to uncheck each file server on the File Server Settings window before you assign an Edge device or group to this connection.

Step 6 Click **OK** after reading the message.

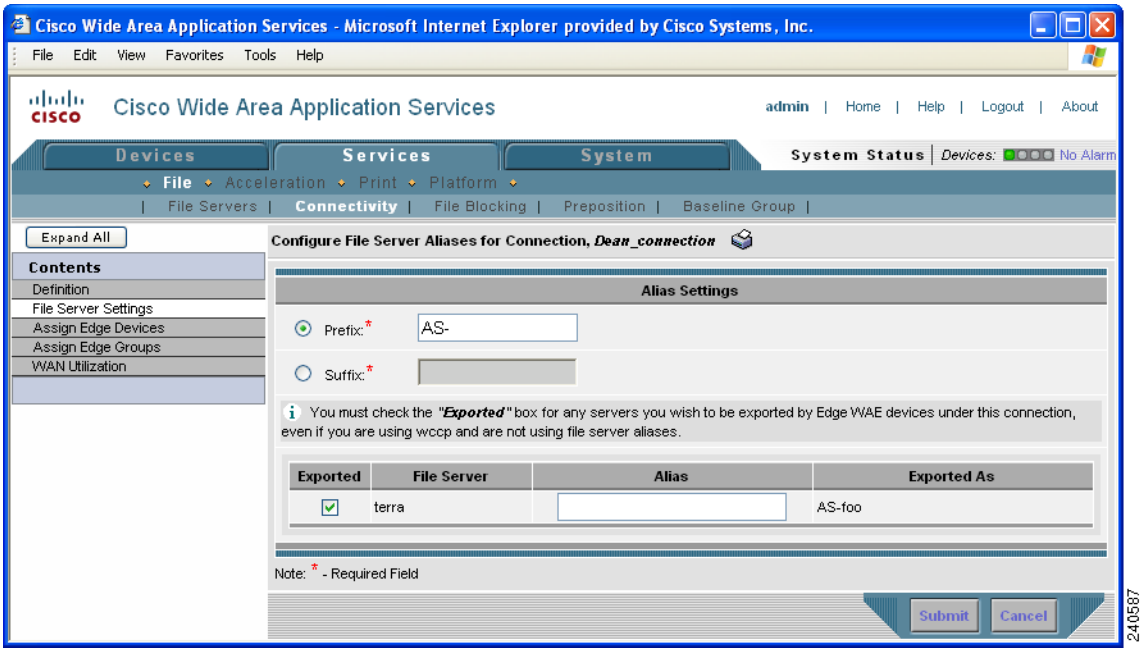
The Contents pane refreshes with additional options.

If you are relying on the automatic discovery feature instead of explicitly registering file servers, you do not need to configure file server settings and you can skip to Step 12.

Step 7 From the Contents pane, select **File Server Settings**.

The Configure File Server Aliases window appears. (See Figure 11-7.)

Figure 11-7 Configuring File Server Aliases


Cisco Wide Area Application Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
cisco
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
Devices
Services
System
System Status | Devices: No Alarm
File
Acceleration
Print
Platform
File Servers | Connectivity | File Blocking | Preposition | Baseline Group |
Expand All
Contents
Definition
File Server Settings
Assign Edge Devices
Assign Edge Groups
WAN Utilization
Submit
Cancel
240587

Configure File Server Aliases for Connection, ***Dean_connection***

Alias Settings

● Prefix:* AS-

○ Suffix:*

You must check the "***Exported***" box for any servers you wish to be exported by Edge WAE devices under this connection, even if you are using wccp and are not using file server aliases.

Exported	File Server	Alias	Exported As
☑	terra		AS-foo

Note: * - Required Field

This window allows you to define the naming scheme for each file server. You can use the original file server name, the file server name plus a prefix or suffix, or an alias of your own design. For example, if you specify **as-** as a prefix and the name of the file server is **win3srv**, users will see this file server as **as-win3srv**.

