

# ACTASTOR USER'S GUIDE





# ActaStor User's Guide

---



**Cisco Systems, Inc.**

170 West Tasman Drive

San Jose, CA 95134

408.526.4000

Web: [www.cisco.com](http://www.cisco.com)

Information in this document is subject to change without notice.  
Copyright 2004-2005 Cisco Systems, Inc. All rights reserved.

This product or document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be disclosed to any person or firm or reproduced in any form by any means without prior written authorization of Actona Technologies, Inc. and its licensors, if any.

USE OF THIS PRODUCT AND ITS RELATED USER DOCUMENTATION ARE SUBJECT TO THE TERMS AND CONDITIONS OF THE APPLICABLE END-USER LICENSE AGREEMENT (EULA).

Actona and the Actona Logo are trademarks of Actona Technologies, Inc.

All other trademarks are the property of their respective owners.

### **Support Information**

Email: [tac@cisco.com](mailto:tac@cisco.com)

Web: [www.cisco.com](http://www.cisco.com)

Phone: (408) 526-4000 (U.S. and Canada)

# About This Guide

The ActaStor User's Guide is comprised of the following chapters:

- **Chapter 1: Introduction**, provides an overview of the ActaStor system and its architecture, describes the benefits of the system and illustrates how the ActaStor solution is deployed in typical enterprise scenarios.
- **Chapter 2: Getting Started**, provides an in-depth technical overview of the ActaStor, and describes how to plan the ActaStor network and prepare for its installation.
- **Chapter 3: Installation and Deployment**, describes how to install and deploy an ActaStor network.
- **Chapter 4: Gateway Management**, describes how to use the Web-based Gateway Manager application for managing individual gateways.
- **Chapter 5: Central Management**, describes how to use the Web-based Central Manager application to distribute licenses, connect gateways, create coherency, pre-position, file blocking and replication policies, and manage gateway groups and users.
- **Chapter 6: Troubleshooting**, describes various troubleshooting issues that may arise in the system, the symptoms or problems that may occur and the various actions to take in order to resolve them.
- **Appendix A: Sample Installation**, describes a complete, step-by-step installation of a sample ActaStor network.
- **Appendix B: Third-party Licenses**, contains licensing agreements for third-party software components, libraries and modules used by ActaStor.



# Table of Contents

<b>Chapter 1: Introduction .....</b>	<b>1-1</b>
<b>What Is ActaStor? .....</b>	<b>1-2</b>
ActaStor Modules .....	1-3
ActaStor Deployment .....	1-5
ActaStor Features .....	1-6
ActaStor Benefits .....	1-8
<b>Target Audience .....</b>	<b>1-9</b>
<b>Scenarios and Applications .....</b>	<b>1-10</b>
File Server Consolidation .....	1-10
Branch Office Data Protection.....	1-10
Centralized Backup .....	1-11
Global Data Access.....	1-11
Corporate Information Sharing.....	1-12
<b>Chapter 2: Getting Started .....</b>	<b>2-1</b>
<b>Terms and Concepts .....</b>	<b>2-2</b>
File Servers .....	2-2
File System Caching .....	2-2
Pre-positioning .....	2-3
Data Coherency .....	2-3
Concurrency .....	2-3
Authentication .....	2-4
Authorization/Access Control .....	2-4
Replication.....	2-4
Namespace .....	2-4

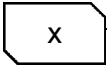
WAN .....	2-5
SNMP .....	2-5
<b>Technical Overview .....</b>	<b>2-6</b>
Data Management Goals .....	2-6
The Challenge .....	2-7
The ActaStor Solution .....	2-8
Integration.....	2-18
<b>Planning an ActaStor Network.....</b>	<b>2-22</b>
ActaStor Capacity Limitations .....	2-24
Calculating the Number of Components .....	2-26
<b>Integrating the ActaStor Network .....</b>	<b>2-27</b>
Pre-Installation.....	2-28
Windows Network Integration.....	2-28
UNIX Network Integration.....	2-31
<b>Chapter 3: Installation and Deployment.....</b>	<b>3-1</b>
<b>Step 1: Unpacking the Hardware .....</b>	<b>3-2</b>
<b>Step 2: Installing the Appliance .....</b>	<b>3-3</b>
<b>Step 3: Using the Setup Wizard .....</b>	<b>3-5</b>
Accessing the Setup Wizard .....	3-6
Defining Local Area Connection Properties .....	3-8
Defining System Properties.....	3-9
Selecting Roles.....	3-11
Defining the EdgeServer Configuration.....	3-12
Defining the CoreServer Configuration .....	3-14
Defining Notification Settings .....	3-20
Registering to the Central Manager .....	3-21
<b>Step 4: Installing the License.....</b>	<b>3-24</b>
<b>Step 5: Starting Components.....</b>	<b>3-24</b>
<b>Step 6: Defining Connectivity.....</b>	<b>3-24</b>



<b>Chapter 4: Gateway Management .....</b>	<b>4-1</b>
<b>Launching the Gateway Manager .....</b>	<b>4-3</b>
<b>Gateway Manager Quick Tour .....</b>	<b>4-4</b>
<b>Gateway Management Workflow .....</b>	<b>4-6</b>
<b>Managing the Gateway .....</b>	<b>4-7</b>
Control Option .....	4-8
Configuration Option .....	4-14
Utilities Option .....	4-24
<b>Managing the CoreServer Component .....</b>	<b>4-27</b>
Configuration Option .....	4-27
<b>Managing the EdgeServer Component .....</b>	<b>4-34</b>
Configuration Option .....	4-34
Policies Option .....	4-39
<b>Managing the Replication Component .....</b>	<b>4-44</b>
Terminating a Replication Task .....	4-48
<b>Monitoring the Gateway .....</b>	<b>4-49</b>
Viewing Monitoring Graphs .....	4-50
Monitoring the Gateway Component .....	4-52
Monitoring the CoreServer Component .....	4-53
Monitoring the EdgeServer Component .....	4-56
<b>Viewing Gateway Logs .....</b>	<b>4-63</b>
<b>Chapter 5: Central Management .....</b>	<b>5-1</b>
<b>Launching the Central Manager .....</b>	<b>5-2</b>
<b>Central Manager Quick Tour .....</b>	<b>5-3</b>
<b>Central Management Workflow .....</b>	<b>5-5</b>
Managing Licenses .....	5-6
Managing Distributions .....	5-7

<b>Managing Tasks</b> .....	<b>5-10</b>
Gateways Option .....	5-11
Defining Connections Between EdgeServers and CoreServers .....	5-17
Defining Coherency Policies .....	5-29
Defining Pre-position Policies.....	5-37
Defining File Blocking Policies .....	5-49
Defining Replication Policies .....	5-54
<b>Managing Groups</b> .....	<b>5-66</b>
Defining EdgeServer Groups .....	5-67
Defining CoreServer Clusters.....	5-74
<b>Managing Users</b> .....	<b>5-82</b>
Adding Users .....	5-83
Editing Users .....	5-85
Deleting Users .....	5-85
<b>Chapter 6: Troubleshooting</b> .....	<b>6-1</b>
<b>Getting Technical Assistance</b> .....	<b>6-2</b>
<b>Installation and Setup Issues</b> .....	<b>6-3</b>
<b>ActaStor Manager Issues</b> .....	<b>6-6</b>
Gateway Manager .....	6-6
Central Manager.....	6-6
<b>Client Operation Issues</b> .....	<b>6-9</b>
<b>Appendix A: Sample Installation</b> .....	<b>A-1</b>
<b>Step 1: Unpacking the Hardware</b> .....	<b>A-4</b>
<b>Step 2: Turning on the Appliance</b> .....	<b>A-4</b>
<b>Step 3: Configuring the Client Installation Console</b> .....	<b>A-5</b>
<b>Step 4: Accessing the Setup Wizard</b> .....	<b>A-6</b>

<b>Step 5: Configuring the CoreServer .....</b>	<b>A-7</b>
Defining Local Area Connection Properties .....	A-7
Selecting Roles .....	A-8
Defining the CoreServer Configuration .....	A-9
Defining Notification Settings .....	A-10
Registering to the Central Manager .....	A-11
<b>Step 6: Configuring the EdgeServer .....</b>	<b>A-13</b>
Defining Local Area Connection Properties .....	A-14
Selecting Roles .....	A-15
Defining the EdgeServer Configuration .....	A-15
Defining Notification Settings .....	A-16
Registering to the Central Manager .....	A-16
<b>Step 7: Configuring the ActaStor Network with the Central Manager .....</b>	<b>A-18</b>
Launching the Central Manager .....	A-18
Distributing Licenses .....	A-19
Starting the Gateway .....	A-21
Creating Connectivity Policies .....	A-21
<b>Step 8: Connecting a Client to the EdgeServer .....</b>	<b>A-23</b>
<b>Appendix B: Third-party Licenses .....</b>	<b>B-1</b>
<b>Index .....</b>	<b>I-1</b>



# List of Figures

Figure 1-1: ActaStor Appliance .....	1-2
Figure 1-2: ActaStor Deployment.....	1-5
Figure 2-1: Centralization Scenario .....	2-21
Figure 2-2: Collaborative Scenario .....	2-22
Figure 2-3: Distributed Organization Layout .....	2-26
Figure 3-1: Appliance Ports .....	3-3
Figure 3-2: Power Socket .....	3-4
Figure 3-3: Gateway Front Panel.....	3-4
Figure 3-4: Login Page .....	3-6
Figure 3-5: Local Area Connection Properties Page .....	3-8
Figure 3-6: System Properties Page.....	3-10
Figure 3-7: Role Selection Page .....	3-11
Figure 3-8: EdgeServer Configuration Page.....	3-13
Figure 3-9: CoreServer Configuration – CIFS Page .....	3-15
Figure 3-10: Adding CIFS File Servers .....	3-16
Figure 3-11: CoreServer Configuration – NFS Page .....	3-18
Figure 3-12: Adding NFS File Servers .....	3-19
Figure 3-13: Notification Setting Page .....	3-20
Figure 3-14: Connection to Central Manager Page .....	3-22
Figure 4-1: Login Page – Gateway Manager .....	4-3

Figure 4-2: Gateway Manager .....	4-4
Figure 4-3: Gateway Control Page .....	4-7
Figure 4-4: Components Tab – Starting Components .....	4-9
Figure 4-5: Components Tab – Stopping Components .....	4-10
Figure 4-6: Gateway Control – Appliance Tab.....	4-11
Figure 4-7: Gateway Control – Registration Tab .....	4-12
Figure 4-8: Gateway Control – Backup Tab .....	4-13
Figure 4-9: Gateway Configuration – Manager Tab .....	4-15
Figure 4-10: Gateway Configuration – SNMP Tab .....	4-16
Figure 4-11: Gateway Configuration – Networking Tab.....	4-17
Figure 4-12: Gateway Configuration – Print Services Tab .....	4-19
Figure 4-13: Notifier Tab.....	4-23
Figure 4-14: Utilities – Support Tab .....	4-25
Figure 4-15: Utilities – Cache Tab .....	4-26
Figure 4-16: CoreServer – NFS Servers Tab .....	4-28
Figure 4-17: New NFS File Server Window.....	4-29
Figure 4-18: CoreServer – CIFS Servers Tab .....	4-31
Figure 4-19: New CIFS File Server Window.....	4-32
Figure 4-20: EdgeServer – General Tab .....	4-36
Figure 4-21: EdgeServer – CoreServers Tab .....	4-37
Figure 4-22: EdgeServer – CIFS Tab .....	4-38
Figure 4-23: EdgeServer – Policies .....	4-40