This window also allows you to select the file servers that you want the core cluster to export.

Step 8 Specify a prefix or suffix value by selecting one of the following options:

- **Prefix**—Adds the prefix you enter to the beginning of the exported file server alias.
- **Suffix**—Adds the suffix you enter to the end of the exported file server alias.

The default behavior is for WAAS to add the prefix AS- to the beginning of the file server alias. You cannot enter a blank prefix or suffix value. If you specify an alias, as described in Step 10, it overrides the prefix and suffix setting.

Step 9 Check the check box next to each file server that you want to export in this connection (at least one must be selected). By default, all file servers are selected.

Note If no file servers appear in this window, then you have not assigned this core cluster to a file server as described in the "Assigning a Core Cluster to a Registered File Server" section on page 11-19. You must complete the procedures in that section before proceeding.

Step 10 (Optional) Enter an alias for the selected file servers in the Alias column.

An alias, which can be any name (maximum of 15 characters), overrides the default prefix and suffix setting defined in Step 8.

Step 11 Click **Submit**.

The Exported As column displays the name of each exported file server as it will appear to your end users.

Step 12 Click one of the following options in the Contents pane:

- **Assign Edge Devices** to assign individual edge devices to this connection.
- **Assign Edge Groups** to assign an edge device group to this connection.

The Edge Device Assignments window or the Edge Group Assignments window appears depending on the selected option.

Step 13 Select the edge devices to include in this connection by doing either of the following:

- Click ➡ in the taskbar to assign all available edge devices or groups to this connection.
- Click ✖ next to each edge device or device group that you want to assign to this connection. The icon changes to ➡ when selected.

Note You can only assign edge devices or device groups with edge services enabled on them. You cannot assign regular core clusters or offline devices (identified by ✖) to the connection. For information on enabling edge services, see the "Configuring the Edge Devices" section on page 11-12.

Step 14 Click **Submit**.

The icon next to each edge device or device group you selected changes to ✓ .

Step 15 (Optional) To configure WAN utilization settings for this connection, complete the following tasks:

a. Choose **WAN Utilization** from the Contents pane. The WAN Utilization window appears.

b. Define the following WAN utilization settings that control the bandwidth that is used for WAFS traffic between the Edge and Core WAEs:

   - **Maximum allocated bandwidth**—Enter the maximum bandwidth allocated to the connection (in Kilobits per second). This value must be less than or equal to the maximum bandwidth of the physical WAN link between the WAEs in this connection. This setting has a default value of 1544 KB per second. WAFS throttles its bandwidth usage to 1.5 times the value of this setting.
   - **Minimum roundtrip delay**—Enter the length of time (in milliseconds) it takes a bit to travel roundtrip from one WAE to the other end and back when the link is idle. This setting has a default value of 80 msec.

Note If you later change any of the WAN utilization settings for this connection, you need to restart the Edge WAE for the new values to take effect.

Step 16 Click **Submit**.

Creating a File-Blocking Directive

The file-blocking option allows you to define one or more file-blocking directives that prevent users from opening, creating, or copying files that match a defined file pattern. These directives, which apply to all Edge WAEs enabled with file services, prevent bandwidth as well as file server and cache space from being wasted on files that system administrators decide to block.

For example, if you create a file-blocking directive for MP3 files, all users connected to the Cisco WAAS network will be unable to create, open, or copy MP3 files from the Edge WAE cache. The only action permitted to users is to delete these files.

You can add file-blocking directives only for explicitly registered file servers. File blocking is not supported on automatically discovered file servers.

Note Blocked files can only be accessed through direct access to the original file server.

To create a file-blocking directive, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > File > File Blocking**. The File Blocking Directives window appears.

The File Blocking window displays the following information about each file-blocking directive:

- **Name**—The name of the file-blocking directive.
- **Status**—Whether the file-blocking directive is enabled or disabled.
- **Pattern Operation**—The clarifying operation for the specified pattern.
- **Pattern**—The file pattern blocked by the policy.

From this window you can perform the following tasks:

- Edit the configuration of an existing blocking definition by clicking the **Edit** icon next to the definition. You can then delete the file-blocking directive, or modify any of the definition settings.
- Create a new file-blocking directive, as described in the next steps.

Step 2 Click the **Create New File Blocking Directive** icon in the taskbar to create a new file-blocking directive. The Creating a New File Blocking Directive window appears.

Step 3 Enter a name for the directive.

Step 4 Select one of the following matching patterns from the **File Name** drop-down list:

- equals
- starts with
- ends with
- contains

Step 5 Complete the file pattern definition in the field to the right of the drop-down list. For example, if **ends with** is selected from the drop-down list, and **.MP3** is entered in the field to the right, all files on exported file servers ending with .MP3 will be blocked from users.

Step 6 Select the status of the policy (**enabled** or **disabled**) from the **Status** drop-down list. Disabled policies are not executed.

Step 7 Click **Submit**.

All edge devices are updated with the new directive, and the blocking definition is added to the table on the File Blocking Directives window.

Step 8 Repeat the previous steps to create other file-blocking directives.

Creating a 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 WAEs. Prepositioning enables you to take advantage of idle time on the WAN to transfer frequently accessed files to selected WAEs, where users can benefit from cache-level performance even during first-time access of these files.

You can add preposition directives only for explicitly registered file servers. Prepositioning is not supported on automatically discovered file servers.

When defining a preposition directive, you select the Edge WAEs that you want to be prepositioned with content from the file server, then specify the root directories on the file server to be prepositioned. Initially, the preposition directive is in the unscheduled state. You must create a schedule that determines when and how often the content is prepositioned. Because content can be prepositioned on a regular basis, you can specify whether each new iteration of the task should copy all designated files, or only those files that have changed over a specified time interval.

In addition, you can specify time and size limits to prevent a preposition task from consuming too much bandwidth on the WAN or too much space on the Edge WAE cache. We strongly recommend that you use these limits to optimize network efficiency and prevent misuse of this feature.

When the activation time of a preposition directive arrives, a preposition task starts on the Edge WAE. Each preposition task can be monitored in the WAAS Central Manager GUI during and after processing. You can also terminate active preposition tasks if required.

If you are running mixed versions of WAAS and either the Edge or the Core device is running a version prior to 4.0.13, the preposition task will always use the preposition settings from the Core device.

Prepositioning requires that the username and password needed to access the file server be specified in the Configure Core Server Settings window. For details, see Step 11 in the "Configuring the Core Cluster" section on page 11-9.

Prepositioning includes the ability to configure multiple roots. See the "Creating a New Preposition Directive" section on page 11-27.

Note A warning message appears if the required connections do not exist for defining preposition directives.

The following topics describe how to create a preposition directive:

- Creating a New Preposition Directive, page 11-27
- Assigning Edge Devices to a Preposition Directive, page 11-31
- Creating a New Preposition Schedule, page 11-31

Creating a New Preposition Directive

To create a preposition directive, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > File > Preposition**.

The Preposition Directives window appears. This window displays the following information about preposition directives that exist on the system:

- **Preposition Directive**—The name of the preposition directive.
- **Type**—Whether the preposition directive affects all files (Full) or just those that have changed since the last preposition task (Differential).

  When the type is Full, all the files that match the other filters of the task and that are found on the file server are sent to the Edge to be compared with the cache.

  When the type is Differential, only the files that are found as changed since the last successful preposition are sent to the Edge cache. The time of the last successful preposition is taken from the Edge device, so make sure that the clock is synchronized with the file server. The first scan is always a full scan. If you change the preposition task, the last successful scan time is reset.
- **Status**—Whether the preposition directive is enabled or disabled.
- **File Server**—The name of the exported file server.