Figure 4-24: Pre-position Task Details.....	4-41
Figure 4-25: Replication Policies .....	4-45
Figure 4-26: Replication Task Details .....	4-46
Figure 4-27: Replication Task History.....	4-47
Figure 4-28: Sample Graph Window.....	4-50
Figure 4-29: Sample Index Graph Window.....	4-51
Figure 4-30: Gateway Component Monitoring Page.....	4-52
Figure 4-31: CoreServer Monitoring – Connectivity Tab.....	4-54
Figure 4-32: CoreServer Monitoring – Graphs Tab .....	4-55
Figure 4-33: EdgeServer Monitoring – Connectivity Tab .....	4-57
Figure 4-34: EdgeServer Monitoring – CIFS Tab .....	4-58
Figure 4-35: EdgeServer Monitoring – Cache Tab .....	4-59
Figure 4-36: EdgeServer Monitoring – Graphs Tab.....	4-61
Figure 4-37: Gateway Component Logs Page.....	4-65
Figure 5-1: Login Page – Central Manager.....	5-2
Figure 5-2: Central Manager Interface.....	5-3
Figure 5-3: License Installation Window .....	5-6
Figure 5-4: Distribution Tasks Window .....	5-8
Figure 5-5: Distribution Status .....	5-9
Figure 5-6: Gateways Page .....	5-10
Figure 5-7: Table of Registered Gateways .....	5-12
Figure 5-8: Gateway Information Window.....	5-13

Figure 5-9: Gateway Information Page – Advanced .....	5-14
Figure 5-10: Gateway Operations Page .....	5-16
Figure 5-11: Connectivity Page .....	5-18
Figure 5-12: Selecting CoreServers for Connection .....	5-19
Figure 5-13: Selecting EdgeServers for Connection .....	5-21
Figure 5-14: Defining File Server Aliases .....	5-22
Figure 5-15: Defining WAN Utilization Parameters.....	5-24
Figure 5-16: Defining NFS Parameters .....	5-25
Figure 5-17: Coherency Page.....	5-30
Figure 5-18: New Coherency Policy Window – Coherency Tab.....	5-31
Figure 5-19: New Coherency Policy Window – CoreServer Tab.....	5-32
Figure 5-20: New Coherency Policy Window – Content Tab.....	5-33
Figure 5-21: Defining the Root Directory .....	5-34
Figure 5-22: Pre-position Page.....	5-38
Figure 5-23: Pre-position Details Window – General Tab .....	5-39
Figure 5-24: Pre-position Details Window – CoreServer Tab.....	5-41
Figure 5-25: Pre-position Details Window – EdgeServer Tab .....	5-42
Figure 5-26: Pre-position Details Window – Content Tab.....	5-43
Figure 5-27: Pre-position Details Window – Schedule Tab .....	5-44
Figure 5-28: Schedule Tab – Monthly, Weekday Option .....	5-45
Figure 5-29: Pre-position Details Window – Limits Tab.....	5-46
Figure 5-30: File Blocking Page.....	5-50



Figure 5-31: New File Blocking Policy Window.....	5-51
Figure 5-32: New File Blocking Policy Window – Content Tab.....	5-52
Figure 5-33: Replication Page .....	5-56
Figure 5-34: Replication Details Window – General Tab .....	5-57
Figure 5-35: Replication Details Window – Source Tab .....	5-58
Figure 5-36: Replication Details Window – Target Tab .....	5-59
Figure 5-37: Replication Details Window – Schedule Tab.....	5-60
Figure 5-38: Replication Details Window – Options Tab.....	5-61
Figure 5-39: Groups View .....	5-66
Figure 5-40: EdgeServer Groups Page .....	5-67
Figure 5-41: EdgeServer Groups Configuration – Coherency Tab.....	5-69
Figure 5-42: EdgeServer Groups Configuration – CIFS Tab .....	5-70
Figure 5-43: EdgeServer Groups Configuration – Notifier Tab.....	5-71
Figure 5-44: CoreServer Clusters Page.....	5-75
Figure 5-45: CoreServer Cluster Configuration .....	5-76
Figure 5-46: New NFS File Server Window .....	5-78
Figure 5-47: CoreServer Clusters – CIFS Servers Tab .....	5-79
Figure 5-48: New CIFS File Server Window .....	5-80
Figure 5-49: New User Page .....	5-83
Figure 5-50: Defining Gateways to Manage .....	5-84
Figure A-1: Sample Network Setup .....	A-2
Figure A-2: System Back-end Connectors.....	A-5

Figure A-3: Gateway Control Page – Components Tab .....	A-12
Figure A-4: Tasks View.....	A-19
Figure A-5: License Installation Window.....	A-20
Figure A-6: Selecting CoreServers for Connection.....	A-22

# Chapter 1

## Introduction

### ABOUT THIS CHAPTER

This chapter provides an overview of the ActaStor system and its architecture, describes the benefits of the system, and illustrates how the ActaStor solution is deployed in typical enterprise scenarios. It includes the following sections:

- **What Is ActaStor?**, beginning on page 1-2, provides an overview of the ActaStor system and describes some of its main benefits.
- **Target Audience**, beginning on page 1-9, describes the personnel for whom this manual is intended.
- **Scenarios and Applications**, beginning on page 1-10, describes various scenarios in which ActaStor can be used to improve the management of data by today's global enterprises.

# What Is ActaStor?

ActaStor is a plug-and-play file caching solution that significantly improves how a company stores, protects and manages the data accessed at the corporate network edge. ActaStor combines the benefits of centralized storage with local file services, enabling distributed enterprises to consolidate servers and storage, as well as centralize backup and recovery processes, while providing LAN-like performance to remote users.



**Figure 1-1: ActaStor Appliance**

ActaStor achieves this through the use of technologies that overcome the bandwidth and latency barriers common when working over the wide area network (WAN). The results are dramatically increased data protection, reduced storage management costs and improved file access and sharing for today's global enterprise.

The ActaStor solution requires no software to be installed on client machines or file servers. By supporting standard network file access protocols, its operation is completely transparent to the end user and is seamlessly integrated into the existing network and storage infrastructure.

## ActaStor Modules

Every ActaStor appliance (also known as a gateway) comes pre-loaded with the following software modules:

▀ **EdgeServer:** A client-side, file-caching module that serves client requests at remote sites and branch offices (#1 in Figure 1-2, page 1-5). By caching the data most likely to be used at these sites, EdgeServers (#2) greatly reduce the number of requests and the volume of data that must be transferred over the WAN between the data center and the edge.

When requests for data not located in the cache are received, the EdgeServer encapsulates the original CIFS or NFS request using a TCP/IP-based protocol, compresses it and sends it over the WAN to the CoreServer. Data returned from the data center is distributed by the EdgeServer to the end user who requested it.

▀ **CoreServer:** A server-side module that provides access to designated file servers at the data center. CoreServers (#3) are placed between the file servers at the data center (#4) and the WAN connecting the data center to the enterprise's remote sites and branch offices. Requests received from EdgeServers over the WAN are translated by the CoreServer back into its original file server protocol and forwarded to the appropriate file server.

When the data is received from the file server, the CoreServer encapsulates and compresses it before sending it over the WAN back to the EdgeServer that requested it. CoreServers can be arranged in logical clusters to provide scalability and automatic failover capabilities for high-availability environments.

- ▀ **Gateway Manager:** A Web-based management module that enables control and monitoring of the ActaStor gateway. The Gateway Manager enables complete management of individual gateways, such as starting/stopping components, shutting down/rebooting the appliance and manipulating gateway configuration parameters. The Gateway Manager is also used to generate graphs that display various system statistics, run maintenance utilities and view event logs.
- ▀ **Central Manager:** A Web-based management module that enables central management, configuration, monitoring and maintenance of the ActaStor network as a whole. The Central Manager enables network-wide management of gateways, such as viewing information about each gateway as well as performing selected operations on all gateways.

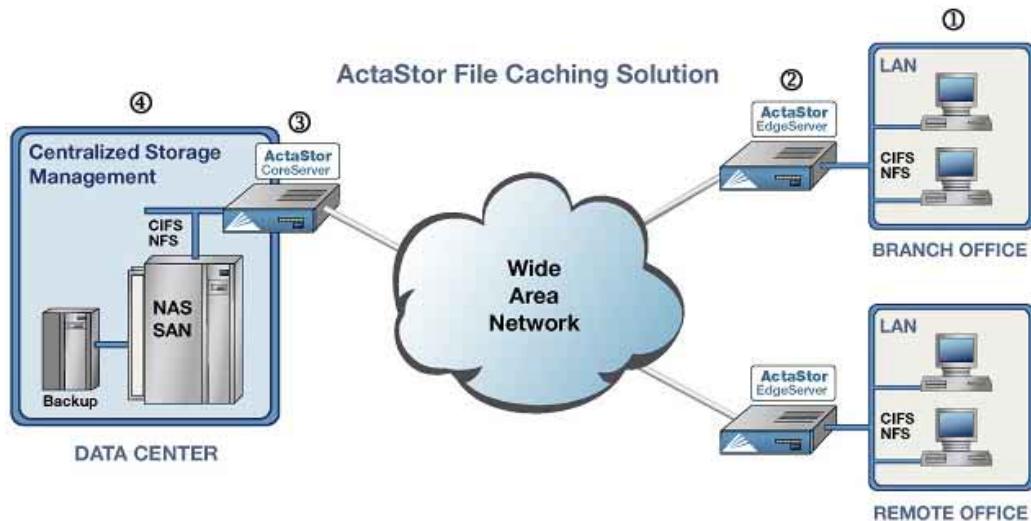
The Central Manager is used to define the connections between EdgeServers and CoreServers, which includes selecting which file servers are exported to each site, as well as the naming system used to represent these servers.

The Central Manager is also used to define the policies that govern the behavior of the ActaStor network. This includes coherency policies that determine the freshness of files stored in the EdgeServer cache, pre-position policies that proactively move selected files to the EdgeServer cache at scheduled times, file blocking policies that prevent users from opening and manipulating certain file types, and replication policies that physically copy data between sites.

In addition, the Central Manager is used to distribute the licenses required by each gateway, to manage groups of EdgeServers and CoreServers, and to manage the users who can access the Gateway Manager and Central Manager.

## ActaStor Deployment

When fully deployed, the ActaStor file-caching solution stands between the data center and each remote office, as shown below.



**Figure 1-2: ActaStor Deployment**

This solution, which consists of multiple, connected ActaStor appliances running one or more software components, comprises the ActaStor network. Sophisticated caching, compression and optimization techniques ensure fast, efficient and protocol-compliant operation over low-bandwidth, high-latency network links.

## ActaStor Features

Key features of the ActaStor system include the following:

- **Read/write caching:** ActaStor's innovative caching technology maintains files locally, close to the clients. Changes made to files are immediately stored in the local EdgeServer and then "streamed" to the central file server. Files stored centrally appear as local files to branch users, improving access performance.
- **Centralized cache pre-positioning:** ActaStor enables files to be "pre-positioned", or pushed, from the data center to each site according to policies that define the schedule, file size and file type. This pre-positioning feature dramatically increases performance for first-time file access, and optimizes bandwidth use over the WAN during off-peak hours.
- **Global coherency and concurrency:** ActaStor enables multi-site access to the most current version of each file, while using a locking mechanism to ensure global consistency for shared file access. System-wide data integrity is maintained.
- **Centralized control and management:** ActaStor's Web-based management tools (Central Manager and Gateway Manager) enable IT administrators to centrally define, monitor and manage policies for each gateway.
- **Policy-based replication:** Files and directories needed at a remote site can be copied to an external directory. The replication process is controlled through management policies, which are easily set using the Central Manager.
- **Print services:** All CIFS-connected ActaStor gateways can be configured to provide a full range of print services to the clients they serve. Printer configuration is performed via the third-party CUPS application. ActaStor supports Point and Print, which provides easy connection to remote printers without the need for installation disks.



- ▶ **CoreServer clustering:** ActaStor uses CoreServer clustering to provide a reliable failover mechanism that maintains high availability and minimizes the probability and duration of CoreServer downtime.
- ▶ **File blocking:** ActaStor can be configured to block files of certain types from being accessed by users, preventing network and storage resources from being consumed inappropriately.
- ▶ **Native protocol support:** ActaStor provides complete end-to-end support for the underlying file system protocols being used by the enterprise (Windows/CIFS and UNIX/NFS). The full file system semantics (such as security, concurrency and coherency) are preserved between each client and file server.
- ▶ **Transparency:** ActaStor is fully transparent to applications, file systems and protocols, enabling seamless integration with existing network infrastructures, including mixed environments. Furthermore, ActaStor has no impact on any security technology currently deployed.
- ▶ **SNMP support:** ActaStor supports SNMP (Simple Network Management Protocol), enabling it to integrate into a common SNMP management system. ActaStor exports parameters based on a private MIB as well as several industry-standard MIBs.
- ▶ **Network monitoring:** ActaStor uses SNMP parameters to collect connectivity data and generate graphs that measure a wide range of gateway metrics. These graphs provide daily, weekly, monthly and yearly perspectives on ActaStor performance.
- ▶ **Easy installation:** ActaStor can be installed in minutes without field IT support, and requires no software to be installed on either client machines or file servers.