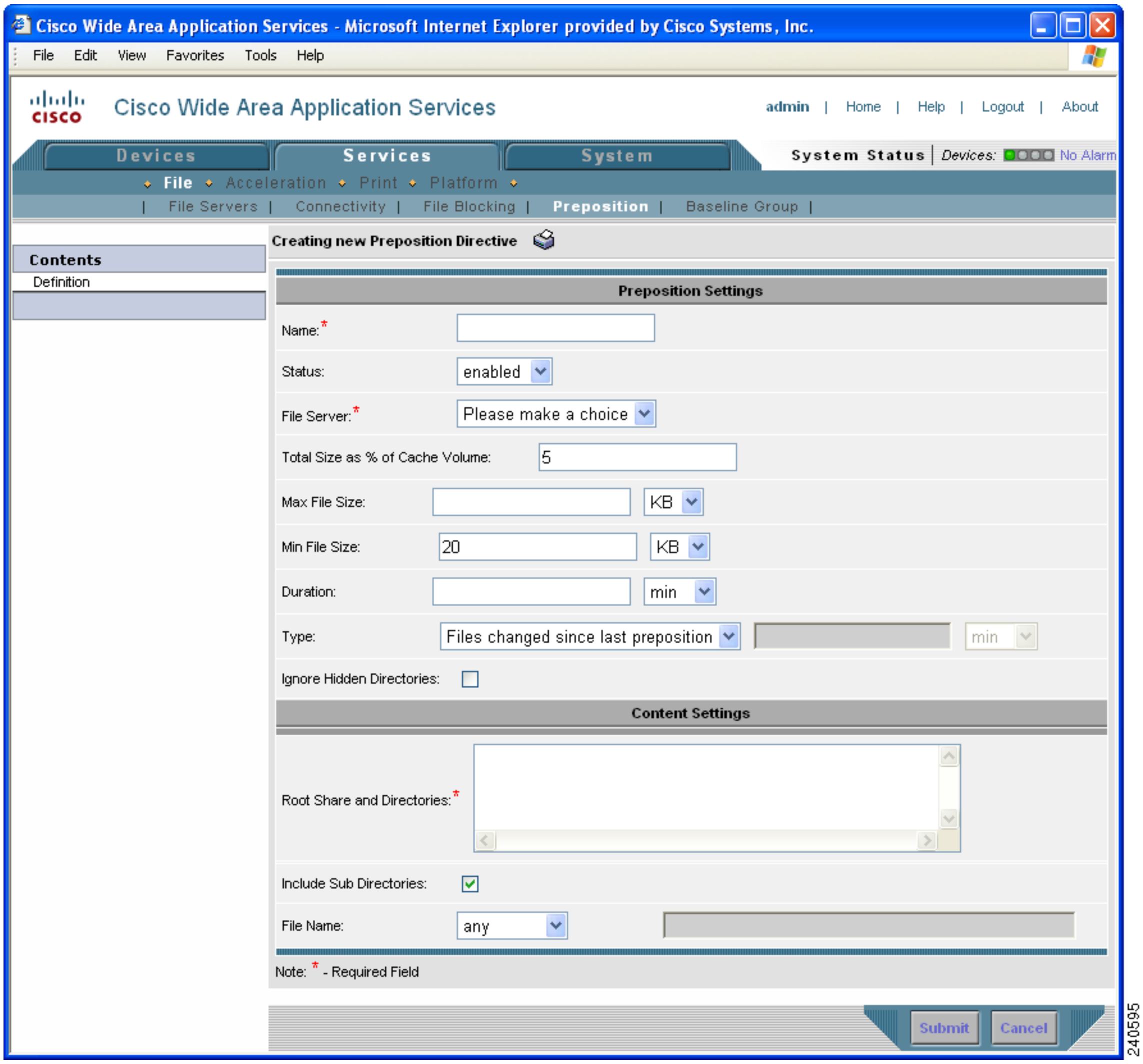
From the Preposition Directive window you can perform the following tasks:

- Edit the configuration of an existing preposition directive by clicking the **Edit** icon next to the directive. You can then delete the preposition directive, or modify any of the settings.
- Add a new preposition directive, as described in the following steps.

Step 2 Click the **Create New Preposition Directive** icon in the taskbar to create a new preposition directive.

The Creating New Preposition Directive window appears. (See Figure 11-8.)

Figure 11-8 Creating a New Preposition Directive



Cisco Wide Area Application Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
CISCO
Cisco Wide Area Application Services
admin | Home | Help | Logout | About
Devices
Services
System
System Status | Devices: No Alarm
File Acceleration Print Platform
| File Servers | Connectivity | File Blocking | Preposition | Baseline Group |
Contents
Definition
Submit
Cancel
240595

Creating new Preposition Directive

Preposition Settings

Name:*	
Status:	enabled
File Server:*	Please make a choice
Total Size as % of Cache Volume:	5
Max File Size:	KB
Min File Size:	20 KB
Duration:	min
Type:	Files changed since last preposition min
Ignore Hidden Directories:	□

Content Settings

Root Share and Directories:*	
Include Sub Directories:	☑
File Name:	any

Note: * - Required Field

Step 3 Enter a name for the directive.

Step 4 From the Status drop-down list, choose either **enabled** or **disabled**. Disabled directives are not put into effect.

Step 5 From the File Server drop-down list, choose the file server to export.

Only the registered file servers are displayed in this drop-down list. For information on registering a file server, see the "Registering a File Server with the WAAS Central Manager" section on page 11-16.

Step 6 (Optional) Define time and size limitations using the provided fields.

Table 11-5 describes the time and size limitation fields.

Table 11-5 Preposition Time and Size Limitations

Field	Description
Total Size as % of Cache Volume	Percent of the overall Edge WAE cache that prepositioned files can consume. For example, if you do not want this prepositioning directive to consume more than 30 percent of a WAE's cache, enter 30 in this field. The default value is 5 percent. The percent of cache defined for a preposition task defines the maximum size that can be prepositioned in a single iteration of the task regardless of how much is already in the cache. When the cache is full, regardless of the reason, prepositioning operates like on-demand caching: an eviction process begins and the files with the oldest time-last-accessed values are removed from the cache.
Max File Size	Maximum file size that can be exported. Files that are larger than this value are not exported to the WAE cache.
Min File Size	Minimum file size that can be exported. Files that are smaller than this value are not exported to the WAE cache. As a general rule, it is inefficient to preposition files smaller than 20 KB because these files can be retrieved quickly over the WAN through normal WAAS. The default value is 20 KB.
Duration	Maximum amount of time it should take WAAS to export the file server. If it takes WAAS longer than this amount of time to export the file server, WAAS stops the exporting process before all files are copied to the Edge WAE cache. If the preposition task does not start at the scheduled start time (for example, because the Edge and the Core have no connection), the start retries are counted in the duration. If you do not specify a value for this field, WAAS takes as much time as needed to export this file server.
Type	Time filter on the scan process. From the Type drop-down list, choose one of the following options: • **All Files**—Exports all files to the Edge WAE cache. This is the default setting. • **Files changed since last preposition**—Exports only the files that have changed since the last preposition to the Edge WAE cache. This differential filter is applied from the second iteration of a task execution onward. If a new directory is moved to an already prepositioned directory (without changing its last-modified time), this new directory is not prepositioned during the next prepositioning session when you choose this option. • **Files changed since last**—Exports only the files that have changed within the specified time. For example, if you want to push out file updates that have been made on the file server in the last two hours, enter **2** in the provided field and select **hour** from the drop-down list.