**NOTE:**

For more information about ActaStor features, refer to *Chapter 2, Getting Started*.

## ActaStor Benefits

ActaStor provides the following benefits:

- **Simplified storage management:** By migrating storage from remote locations to a central data facility, existing storage systems and IT staff can be more effectively utilized. This means a dramatic reduction in the cost and complexity of storage management for the extended enterprise.
- **Global data access:** Users gain seamless and transparent global access to centralized storage. Files stored centrally appear as local files to branch office users, enabling global file access and eliminating the need to maintain and reconcile multiple file copies throughout the enterprise.
- **Data protection:** By consolidating data, centralized storage management procedures can be readily applied to branch office data. In the event of data loss, backup files in the central data facility can be quickly and easily restored to the branch office.
- **Reduced costs:** Storage hardware costs are significantly reduced through optimal provisioning of existing storage systems across the extended enterprise. In addition, the need and cost associated with local, branch office IT support is greatly reduced by consolidating storage from branch offices into a controlled and manageable data center.
- **Performance:** Organizations using remote access to file servers enjoy improved performance that greatly enhances the user experience.

# Target Audience

The ActaStor solution is intended to be operated by IT administrators, who are responsible for the planning, configuration, integration and maintenance of the system.

This chapter is intended as an introduction for all users wishing to become acquainted with the ActaStor solution. *Chapter 2, Getting Started* and *Chapter 3, Installation and Deployment*, provide in-depth information intended for the IT administrators responsible for system planning and deployment.

*Chapter 4, Gateway Management* and *Chapter 5, Central Management*, are intended for those personnel responsible for ActaStor management and routine maintenance. *Chapter 6, Troubleshooting*, is intended for those needing to deal with specific issues should they arise at any point during installation, deployment or operation.

# Scenarios and Applications

Data is one of the most valuable assets of any enterprise. How a company protects, manages and makes data available to its users often determines the difference between the company's success and failure. This goes beyond the data created and stored in the data center. Just as important is the vast amount of data created in the branch offices.

The ActaStor file-caching solution successfully addresses these challenges by providing measurable benefits for the critical applications of today's global enterprises.

## File Server Consolidation

ActaStor enables enterprises to migrate file servers and storage media facilities from remote sites and branch offices to a controlled and manageable data center. File services can be delivered to these branch offices, meeting the performance requirements that end users demand. By eliminating the need to deploy file servers and storage media at remote sites, enterprises can reduce costs, increase their storage asset utilization and simplify their storage management across the extended enterprise.

## Branch Office Data Protection

ActaStor significantly increases data protection at branch offices. Its file cache appears on the office's local area network (LAN) in the same way as a local file server. End users can map their personal document folders onto the file cache using Windows or UNIX utilities, as they did previously. A cached copy of user data is stored locally in the EdgeServer for fast access. The master copy is stored centrally in the well-protected data center.

In addition, ActaStor's replication utility can copy data that does not reside on the file cache to the data center, thus providing complete data protection for the branch office.

## **Centralized Backup**

By consolidating data across the extended enterprise into a data center, ActaStor makes it easy to apply centralized storage management procedures to branch office data. Backup and restore operations become simpler, faster and more reliable than previously using decentralized solutions.

In the event of data loss, backup files exist in the data center, which can be quickly accessed for recovery purposes. Furthermore, the amount of data loss is greatly reduced, due to the increased frequency of backups performed on the centralized storage in the data center. This makes disaster recovery much more efficient and economical than when working with standalone file servers or NAS appliances coupled with local backup servers and media.

## **Global Data Access**

By overcoming the bandwidth and latency limitations associated with the typical WAN, ActaStor provides users with seamless and transparent global access to centralized storage. Users can access data throughout the distributed enterprise with virtually the same user experience as files stored locally.

Global data access eliminates the need to maintain multiple file copies throughout the enterprise, removing concerns that multiple versions of the file may be in use. Users enjoy fast access to the most recent copy of a file, resulting in great improvements in productivity and data assurance, as well as significant cost savings.

## Corporate Information Sharing

ActaStor is a powerful solution that utilizes global locking capabilities to enable multiple sites to access the same data while maintaining file concurrency and coherency. As a result, multiple users can simultaneously manipulate a file without losing synchronization between versions, enabling them to collaborate on shared files.

By enabling collaboration over the WAN, the ActaStor global file system is well suited for applications such as Product Lifecycle Management (PLM), product development or team collaboration. ActaStor can accelerate product development schedules, improve coordination with global suppliers and enhance inter-office project collaboration.

## Chapter 2

# Getting Started

### ABOUT THIS CHAPTER

This chapter provides the necessary information about ActaStor prior to installing and deploying the solution on your network. This chapter includes the following sections:

- ▶ **Terms and Concepts**, beginning on page 2-2, describes in detail the terms and concepts that are key to understanding ActaStor.
- ▶ **Technical Overview**, beginning on page 2-6, describes the challenges enterprises face in today's networked environment and the ways in which ActaStor overcomes those challenges.
- ▶ **Planning an ActaStor Network**, beginning on page 2-22, provides guidelines for planning an ActaStor network, including which components to use and where to deploy them in the network. It also describes its capacity limitations.
- ▶ **Integrating the ActaStor Network**, beginning on page 2-27, describes the actions to be taken to integrate ActaStor into your network.

# Terms and Concepts

This section describes in detail the terms and concepts that are key to understanding ActaStor.

## File Servers

A file server is a computer responsible for the central storage and management of data files, thereby enabling other computers on the network (known as file system clients) to access the files. File servers and their clients typically communicate via a well-defined network file system protocol, such as CIFS (for Windows) or NFS (for UNIX).

There are two major types of file servers:

- ▲ File servers that run on general-purpose operating systems and hardware, such as Windows 2000 on an Intel platform.
- ▲ NAS (Network Attached Storage) devices, which feature special-purpose operating system and hardware, and are dedicated only to file serving.

### **WARNING:**



When configuring the Core-FE CIFS server, do not use the IP address of the CIFS server.

## File System Caching

A file system cache is a local (or nearby) file store that contains copies of file system objects, such as files, directories and their properties. A cache speeds access to remote files by storing a subset of some larger file set, thus providing a full file-system view without fully replicating the file-system volume. A cache also reduces load on the file server and the interconnecting network.

For more information about caching in ActaStor, refer to page 2-9.



## Pre-positioning

Pre-positioning enables system administrators to proactively "push" frequently used files from the central storage into the cache of selected EdgeServers. This provides users with quicker first-time file access, and makes more efficient use of available bandwidth. Pre-positioning is policy driven via the Central Manager.

For more information about pre-positioning, refer to page 2-10.

## Data Coherency

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" (that is, whether the copy is up to date or not) and the propagation of updates to and from the origin file server.

Coherency algorithms can provide either strong or weak coherency. Strong coherency uses single-copy semantics to force all nodes in the distributed system to see the same file state. Systems using weak coherency do not guarantee real-time updates of all nodes. Instead, they merely promise that all copies of the data file in the system will eventually be synchronized.

For more information about coherency, refer to page 2-11.

## Concurrency

Concurrency control enables multiple clients to synchronize their access to shared data by establishing and removing file system locks. These locks enable a client to restrict access (for example, write lock for exclusive access) to some portion of a file.

For more information about concurrency, refer to page 2-13.

## Authentication

Authentication is the process of establishing and verifying an entity's identity, that is, whether someone or something is, in fact, who or what it is declared to be. The authentication process is typically external to the file system protocol, although the file server must be aware of the client's identity in order to enforce access permissions.

## Authorization/Access Control

Authorization refers to the process of enforcing access policies. These policies determine the type and level of activities, resources or services a user is permitted to access. In the context of file systems, these activities may include reading or writing of files, creating and listing directories, and so on.

## Replication

Replication is the process of creating a replica (a copy) of something. In the context of file systems, replication refers to copying a file system sub-tree, or a subset, from one file server to another. Replication maintains multiple distinct copies, and provides no guarantee of sharing or coherency between consecutive replication cycles.

For more information about replication, refer to page 2-17.

## Namespace

A namespace is a scheme that uniquely identifies a set of names so there is no ambiguity when objects having different origins but the same names are mixed together. For example, DFS (Distributed File System) is a Microsoft technology that enables a global namespace to be created across the entire network.

For more information about namespaces, refer to page 2-20.

## **WAN**

A WAN (wide area network) is a geographically dispersed data communication network. A WAN denotes a broader data communication structure than a LAN (local area network). A WAN is typically characterized by high latency and low bandwidth between the communicating parties.

## **SNMP**

SNMP is the most common protocol for network monitoring and control. With SNMP, network management applications can query agents, which are processes (hardware and software) that report activity in each network device to the management console. The type of information they report is defined in the supported Management Information Database (MIB).

# Technical Overview

The following sections describe the ActaStor system in detail, including the technical issues that need to be addressed to make a file system effective over the WAN, the technologies employed by ActaStor to meet these challenges and the ways in which ActaStor should be integrated with the existing enterprise network.

## Data Management Goals

Enterprises today have remote offices spread across 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, in particular to protect the data in case of 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. Multiply this scenario by tens, hundreds and thousands of remote offices, and it is clear 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 the enterprise's important data to a central location containing the facilities, trained personnel and storage mass required to manage the data properly. Having a data center provide backup and other storage management facilities enables the enterprise to achieve better utilization of both personnel and storage, as well as a higher level of data assurance and security.

## The Challenge

The challenge involved in achieving this optimal solution revolves around what lies between the enterprise's data center and its remote offices, the WAN. As enterprises have learned the hard way, WANs tend 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 such obstacle is posed by the file server protocols that are forced to operate over the WAN. Both CIFS, which is the file server protocol for Windows, and NFS, which is the standard protocol for UNIX, were designed to operate over a LAN. As such, both protocols tend to be "chatty". Every file operation generates several exchanges of protocol messages between the client and the file server. This is usually not noticeable on the LAN, but quickly becomes unbearable over the WAN. Occasionally, the high latency of the WAN breaks the file server protocol altogether.

Another obstacle to implementing the data center solution is the effect on user applications from having to perform file operations over the WAN. Even in cases where the file server protocols are 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, design tools and so on, causing them to stop functioning correctly.

When taken together, all three of these problems, unreliable WANs, file system protocol compatibility and user application compatibility add up to an unfriendly work environment that impacts the user experience and diminishes productivity.

## The ActaStor Solution

The ActaStor solution has been created to overcome the barriers posed by the WAN. The solution is based on several key concepts:

- ▲ **Use the WAN as little as possible:** The more accomplished on the remote side, the better. By minimizing the number of operations that need to traverse the WAN, ActaStor effectively shields users from many of the drawbacks that WANs create.
- ▲ **Use the WAN optimally:** The companion concept to that above is to make the best use of the WAN when it is needed. ActaStor makes use of several technologies, all of which result in the system using the WAN in an optimized fashion.
- ▲ **Preserve file system protocol semantics:** Although ActaStor uses its own proprietary protocol over the WAN, it leaves the complete semantics of all file system protocol commands intact. This is essential in order 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 or forcing them to change their way of doing business. The ActaStor 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. In short, users derive all the benefits of having a secure data center without needing to change any of their work habits.

The ActaStor solution utilizes sophisticated caching, compression and network optimization technologies to overcome the barriers associated with operating standard file system protocols over low-bandwidth, high-latency network links. Additional features, such as replication, have been added to the solution to address other enterprise needs. These technologies and their integration in existing networks are described in detail in the sections that follow.

## File System Caching

File system caching is central to ActaStor operation. The file cache module resides in the EdgeServer, enabling it to address many client requests locally without using the WAN to access the origin file server.

Main features of the cache include:

- ▲ A self-managed storage capacity. When its storage is full, disk space is freed for new files by deleting files that have not been recently used.
- ▲ Meta-data, such as file attributes, is kept in a dedicated database optimized for fast I/O retrieval. This allows fast response times for the frequently accessed meta-data, including operations that involve mostly meta-data, such as browsing.
- ▲ Partial file caching enables file segments to be cached in order to serve read request to clients. Similarly, upon write requests, ActaStor propagates only those segments of the file that have been actually updated, as opposed to sending the entire file to the file server. This enables ActaStor to efficiently support applications that read or write only a small portion of very large files.
- ▲ Asynchronous-write operations improve user-perceived responsiveness, as they propagate data from EdgeServer to CoreServer asynchronously from the client request. ActaStor minimizes the amount of uncommitted cached updates in the file server by continuously streaming updates to the CoreServer and by enforcing a configurable limit on the write buffers.
- ▲ Negative caching enables ActaStor to store information about missing files in the cache to avoid unnecessary roundtrips over the WAN in cases where it is known that the requested file does not exist.

## Pre-positioning

When an end user attempts to open a file not found in the EdgeServer cache, ActaStor fetches it across the WAN from the file server where it is stored. Pre-positioning is a feature that enables administrators to push large, frequently accessed files from file servers to selected EdgeServer caches according to a predefined schedule. Through proper use of pre-positioning, administrators can enable users to benefit from cache-level performance even during first-time access of these files. Pre-positioning improves WAN bandwidth utilization by transferring heavy content when the network is otherwise idle (for example, at night), thus freeing up bandwidth for other applications during the day.

ActaStor enables administrators to create multiple, overlapping pre-position policies, each with its own schedule, list of target EdgeServers and defined time and size constraints.

For more information, refer to *Defining Pre-position Policies* in *Chapter 5, Central Management*.

## Print Services

Having ActaStor gateways installed at branch offices to provide access to remote files servers makes them ideal for providing clients with other services as well, such as print services. Any gateway, regardless of its role, can be configured to provide a full range of print services to the clients connected to it. ActaStor supports Microsoft's Point and Print architecture, which enables Windows users to connect to remote printers by downloading the necessary files and configuration information from the print server, eliminating the need for installation disks.



## Security

ActaStor does not introduce any additional maintenance overhead on already overburdened IT staffs. To that end, ActaStor avoids adding its own proprietary user management layer, making use instead of the users, user credentials and access control lists maintained by the file servers themselves. All security-related protocol commands are delegated directly to the source file servers and the source domain controllers. Any user recognized on the domain and source file server are automatically recognized by ActaStor with the same security level, and all without additional configuration or management.

ActaStor delegates access control and authentication decisions to the origin file server. It also supports cross-domain authentication and authorization for NFS. This enables users defined in one domain to access files that reside in a different domain.

## Data Integrity

In ActaStor, data integrity across the system is ensured by two interrelated features – coherency, which governs the freshness of the data, and concurrency, which controls the access to the data by multiple clients.

### Coherency

Coherency determines the freshness level of files and directories as they are accessed from the EdgeServer cache. The choice of proper coherency policies for WAN file systems is not simple, due to the inherent tradeoff between access performance and the degree of global sharing and coherency. Furthermore, coherency is more challenging in ActaStor, as it allows users who are local to the file server to access the file server directly, that is, without passing through ActaStor.

When a client requests a file or block of data, the EdgeServer component first checks its local cache. If the data is missing or invalid, the most recent data is retrieved from the remote server. The policies and algorithms involved in ensuring the cached data freshness are referred to as coherency.

ActaStor provides three coherency modes:

- **Global:** Standard inter-site coherency intended to support widely used applications invoked by users from multiple sites on shared files. This is the default mode for CIFS.

**NOTE:**



Global mode is not applicable for NFS.

- **Local:** Intra-site coherency that preserves coherency semantics for all users accessing shared data from the same site. This is the default mode for NFS.
- **Strict:** High-level coherency that assures that any access to cached data can be considered equivalent to accessing the remote file server.

Each of these modes can be defined as needed for selected file servers, folders or file types. For more information, refer to *Defining Coherency Policies* in *Chapter 5, Central Management*.

## Common Coherency Semantics

ActaStor applies the following coherency semantics to its coherency policies:

- **Strict CIFS/NFS Behavior for Intra-site:** Regardless of the selected coherency mode, users of the same cache are always guaranteed standard, strict CIFS/NFS coherency semantics.

- ▶ **Validate on CIFS Open:** In CIFS, the File Open operation is passed through to the file server. For coherency purposes, ActaStor validates the freshness of the file on every Open, and invalidates the cached file if a new version exists on the file server.
- ▶ **Flush on CIFS Close:** In CIFS, the File Close operation forces all write buffers to be flushed to the file server, and the Close command returns to the user only after all updates have been propagated to the file server. From a coherency standpoint, the combination of validate on Open and flush on Close ensures that well-behaved applications, such as Microsoft Office, operate in session semantics. This means that the Open-Lock-Edit-Unlock-Close commands are guaranteed to work correctly on the ActaStor network.
- ▶ **Age-based Validation on Directories (CIFS/NFS):** Directories are associated with a pre-configured age. When the age expires, the EdgeServer cache revalidates the directory. The value of the age depends on the required coherency mode. For local or global coherency, this value should be high in order to minimize roundtrip validations (the current default is 15 minutes).
- ▶ **Age-based Validation on NFS files:** Due to the stateless nature of the protocol, NFS validation is age-based only.

## Concurrency

Concurrency control is important in multi-user scenarios where multiple clients access the same data to read, write or both. The ActaStor appliance has native support for NFS (NLM) and CIFS locks/share modes. Each protocol presents different challenges when trying to address the concurrency issues involved with intra-site, inter-site and direct access operations.

Concurrency control in ActaStor defines three levels:

- ▲ **Local:** Ensures correct concurrency control for intra-site users accessing shared data from the same site.
- ▲ **Global:** Standard inter-site concurrency intended to support widely used applications invoked by users from multiple sites, either via ActaStor or directly on shared file servers.
- ▲ **Strict:** High-level concurrency assures that any access to cached data can be considered equivalent to accessing the remote file server.

## WAN Adaptation

A key benefit of the ActaStor solution is the ability to provide remote users with near-LAN access to files located at the data center. A critical part of achieving this goal over the enterprise WAN is the proprietary protocol developed by Actona that optimizes the way traffic is forwarded between the gateways. If communication between gateways is disrupted, the system automatically switches into disconnected mode, preventing operations that could jeopardize the coherency of files in the network.

## Optimizations

ActaStor uses its own proprietary adaptation protocol layer over the WAN between the EdgeServer and CoreServer, while retaining the standard CIFS/NFS protocol at the client and server ends. This proprietary network protocol provides reliable and efficient communication over WANs, especially under high-latency, low-bandwidth conditions.

The ActaStor protocol offers the following benefits:

- ▶ **Reliability:** The ActaStor protocol maintains its own internal message queuing and ordering, enabling it to overcome transient disconnects, network jitters and message loss. The ActaStor transport layer handles temporary network failures by re-establishing the connection and then retransmitting requests that did not receive a response on the disconnected socket.
- ▶ **Efficiency:** For greater WAN traffic efficiency, the ActaStor protocol supports compound requests, grouping multiple, dependant requests and responses into a single message. The processing of individual calls within a compound message is serialized, enabling the output of one command to be used as input for the next.
- ▶ **Link Utilization Optimization:** The ActaStor protocol utilizes a configurable number of concurrent TCP connections for each EdgeServer-to-CoreServer link. Requests and responses may be delivered across any open connection. For example, multiple requests (and responses) for data delivery can be split across multiple connections to increase the effective utilization of the network in cases of high-latency/high-loss WAN connections, where TCP performance degrades.

 **NOTE:**

The administrator sets the actual WAN conditions for each link and the Wide Area File Services (WAFS) fine tunes the desired internal transport parameters and configuration for the number of sockets, buffer sizes, etc. WAFS is WAN-aware and optimizes itself according to the WAN link (bandwidth and latency configured for each link).

- ▶ **Command prioritization:** ActaStor assigns high-priority to requests from active clients, minimizing the WAN latency experienced by users. Batch tasks (replication or pre-position, for example) are assigned a lower priority and are performed in the background.

- ▲ **Conserves Bandwidth:** All ActaStor protocol messages (requests and responses) are compressed. Before compression, the message is encoded, allowing efficient delivery of both textual and binary data. The protocol layer applies the compression automatically, regardless of the message content.
- ▲ **Firewall-friendly:** The ActaStor protocol is layered over TCP/IP, and requires only a single port per CoreServer, making it a firewall-friendly protocol.

## Disconnected Mode

When communication is interrupted between the EdgeServer and the CoreServer or between the CoreServer and the file server, the ActaStor network switches to working in a disconnected state until full communication is restored. If the interruption is brief, the network enters a transient disconnect state, enabling a select number of services and commands for a limited time (typically lasting about one minute), such as read commands for files that are already open.

If the network outage is prolonged, ActaStor switches to a full disconnect state where no services are provided to clients. In this mode, the system denies access to any file (including cached files) until reconnection occurs. From a user viewpoint, the EdgeServer responds as if the network to which it is connected is disconnected.

This approach is required to maintain the security of the data. If a no-service state were not enforced, it would be possible for users connected locally to the file servers to continue working on files, creating conflicts with other users who may have been working on those files remotely when the network interruption occurred.

ActaStor is designed to prevent scenarios that could compromise data coherency and concurrency.

## Replication

ActaStor employs a two-way replication system controlled by policies set in the Central Manager. In one direction, replication enables you to copy files and directories from a local file server to the data center. In the other direction, you can copy files directly from the data center that are accessed locally and not through the EdgeServer cache.

Replication is always performed by two ActaStor gateways working together, as follows:

- ▲ **Replication server:** Provides the files for replicating data.
- ▲ **Replication client:** Receives the files provided by the Replication server.

### NOTE:



All gateways may act as both replication server and replication client, regardless of their role as CoreServer or EdgeServer.

Each instance of replication performed by two gateways is defined as a separate replication task, with its own set of files and activation schedule. Replication tasks are defined from the replication client gateway, which is responsible for activating these tasks according to the defined schedule.

For more information on replication, refer to *Defining Replication Policies* in *Chapter 5, Central Management*.

## Integration

The following sections describe how the ActaStor solution integrates with file servers on one side of the WAN and end users on the other. It also describes the failover mechanism that is used to maintain high availability and minimize possible downtime.

### ActaStor and File Servers

The ActaStor component that interacts with file servers is the CoreServer. It passes the user requests it receives over the WAN from EdgeServers through to the file servers with all semantics intact. The CoreServer appears to file servers as a standard client, using the relevant file system protocol, either CIFS or NFS. It is a completely transparent setup, with no software agents to install on the file servers. This enables CoreServers to be integrated into any file server environment provided by any vendor.

### ActaStor and End Users

Each file server exposed to end users through the ActaStor network appears to those users as a standard file server. In addition, each file server appears in its original context, including its name (in practice, a different name is typically used to avoid possible naming conflicts), share list and access control list. This means that users can access these file servers in exactly the same way they access local file servers.

To make the transition from local file servers to a data center even easier, ActaStor managers can optionally assign an alias to selected file servers. This can be used to assign the names of local file servers to remote file servers at the data center, keeping the user experience completely intact.



## Clustering and Failover

ActaStor provides a high-availability failover (and load balancing) mechanism that minimizes the probability and duration of CoreServer downtime. The CoreServer cluster is a defined group of CoreServers that export the same file servers. EdgeServers can be logically connected to any number of CoreServers within the cluster.

In the event that a CoreServer in the cluster fails, all EdgeServers configured to operate with it are redirected to work with an alternate CoreServer previously selected at random from their connection list, thus maintaining high availability without service interruption.

For NFS, this transition is transparent to clients because of its stateless nature. For CIFS, however, this change may not be transparent to users. This means that client connections are closed, requiring CIFS clients to re-establish their connection. Whether such changes impact currently running applications depends on the nature of the application being used, and on the behavior of the specific CIFS client. Typically, however, it is transparent to the client.

## Namespace

For CIFS users, there are several ways to access the file servers cached by the EdgeServers and integrate them within the organizational namespace. One method is to use a prefix, suffix or alias for a specific site, thus creating a unique name for each file server. (Using an alias enables the old name to be retained after replacing the local file server with the new server in the data center.) Another method is to integrate the cached file servers within the DFS namespace as DFS links. When using DFS, the DFS site name must be configured manually for each EdgeServer (or EdgeServer group). This information enables DFS to direct user requests correctly. Remote users are directed to file servers via the appropriate EdgeServer, while local users continue to access files directly, without making use of the EdgeServer cache.