Note If one of these limits is exceeded during a prepositioning task, the task is terminated and a message is sent to the Administrator log. Any remaining files are exported the next time the task is run. If a user requests one of the missing files before this happens, it is fetched over the WAN through Cisco WAAS as usual.

Step 7 Check the **Ignore Hidden Directories** check box if you want prevent hidden directories on the file server from being prepositioned. This check box is unchecked by default. If you leave this box unchecked, hidden directories will be prepositioned.

If you are running mixed versions of WAAS and either the Edge or the Core device is running a version prior to 4.0.13, the preposition task will use the preposition settings from the Core device.

If you are relying on the automatic discovery feature instead of explicitly registering file servers, this check box does not apply because prepositioning is not supported for automatically discovered file servers.

Step 8 In the **Root Share and Directories** field, enter the directories on the file server that you want to export. Use any of the following methods to identify a directory:

- Manually enter one or more directory paths in the following format: *protocol*://*server*/*share* or *server*\share. For example, cifs://win12srv/home or win12srv\home. You may enter multiple lines for multiple directories, with each full directory path on its own line.

  When you define multiple root shares, the preposition sequence that is performed for a single root configuration is repeated for each root serially.

- Click the **Browse** button to browse the directories on the file server. To navigate into a directory, click the file folder icon to the left of the directory name. Check the check box next to the directory that you want to export and then click the **Select Directory** button. The browse window allows you to choose multiple directories.

  The **Browse** button appears only if you have configured the **File Server access username** and the **File Server access password** fields in the Core Server Settings configuration window. (See Figure 11-3.)

- Check the **Include Sub Directories** check box to include all subdirectories under the specified root directory. If this option is not selected, only the files in the specified root directory are prepositioned and you cannot select subdirectories when you are browsing.

- Narrow the policy definition to a particular type of file by selecting a pattern operator from the **File Name** drop-down list and in the adjacent text box enter free text describing the pattern. For example, enter **ends with .doc**.

Step 9 Click **Submit**.

The directive is saved to the system and additional options appear in the Contents pane.

Assigning Edge Devices to a Preposition Directive

After you create a preposition directive, you need to assign Edge WAEs or device groups to the directive. This task determines which Edge WAEs will store preposition content in their cache.

Note Prepositioning includes the ability to configure multiple roots. See the "Creating a New Preposition Directive" section on page 11-27.

To assign an Edge WAE or device group to a preposition directive, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > File > Preposition**.

The Preposition Directives window appears, which lists the preposition directives that exist on the system.

Step 2 Click the **Edit** icon next to the preposition directive that you want to assign to an Edge WAE or device group.

Step 3 In the Contents pane, click one of the following options:

- **Assign Edge Devices**—Allows you to select one or more Edge WAEs to assign to this directive.
- **Assign Edge Groups**—Allows you to select a device group to assign to this directive.

The Edge Device Assignments window or the Device Groups Assignments window appears, depending on the selected option.

Step 4 Select the Edge WAEs or device groups to assign to this preposition directive by doing either of the following:

- Click ➡ in the taskbar to assign all available Edge WAEs or device groups to this directive.
- Click ✖ next to the individual Edge WAE or device group that you want to assign to this directive. The icon changes to ➡ when selected.

Note If a device or device group is offline (identified by ✖), then you cannot assign that device or group to this directive. The preposition directive, when assigned to a device group, is applied only to connected Edge devices in the assigned device group.

Step 5 Click **Submit**.

The icon next to each edge device or device group you selected changes to ✓.

Creating a New Preposition Schedule

Once you create a preposition directive and assign WAEs to the directive, we recommend you create a schedule that determines when and how often prepositioning occurs.

For example, you may want to schedule prepositioning to occur at night to minimize the amount of traffic during business hours. Or you may want to schedule prepositioning to occur on a recurring basis if the exported data changes often. This will help ensure that the WAEs assigned to this directive have the latest file updates in their cache.