For NFS users, the EdgeServer exports the original file server shares using a fixed share naming scheme. This creates unique share names while preserving their origins and context. The EdgeServer can be integrated with auto-mount facilities to provide full transparency to end users.

## SNMP Support

ActaStor exports a wide range of SNMP parameters based on SNMPv2, enabling it to integrate smoothly into an existing SNMP management system. These parameters enable system administrators to monitor the current state of the ActaStor network and its level of performance. ActaStor uses a standard, Linux-based SNMP agent that supports many of the most commonly-used SNMP managers, such as HP OpenView™ and IBM Tivoli NetView™.

ActaStor has a private, read-only MIB, starting with the OID prefix .1.3.6.1.4.1.17471.1. It can be found in each appliance at **`/usr/share/snmp/mibs/ACTONA-ACTASTOR-MIB.txt`**.

In addition, ActaStor supports the following standard MIBs:

- ▶ **MIB-2 General Network Statistics** (RFC 1213 and 1157):  
Contains essential parameters for the basic management of TCP/IP-based networks.
- ▶ **UCD Agent Extensions:** Including processes, disks, memory, load average, shell commands and error handling.
- ▶ **Host Resources** (RFC 1514)
- ▶ **SNMPv3 MIBs** (RFC 2571 through 2576)

ActaStor supports the full functionality of each of these standard MIBs, including the setting of traps. Most ActaStor traps are also recorded in the logs displayed in the Gateway Manager, although some (such as exceeding the maximum number of sessions) are reported only to the SNMP manager.

**NOTE:**



For more information about the logs, refer to *Viewing Gateway Logs* in *Chapter 4, Gateway Management*.

Exported parameters can be divided into the following categories:

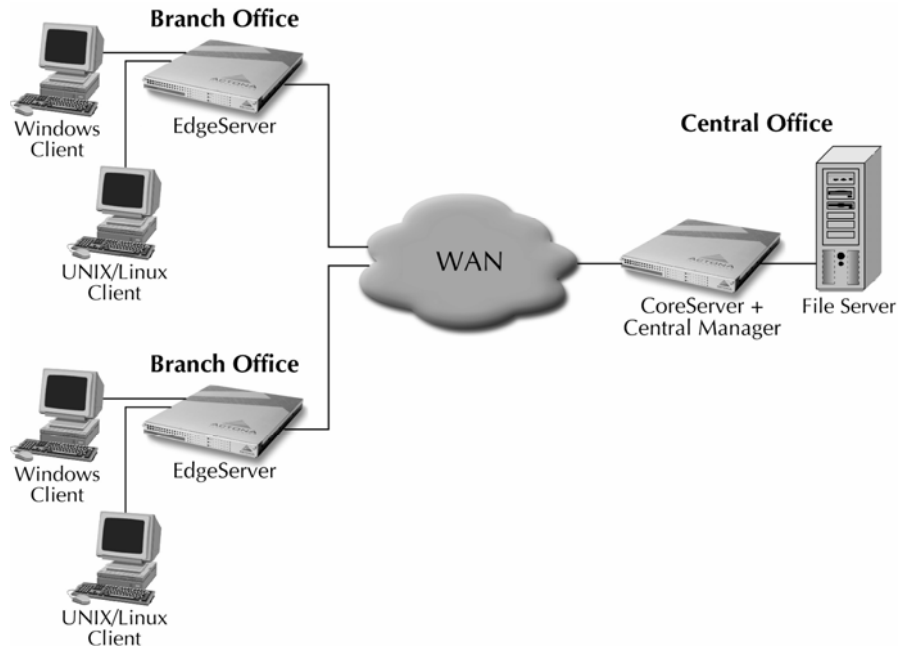
- ▶ **General parameters**, for example, the version and build numbers and license information
- ▶ **Management parameters**, for example, the location of the Central Manager
- ▶ **CoreServer parameters:**
  - General parameters
  - Network connectivity parameters
  - File servers being exported
- ▶ **EdgeServer parameters:**
  - General parameters
  - Network connectivity parameters
  - CIFS statistics
  - Cache statistics

# Planning an ActaStor Network

A typical ActaStor network is comprised of components that should be logically deployed in your network according to their defined functionality. This means that, from a functional point of view, CoreServers should be deployed near the file servers and EdgeServers should go near the users. A single Central Manager with Web-based interface (per ActaStor network) manages all the components.


There are two possible scenarios in which ActaStor is deployed:

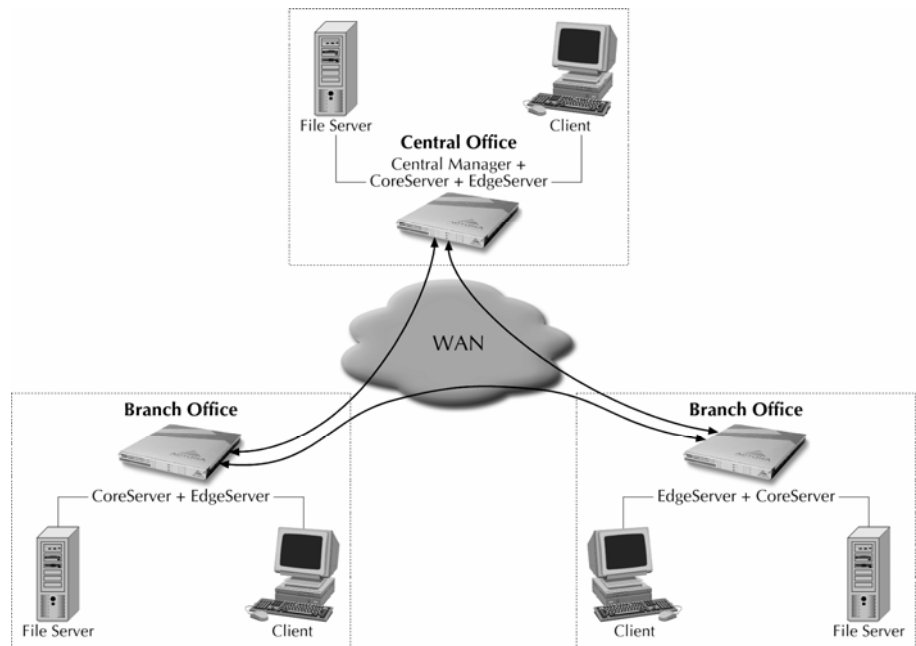
- ▲ **Centralization:** Defines an organization that consolidates its storage using file systems, as shown below in a typical centralization scenario.



**Figure 2-1: Centralization Scenario**

In this scenario, there is one Central Office (data center) that contains one or more file servers, which are exported to the users in the remote offices. Different LANs service the remote offices, with the WAN connecting the Central and branch offices. In this scenario the CoreServer is deployed in the Central Office (data center) with EdgeServers deployed in each remote office. Centralization places most of the users in the remote offices and the file servers in the Central Office. You can have users in the Central Office, but these users would typically access the main file server directly, and not through the ActaStor network. The Central Manager is typically located at the data center, either on one of the CoreServer gateways, or on a separate appliance.

- 
**Collaboration:** Defines an organization whose data is shared in a cross-like manner, as shown below in a typical collaborative scenario.



**Figure 2-2: Collaborative Scenario**

In this scenario, there are co-located CoreServers and EdgeServers deployed throughout the network, which are configured to share data in opposite directions (two cross-linked servers). The CoreServer is linked to the file server(s) and the EdgeServers are linked to the users. There is no data center concept since data sharing is symmetrical among the offices.

Logically in this scenario, the CoreServers and EdgeServers would be two separate entities. However, ActaStor currently supports a single physical appliance running both the CoreServer and EdgeServer functions.

In this scenario, the Central Manager can be located on any ActaStor gateway in the organization.

## ActaStor Capacity Limitations

When the threshold value of an operational system aspect is exceeded, ActaStor may not meet its expected service level. This may result in degraded performance.

The source of the limitation might lie in an ActaStor software component (CoreServer, EdgeServer, Gateway Manager, Central Manager or the ActaStor system as a whole), a hardware constraint or the network connecting the distributed software entities. In some cases, a limit may be resolved by adding more resources, or by upgrading the hardware or software.

When planning your network, it is important to consider its operational capacity. This means the number of users it should support, how many files it should support, how much data it should cache, and so on.

When considering the quantity of each component type required by your organization, the following factors should be taken into account:

- ▶ **The number of users connecting to the system:** This number depends on the static and dynamic capacities defined for the system:
  - **Static capacities:** Defines the number of user sessions that can connect to the system before it reaches its capacity.
  - **Dynamic capacities:** Defines the amount of traffic handled by the servers, meaning the amount of work being performed on the network. For example, whether the users currently connected to the system place a heavy or light load on it.

**NOTE:**



Dynamic limits should be calculated based on specific load assumptions, which are particular to each customer. Contact Actona Support for the limits associated with the most current ActaStor software version.

- ▶ **The total number of users in all branches that connect to the file servers through the CoreServer:** When the number of users is more than one CoreServer can support, one or more additional CoreServers must be added to the network.

To prevent loss of data due to system limitations, ActaStor provides the CoreServer cluster. This defined group of CoreServers is used primarily for the following purposes:

- To increase the scalability of the capacity of the system.
- To provide redundancy.

## Calculating the Number of Components

In order to calculate the number of CoreServer and EdgeServer components your organization requires, it is recommended to use the following criteria:

- ▲ **CoreServer:** Depends on the level of redundancy required by the organization. Each organization should have at least one CoreServer. The minimum number of CoreServers per organization is determined by  $n$ , where  $n = \frac{\text{total user population}}{\text{CoreServer capacity}}$  (the number of required CoreServers).  
To create failover clusters, it is recommended to take the following formulas into consideration:
  - **$2 * n$ :** Creates a double redundancy, meaning every EdgeServer will have an alternate CoreServer to fall back on.
  - **$n + i$  ( $i \geq 1$ ):** Solves capacity limitations by adding more machines (depending on the cost) for redundancy. In this calculation,  $i$  is the number of machines added for excess capacity and failover.
- ▲ **EdgeServer:** At least one EdgeServer is required in each remote office. Larger offices usually have multiple departments whose users work with different servers in the Central Office. In this case, it would be easier to manage your system following an organizational structure, with an EdgeServer per department. In certain cases, multiple EdgeServers can be configured as an EdgeServer group that export the same file server, providing DFS failover capabilities.
- ▲ **Central Manager:** There is always a single Central Manager in an ActaStor network.

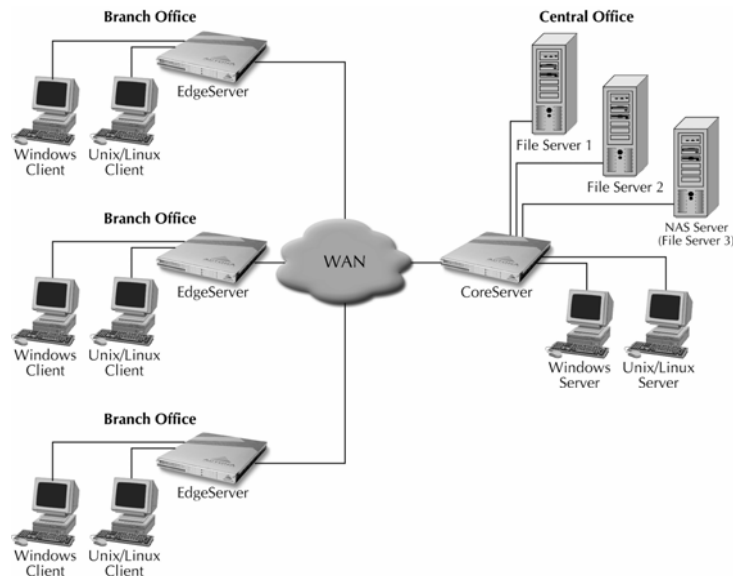


# Integrating the ActaStor Network

Prior to installing and deploying ActaStor appliances, it is necessary to collect information about your network to accommodate the ActaStor installation. In addition, a few minor adjustments may be required.

In a typical distributed organizational layout, as shown below in Figure 2-3, there are two types of networks where ActaStor is installed:

- ▶ The Central Office, where one or more co-located CoreServers provide access to the resident file servers.
- ▶ The branch offices, where EdgeServers enable users to access the file servers over the WAN.



**Figure 2-3: Distributed Organization Layout**

In collaborative networks, as described on page 2-23, there are co-located CoreServers and EdgeServers deployed throughout the network, which are configured to share data in opposite directions (two cross-linked servers).

## Pre-Installation

In order for the two appliances (CoreServer and EdgeServer) to communicate with each other, the firewall must be open. To do this, configure the firewall to open port 2000. This enables open communication between the CoreServer and EdgeServers.

### NOTE:



The default port is 4050 for Cisco WAFS. Customers running 2.5.x can manually configure their Core FE port to 4050 to avoid potential conflicts with other applications.

## Windows Network Integration

In order to successfully integrate ActaStor into the Windows environment, certain preparations may be necessary on both the CoreServer and EdgeServer sides of the network, as described in the following sections:

- ▲ **CoreServer Integration**, page 2-29, describes the preparations for the CoreServer side of the network.
- ▲ **EdgeServer Integration**, page 2-30, describes the preparations for the EdgeServer side of the network.

ActaStor supports most available Windows versions and architectures. For more information, contact Actona Support, as described in *Chapter 6, Troubleshooting*.

### NOTE:



In the Windows environment, ActaStor does not assume Windows server roles on its network, nor does it act as a Domain Controller or Master Browser. Another Windows machine should fill these roles in the EdgeServer-CoreServer network.

## CoreServer Integration

Prior to initial configuration of the CoreServer, the following parameters must be known:

- ▲ WINS server (if applicable).
- ▲ DNS server and DNS domain (if applicable).
- ▲ A browsing user with file-server directory traversal (read-only) privileges. This user, which is usually set up as a domain or service user, is required for running pre-position policies and for browsing when defining coherency policies.

### Registering the CoreServer in the DNS Server

In order to successfully integrate ActaStor into the Windows environment on the CoreServer side of a network where DHCP is not being used, you must manually add the name and IP address of the CoreServer to the DNS server. This action should be performed prior to installing and deploying the ActaStor appliances.

#### **NOTE:**



It is necessary for all ActaStor users in the EdgeServer domain to be defined in the CoreServer domain with the proper access rights to the file servers (if these were not previously defined).

## EdgeServer Integration

Prior to initial configuration of the EdgeServer, the following parameters must be known:

- ▲ DNS server and DNS domain
- ▲ Windows Domain Name
- ▲ WINS server (if applicable)
- ▲ DFS site name (if applicable)

In order to successfully integrate ActaStor into the Windows environment on the EdgeServer side of the network, the preliminary actions described below should be performed prior to installing and deploying the ActaStor appliances.

### Registering on the Domain Master Browser

In order to enable all EdgeServers in the specified domain to appear in the Network Neighborhood of users within the same domain, a Domain Master Browser or local Master Browser should be active.

### Registering the EdgeServer in the DNS Server

If DHCP is not used, you must manually add the name and IP address of the CoreServer to the DNS server.

### Adding Cached Server Names to the Active Directory Catalog

In Active Directory (AD) environments, ActaStor-cached file server names should be added manually to the AD Computer Catalog. Adding these names (including the default prefix/suffix, if any) enables future integration with AD services such as DFS. If DFS is used, note the AD Site name for the current EdgeServer location and update it in the CIFS section of the EdgeServer configuration.

## UNIX Network Integration

Prior to initial configuration of the ActaStor appliance, the following parameters must be known:

- ▲ DNS server and DNS domain.
- ▲ NIS server parameters (if applicable). For more information, refer to *Mapping Users*, page 2-32.
- ▲ [CoreServer side] A browsing UID and/or GID with file-server directory traversal (read-only) privileges. This UID/GID, which is usually set up as a domain or service user, is required for browsing when defining coherency policies.

In order to successfully integrate ActaStor into the UNIX environment, certain actions must be performed on both the CoreServer and EdgeServer sides of the network.

### Registering the Gateways in the DNS Server

In addition to the actions that ActaStor performs, and before it can be successfully integrated into the UNIX environment, you must manually add the name and IP of both the CoreServer and the EdgeServer to the DNS server.

## Mapping Users

When separate domains are used, UNIX users may be defined at the remote (branch) offices and/or on the central servers. This may result in the same user name being defined in different domains. It may then happen that a user is defined differently in the branch and center, or is defined only on one end and not the other. Consistency in such cases can be assured using NIS, or by mapping between the different domains, either manually or automatically. That is, users can be mapped from the remote server to the central servers by translating their identities from the Central Office to the remote offices, as described in *Defining Connections Between EdgeServers and CoreServers* in *Chapter 5, Central Management*.

**NOTE:**

To map users using automatic management, you must first configure the NIS server in both the CoreServer (primary) and EdgeServer (secondary).



## Chapter 3

# Installation and Deployment

### ABOUT THIS CHAPTER

This chapter describes how to install and deploy an ActaStor network, and includes the following sections:

- ▲ **Step 1: Unpacking the Hardware**, beginning on page 3-2, describes the system requirements for the ActaStor gateway and the items contained in the installation package.
- ▲ **Step 2: Installing the Appliance**, beginning on page 3-3, describes the physical installation of the gateway.
- ▲ **Step 3: Using the Setup Wizard**, beginning on page 3-5, describes how to configure the gateway and define its role in the ActaStor network via the Setup Wizard.
- ▲ **Step 4: Installing the License**, beginning on page 3-24, describes how the license file for gateway components must be installed and distributed before proceeding.
- ▲ **Step 5: Starting Components**, beginning on page 3-24, describes how the components inside the gateway must be started in order for the gateway to function.
- ▲ **Step 6: Defining Connectivity**, beginning on page 3-24, describes how to connect the gateway to other gateways.



# Step 1: Unpacking the Hardware

Prior to installing the ActaStor gateway on your local area network, make sure all the following items are in the installation package:

- ▲ ActaStor appliance
- ▲ RJ-45 Ethernet crossover cable
- ▲ Power cable
- ▲ Mounting kit for 19-inch rack
- ▲ Installation notes
- ▲ Installation disks
- ▲ ActaStor User's Guide

In addition, make sure that you have all the required data about the planned installation. For more information, refer to *Chapter 2, Getting Started*.

When DHCP (Dynamic Host Configuration Protocol) is available, gateway installation can be performed from any workstation on the network. Otherwise, installation is performed offline using a PC or laptop connected directly to the gateway as an installation console. The gateway is then connected to the network after it has been completely configured.

Using either option, make sure the PC or laptop with which you will configure the ActaStor gateway meets the following system requirements:

- ▲ Windows 2000 or Windows XP
- ▲ Available Ethernet port
- ▲ Internet Explorer 5.5 or higher

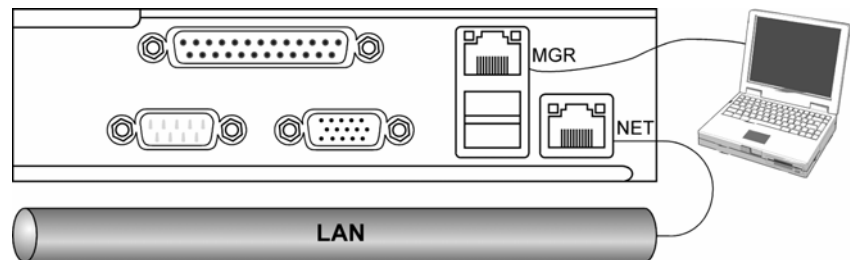
## Step 2: Installing the Appliance

To perform the installation, remove the following items from the installation package:

- ▲ ActaStor appliance
- ▲ Mounting kit for 19-inch rack
- ▲ RJ-45 Ethernet crossover cable
- ▲ Power cable

### ➤ To install the appliance:

- 1 Using the mounting kit supplied, install the appliance into the 19-inch rack. If you are using DHCP, continue with step 3.
- 2 [If not using DHCP] At the back of the appliance, connect one end of the Ethernet crossover cable to the MGR Ethernet port, as shown in Figure 3-1 below. Connect the other end of the Ethernet crossover cable to the RJ-45 Ethernet port on the installation console.



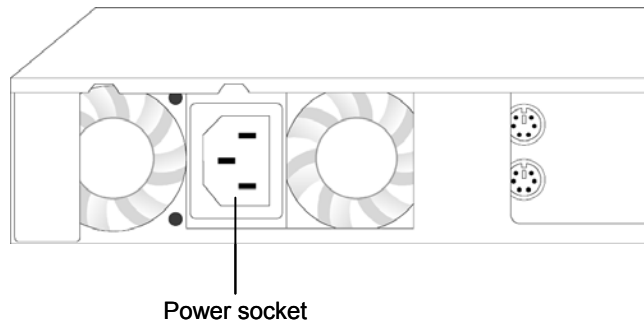
**Figure 3-1: Appliance Ports**

- 3 Connect one end of a regular Ethernet cable (not supplied) to the NET Ethernet port, as shown in Figure 3-1. Connect the other end to the local network.

**NOTE:**

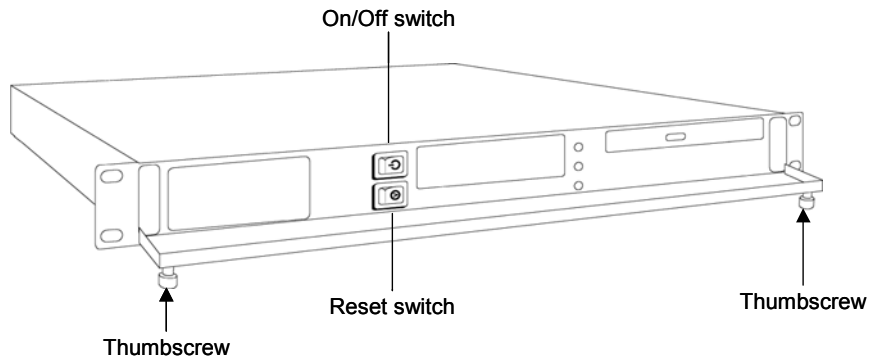
By default, ActaStor is designed to work with Ethernet networks. If a different network architecture is being used, such as Token Ring, contact Actona for further instructions.

- 4 On the left side of the appliance rear panel, connect the AC power cable to the power socket, as shown below.



**Figure 3-2: Power Socket**

- 5 On the front of the gateway, unscrew the two thumbscrews securing the front panel and open the panel, as shown below.



**Figure 3-3: Gateway Front Panel**

- 6 Power on the gateway. The upper LED lights up, indicating that the gateway has been successfully turned on. Wait for the software to load (approximately two minutes).



**NOTE:**

The installation console that will be running the Setup Wizard automatically receives the IP address from the gateway, as long as it is turned off at the time it is connected to the gateway. If the console is already running at the time of the connection and does not receive the IP address 172.30.30.xxx automatically, issue the following at the command line: `ipconfig /renew`. If this fails, reboot the console.

## Step 3: Using the Setup Wizard

After connecting the ActaStor gateway using either the crossover cable and the MGR port, or the NET port and the local network switch, you must access the Setup Wizard inside the Gateway Manager to configure the gateway. The Setup Wizard features a series of screens for defining the gateway connections and its role in the ActaStor network (EdgeServer, CoreServer or both), as well as defining whether the gateway supports replication and whether it will act as the Central Manager. After a role is selected, different configuration screens appear in the Setup Wizard according to the role(s) selected.

## Accessing the Setup Wizard

This step describes how to access the Setup Wizard using Internet Explorer 5.5 or above.

### IMPORTANT NOTE:



JavaScripts, cookies and popup windows must be enabled in the Web browser in order to use the Setup Wizard.

### ➤ To access the Setup Wizard:

- 1 Open Internet Explorer 5.5 or above, and enter the ActaStor Management address, as follows:
  - Over the network: **http://actona/mgr** or **http://actona.<your\_DNS\_domain>/mgr**
  - Using an installation console: **http://172.30.30.172/mgr**

The *Login* page is displayed.



Figure 3-4: Login Page

### NOTE:



If you cannot reach the *Login* page, refer to *Chapter 6, Troubleshooting*.