When a preposition task is scheduled to begin at the same time for multiple Edge WAEs that are located in different timezones, the task will begin on the Edge WAEs based on the Core WAE timezone. If the clocks of the Edge WAE and the Core WAE are not synchronized, the task will not start on time.

To create a preposition schedule, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > File > Preposition**.

The Preposition Directives window appears, which lists the preposition directives that exist on the system.

Step 2 Click the **Edit** icon next to the preposition directive for which you want to create a schedule.

Step 3 In the Contents pane, click **Schedule**.

The Creating New Preposition Schedule window appears. By default, no schedule is configured.

Step 4 Choose one of the following scheduling options:

- **Now**—Prepositioning occurs within a few minutes after you submit this schedule.

  A Now schedule begins again each time you make a change to the preposition directive and click the **Submit** button. A Now schedule also begins again as soon as an edge device that has been reloaded comes back online.
- **Daily**—Prepositioning occurs daily at the defined time.
- **Date**—Prepositioning occurs at the defined time and date.
- **Weekly**—Prepositioning occurs on the selected days of the week at the defined time.
- **Monthly Days**—Prepositioning occurs on the selected days of the month at the defined time.
- **Monthly Weekdays**—Prepositioning occurs on the defined day (as opposed to a defined date) and time during the month. For example, you can schedule prepositioning to occur on the second Tuesday of every month.

Step 5 Specify a start time for the prepositioning task.

The time is expressed in 24-hour format with 00:00 representing midnight.

Note You cannot schedule a start time for the **Now** option.

Step 6 Click **Submit**.

The message Changes Submitted appears at the bottom of the window confirming that your schedule was saved.

Step 7 Verify that the preposition directive completed successfully by checking the preposition status. For more information, see the "Checking Preposition Status" section on page 11-33.

Managing File Services

The following topics in this section describe how to manage file servers:

- Checking Preposition Status, page 11-33
- Starting and Stopping Preposition Tasks, page 11-33

- Preparing Your WAAS Network for WAN Failures, page 11-33
- Viewing Members of a Core Cluster, page 11-35

Checking Preposition Status

After you create one or more preposition directives, you can check the status of all the preposition tasks to make sure they completed successfully. If a task does not complete successfully, then some of the prepositioned files may have not been successfully copied to the Edge WAE cache.

To check the status of a prepositioning task, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Services > File > Preposition**.

The Preposition Directives window appears, which lists the preposition directives that exist on the system.

Step 2 Click the **Edit** icon next to the preposition directive for which you want to check.

Step 3 In the Contents pane, click **Preposition Status**. The Preposition Status window appears.

This page displays the following information:

- **WAE**—The name of each Edge WAE that received the prepositioned files in its cache.
- **Start Time**—The time the preposition task started.
- **Duration**—The amount of time in took the preposition task to complete.
- **Amount Copied**—The amount of data copied to the WAE cache (in bytes).
- **Status**—Whether the preposition task completed successfully.
- **Reason**—The reason a preposition task failed.

Step 4 Make sure the Status column shows Completed.

If this column shows a failure, look in the Reason column for an explanation that can help you troubleshoot why the preposition task failed. After resolving the issue, you can schedule the preposition task to run again now, or wait until the scheduled start time and check the status again later.

Starting and Stopping Preposition Tasks

You can start or stop a preposition task from the Device Manager GUI. For more information, see Chapter 10, "Using the WAE Device Manager GUI."

Preparing Your WAAS Network for WAN Failures

When you set up a connectivity directive that links an Edge WAE to a core cluster, you have the option to configure the Edge WAE to operate in disconnected mode in the event a WAN failure breaks its link to the core cluster.