- 2 Enter the default user name (**admin**) and password (**actona**) in the fields provided, and click **Login**.

**NOTE:**



Standalone devices must allow resetting of authentication credentials when the credentials that would permit a reconfiguration of these devices have been lost. You can reset the password by deleting the Admin account. This resets the password to default. For more information, refer to “how to reset the FE-Central Manager’s administrator password” document that can be found at the following location:


[http://acpluto.cisco.com/kb/kb.asp?action=article\\_show&articleID=134](http://acpluto.cisco.com/kb/kb.asp?action=article_show&articleID=134)

When logging in for the first time to an uninitialized gateway, the first page of the Setup Wizard is displayed automatically, as shown in Figure 3-5, page 3-8.

**NOTE:**



The Setup Wizard can also be opened at any time from the Gateway Manager.

To do this, click the  icon on the upper-right side of the display area.

The Setup Wizard includes pages for the following actions:

- ▲ **Defining Local Area Connection Properties**, page 3-8, describes how to configure the appliance's local connection.
- ▲ **Defining System Properties**, page 3-9, describes how to set the time zone and the system clock of the appliance.
- ▲ **Selecting Roles**, page 3-11, describes how to select the role of the appliance in the ActaStor network.
- ▲ **Defining the EdgeServer Configuration**, page 3-12, describes how to define the initial configuration of a gateway acting as an EdgeServer.
- ▲ **Defining the CoreServer Configuration**, page 3-14, describes how to define the initial configuration of a gateway acting as a CoreServer.

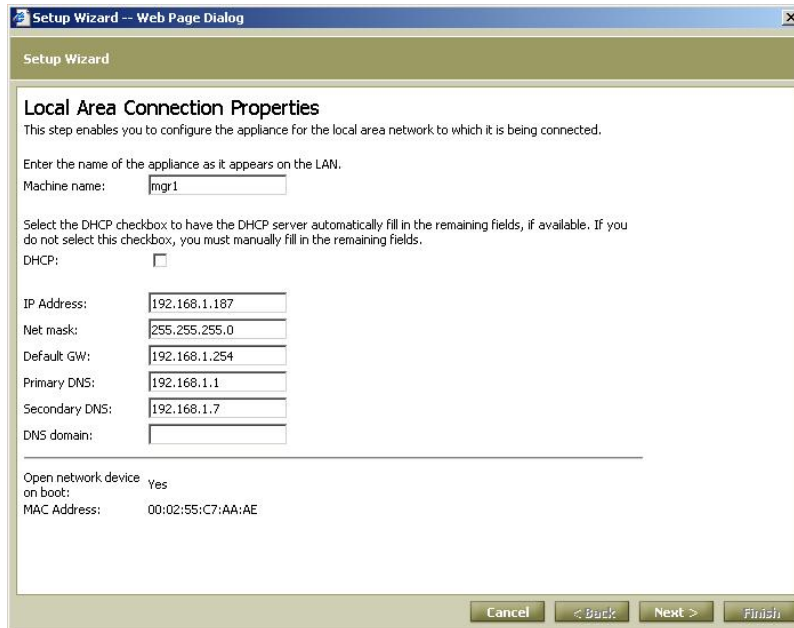
- ▶ **Defining Notification Settings**, page 3-20, describes how to define the initial configuration for email alert and/or SNMP trap notifications.
- ▶ **Registering to the Central Manager**, page 3-21, describes how to define the connection to the Central Manager.

## Defining Local Area Connection Properties

This step enables you to configure the appliance for the local area network to which it is being connected.

### ▶ To define the local area connection:

- 1 When the Setup Wizard is launched, the *Local Area Connection Properties* page is displayed.



Setup Wizard -- Web Page Dialog

Setup Wizard

### Local Area Connection Properties

This step enables you to configure the appliance for the local area network to which it is being connected.

Enter the name of the appliance as it appears on the LAN.

Machine name:

Select the DHCP checkbox to have the DHCP server automatically fill in the remaining fields, if available. If you do not select this checkbox, you must manually fill in the remaining fields.

DHCP:

IP Address:

Net mask:

Default GW:

Primary DNS:

Secondary DNS:

DNS domain:

---

Open network device on boot: Yes

MAC Address: 00:02:55:C7:AA:AE

Cancel < Back > Next > Finish

Figure 3-5: Local Area Connection Properties Page

- 2 In the **Machine name** field, enter the DNS host name of the gateway.
- 3 Select the **DHCP** checkbox to have the DHCP server automatically fill in the remaining fields, if available. If you are using a static IP, clear this checkbox and manually fill in the remaining fields, including:
  - **IP Address**
  - **Net mask**
  - **Default GW**
  - **Primary DNS**
  - **Secondary DNS** (optional)
  - **DNS domain** (optional)



**NOTE:**

Be sure to allocate and reserve an IP (static or dynamic) for the gateway.

- 4 Click **Next**. The *System properties* page is displayed, as described in the section that follows.

## Defining System Properties

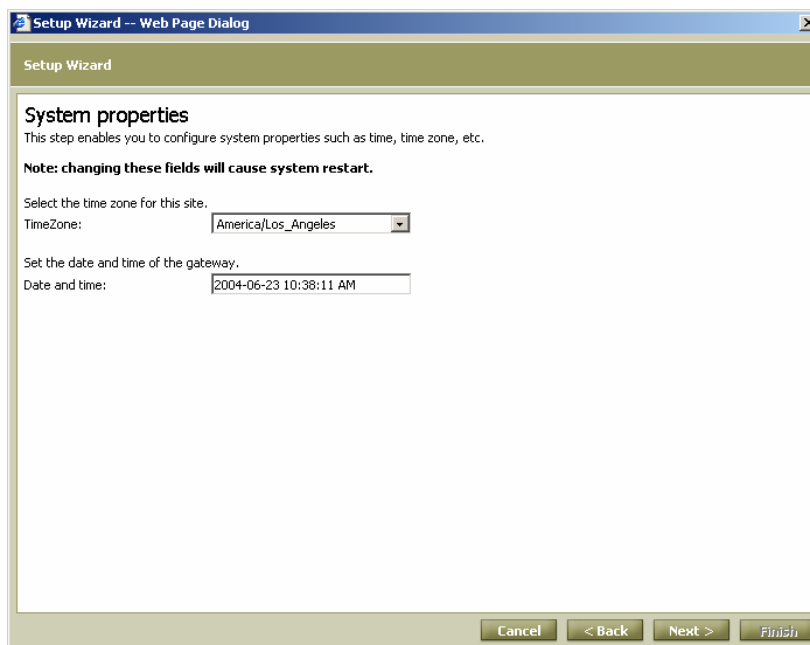
This step enables you to select the time zone of the appliance and to set the system clock. These settings are particularly important for pre-positioning, which adjusts the time when files are scheduled to be forwarded to each EdgeServer based on its time zone difference with the CoreServer.

Whenever a new time zone or clock setting is defined, the ActaStor components in the appliance are automatically restarted at the conclusion of the Setup Wizard.



➤ **To select the time zone:**

- 1 After defining the local area connection properties, click **Next**. The *System properties* page of the Setup Wizard is displayed.



**Figure 3-6: System Properties Page**

- 2 From the **TimeZone** dropdown list, select the proper time zone for the appliance. If a new time zone is selected, the ActaStor components in the appliance are automatically restarted at the end of the Setup Wizard.
- 3 Adjust the information in the **Date and time** field, if required. If the date or time is changed, the ActaStor components in the appliance are automatically restarted at the end of the Setup Wizard.
- 4 Click **Next**. The *Role Selection* page is displayed, as described in the section that follows.

## Selecting Roles

This step enables you to define the role of the gateway. Any gateway can be defined for one or more roles (EdgeServer, CoreServer, Replication, Central Manager), depending on the terms of the license purchased from Actona.

### NOTE:



For more information about the various gateway roles, refer to *Chapter 1, Introduction*.



### To select roles:

- 1 After defining system properties, click **Next**. The *Role Selection* page of the Setup Wizard is displayed.

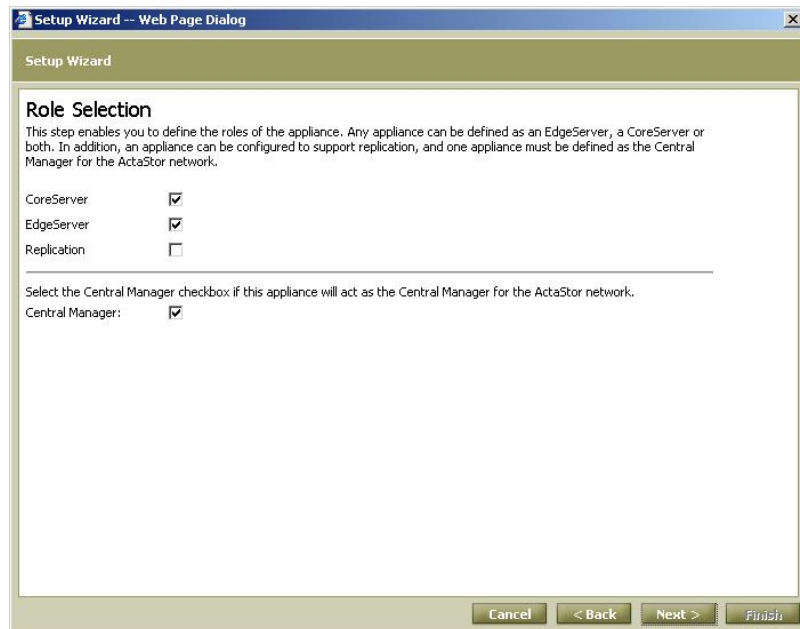


Figure 3-7: Role Selection Page

- 2 Select the checkbox next to each role for which you want the gateway defined:
  - **CoreServer**
  - **EdgeServer**
  - **Replication**
- 3 Select the **Central Manager** checkbox if this gateway will act as the Central Manager for the ActaStor network.
- 4 Click **Next**. The order of the pages following the *Role Selection* page is determined by the role(s) selected for that gateway, as follows:
  - If only the EdgeServer role was selected, the *EdgeServer Configuration* page will be the next page displayed when you click **Next**, as described below.
  - If only the CoreServer role was selected, the *CoreServer Configuration – CIFS* page will be displayed, as described on page 3-14.
  - If both EdgeServer and CoreServer were selected, the *EdgeServer Configuration* page precedes the *CoreServer Configuration – CIFS* page.

## Defining the EdgeServer Configuration

This step enables you to define the local configuration for an EdgeServer that will be used to cache content from CIFS file servers. These settings are required by the gateway to connect to the Windows environment correctly.

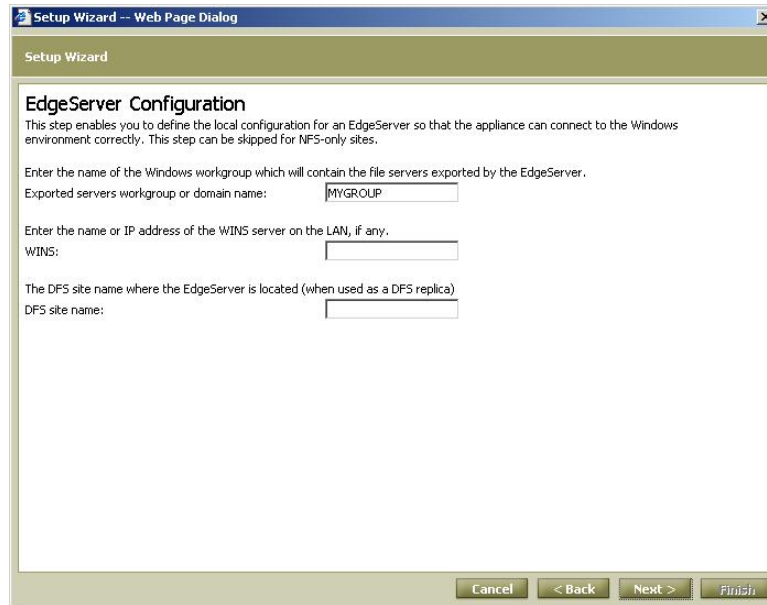
### **NOTE:**



This step can be skipped for EdgeServers that will operate only with NFS file servers.