This section contains the following topics:

- About Disconnected Mode, page 11-34
- DNS and Domain Controller Requirements, page 11-34

- Data Availability in Disconnected Mode, page 11-35
- Configuring Disconnected Mode, page 11-35

About Disconnected Mode

Disconnected mode allows CIFS clients to continue to browse the cache directory and read fully cached files on an Edge WAE when a WAN failure occurs. Because the Edge WAE cannot verify its cached data against the file server during a WAN failure, CIFS clients are provided with read-only access to the cached data.

When the WAN connection between the Edge WAE and core cluster is restored, the Edge WAE automatically switches back to regular connected mode.

An Edge WAE switches to disconnected mode when the Edge WAE loses its connection to the core cluster. This is known as a WAN failure.

Note A file server crash does not trigger a switch to disconnected mode (assuming the Edge WAE maintains its connection to the core cluster).

An Edge WAE can operate in disconnected mode for one connection and in regular connected mode for another connection. For example, if you create two connectivity directives for an Edge WAE where one directive links it to core cluster A and the other directive links it to core cluster B and a WAN failure breaks its link to core cluster A, then the Edge WAE switches to disconnected mode for that connection. The Edge WAE will remain in regular connected mode when interacting with core cluster B.

Disconnected mode operates only with explicitly registered file servers. Disconnected mode is not supported for automatically discovered file servers.

DNS and Domain Controller Requirements

Disconnected mode requires a local domain controller in the branch office to authenticate CIFS clients. An Edge WAE operating in disconnected mode supports all authentication methods except Kerberos.

In DNS-only environments, a local DNS server at the branch office is also required. If WINS is used instead of DNS, there must be a local WINS server in the branch office.

To enable disconnected mode access to cached files, you must add the Edge WAE to the Active Directory or Windows NT domain (to perform windows authentication in case of WAN failure).

Note By default, Windows domain controllers enforce automatic machine account password changes as part of the authentication process. The machine account password for the Edge WAE is automatically negotiated and changed between the Edge WAE and the domain controller every seven days. However, if the authentication service is down, this process may not occur, and the machine account password for the Edge WAE may expire. To prevent this situation, we recommend that you disable automatic machine account password changes for the Edge WAE. For more information, see the “Disabling the Automatic Machine Account Password Changes for the Edge WAE” section on page 6-23.

Note WINS registrations usually have a three-day timeout. As a result, if WCCP is enabled in disconnected mode there is a chance that the WINS registration of the original file servers will expire and clients will experience name resolution problems.

Data Availability in Disconnected Mode

When an Edge WAE is in disconnected mode, CIFS clients are allowed read-only access to fully cached files on the Edge WAE. CIFS clients are able to view partially cached files and non-cached files in the directory structure, but they are not able to open these files.

Directories are available in disconnected mode only if their ACL is cached. This means that shares that have never been accessed, and therefore are not in the cache, are not displayed.

The best way to ensure a file is available in disconnected mode is to set up a preposition directive that proactively places a copy of the file on the Edge WAE cache. For more information, see the "Creating a New Preposition Directive" section on page 11-27.

Configuring Disconnected Mode

When you register a file server with the WAAS Central Manager, you can configure an Edge WAE to operate in disconnected mode. For more information, see the "Registering a File Server with the WAAS Central Manager" section on page 11-16.

You also must add the Edge WAE to the Active Directory or Windows NT domain. For details, see the "Centrally Configuring Windows Domain Server Settings on a WAAS Device" section on page 6-18. Verify that the WAE was successfully added into the domain by clicking the **Show Authentication Status** button. Even if the authentication status is not OK, as long as the **wbinfo -t** command executed successfully (trust via RPC is successful), the WAE will provide authentication for Read Only disconnected mode.

Viewing Members of a Core Cluster

To view the Core WAEs that are members of a Core Cluster device group, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Device Groups**. The Device Groups window appears.

Step 2 Click the **Edit** icon next to the WAFS Core Cluster device group for which you want to view its members. The Modifying Device Group window appears.

Step 3 From the Contents pane, choose **Members**. A list of the devices that belong to the selected device group appears.