➤ **To define the EdgeServer configuration:**

- 1 If you defined the gateway to be an EdgeServer, the *EdgeServer Configuration* page is displayed.



**Setup Wizard -- Web Page Dialog**

Setup Wizard

**EdgeServer Configuration**

This step enables you to define the local configuration for an EdgeServer so that the appliance can connect to the Windows environment correctly. This step can be skipped for NFS-only sites.

Enter the name of the Windows workgroup which will contain the file servers exported by the EdgeServer.

Exported servers workgroup or domain name:

Enter the name or IP address of the WINS server on the LAN, if any.

WINS:

The DFS site name where the EdgeServer is located (when used as a DFS replica)

DFS site name:

Cancel < Back Next > Finish

**Figure 3-8: EdgeServer Configuration Page**

- 2 In the **Exported servers workgroup or domain name** field, enter the name of the Windows workgroup or domain that will contain the file servers exported by the EdgeServer. When end users connect to the gateway, these servers will appear to the users as members of this workgroup or domain.
- 3 In the **WINS** field, enter the name or IP address of the WINS server, if any.
- 4 In the **DFS site name** field, enter the name of the Active Directory site where the EdgeServer is located, if any. This is required in order for the gateway to route requests correctly via DFS.

- 5 Click **Next**. If the gateway was also defined as a CoreServer, the *CoreServer Configuration – CIFS* page is displayed, as described in the following section. Otherwise, the *Notification Setting* page is displayed, as described on page 3-20.

## Defining the CoreServer Configuration

This step enables you to define the file servers to which this CoreServer will be connected. The file servers contain content that can be forwarded by the CoreServer to those EdgeServers connected to it. The ActaStor network supports the following file system protocols:

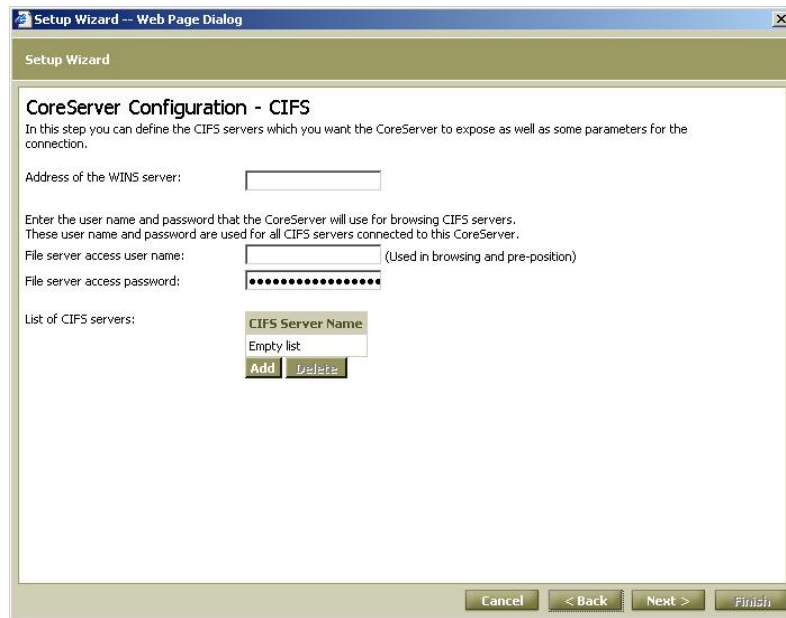
- ▲ **CIFS (Windows)**, enables you to define the CIFS servers to which you want the CoreServer to connect, as described in *Defining CIFS Servers*, page 3-15.
- ▲ **NFS (UNIX)**, enables you to define the NFS servers and connections to which the CoreServer will connect, as described in *Defining NFS Servers*, page 3-17.

## Defining CIFS Servers

You can define the CIFS file servers that you want the CoreServer to expose, as well as selected parameters required for the connection.

### ➤ To define CIFS servers:

- 1 If you defined the gateway to be a CoreServer (as described on page 3-11), the *CoreServer Configuration – CIFS* page is displayed.



The screenshot shows a web-based configuration window titled "Setup Wizard -- Web Page Dialog". The main content area is titled "CoreServer Configuration - CIFS" and contains the following elements:

- A heading "CoreServer Configuration - CIFS" followed by a descriptive paragraph: "In this step you can define the CIFS servers which you want the CoreServer to expose as well as some parameters for the connection."
- A label "Address of the WINS server:" followed by an empty text input field.
- A paragraph: "Enter the user name and password that the CoreServer will use for browsing CIFS servers. These user name and password are used for all CIFS servers connected to this CoreServer."
- A label "File server access user name:" followed by an empty text input field and the text "(Used in browsing and pre-position)".
- A label "File server access password:" followed by a password input field with masked characters (dots).
- A label "List of CIFS servers:" followed by a table with one row containing the text "CIFS Server Name". Below the table is the text "Empty list" and two buttons: "Add" and "Delete".
- At the bottom of the window are four buttons: "Cancel", "< Back", "Next >", and "Finish".

**Figure 3-9: CoreServer Configuration – CIFS Page**

- 2 In the **Address of the WINS server** field, enter the name or IP address of the WINS server, if any.

- 3 In the **File server access user name** field, enter the user name the CoreServer will use for browsing CIFS file servers. This user name is used for all CIFS file servers connected to this CoreServer. The format of the user name is: **[<domain>]\<user name>**. (Enter the domain if this is not a local user.)
- 4 In the **File server access password** field, enter the password the CoreServer will use for browsing CIFS file servers. This password is used for all CIFS file servers connected to this CoreServer.

**NOTE:**

The user name and password are required for browsing during policy definition in the Central Manager and for executing pre-position policies in the EdgeServer.

- 5 In the **List of CIFS servers** field, click **Add**. The following window is displayed:



**Figure 3-10: Adding CIFS File Servers**

- 6 In the **Server Name** field, enter the name of the CIFS file server to which you want the CoreServer to connect.
- 7 Click **Ok**. The new CIFS file server is added to the list.
- 8 Repeat steps 5 through 7 to add additional CIFS file servers, if required.

**NOTES:**



To remove a file server, select it from the list and click **Delete**.

The gateway must be re-registered with the Central Manager after making any changes to the CIFS server list. Refer to *Registering the Gateway* in *Chapter 4, Gateway Management*.

- 9 Click **Next**. The *CoreServer Configuration – NFS* page is displayed, as described in the following section.

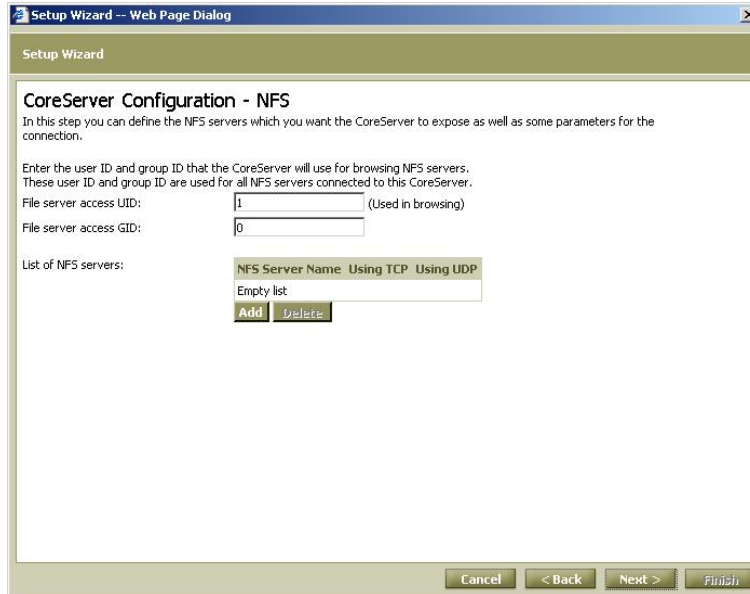
## Defining NFS Servers

You can define the NFS file servers that you want the CoreServer to expose, as well as selected parameters required for the connection.



➤ **To define NFS servers:**

- 1 If you defined the gateway to be a CoreServer (as described on page 3-11), the *CoreServer Configuration – NFS* page is displayed after the *CoreServer Configuration – CIFS* page.



Setup Wizard -- Web Page Dialog

Setup Wizard

### CoreServer Configuration - NFS

In this step you can define the NFS servers which you want the CoreServer to expose as well as some parameters for the connection.

Enter the user ID and group ID that the CoreServer will use for browsing NFS servers. These user ID and group ID are used for all NFS servers connected to this CoreServer.

File server access UID:  (Used in browsing)

File server access GID:

List of NFS servers:

NFS Server Name	Using TCP	Using UDP
Empty list		

**Figure 3-11: CoreServer Configuration – NFS Page**

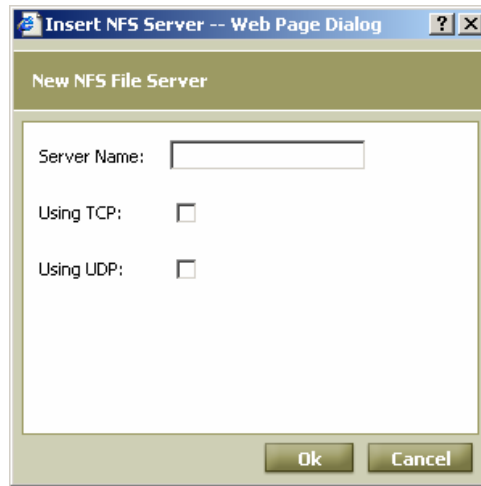
- 2 In the **File server access UID** field, enter the user ID the CoreServer will use for browsing NFS file servers. This user ID is used for all NFS file servers connected to this CoreServer.
- 3 In the **File server access GID** field, enter the group ID the CoreServer will use for browsing NFS file servers. This group ID is used for all NFS file servers connected to this CoreServer.

**NOTE:**



The UID and GID are required for browsing during policy definition in the Central Manager.

- 4 In the **List of NFS servers** field, click **Add**. The following window is displayed:



**Figure 3-12: Adding NFS File Servers**

- 5 In the **Server Name** field, enter the name of the NFS file server to which you want the CoreServer to connect, and then select the checkboxes for the appropriate connection protocols supported by the NFS file server, **Using TCP** and **Using UDP**. At least one protocol should be selected.
- 6 Click **Ok**. The new NFS file server is added to the list.
- 7 Repeat steps 4 through 6 to add more NFS file servers, if required.

**NOTE:**



To remove a file server, select it from the list and click **Delete**.

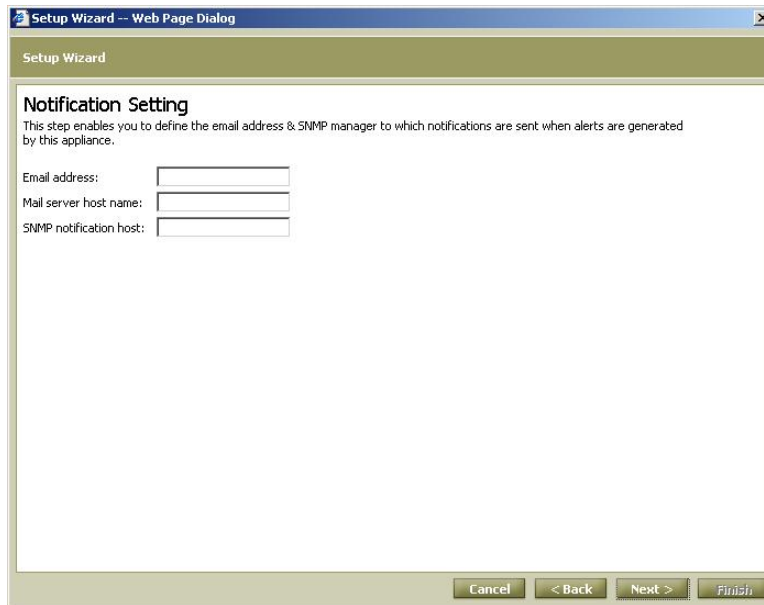
- 8 Click **Next**. The *Notification Setting* page is displayed, as described in the section that follows.

## Defining Notification Settings

This step enables you to define the email address and SNMP host to which alert notifications are sent by this gateway. The information defined on this page is the same for all roles.

➤ **To define notification settings:**

- 1 From the *CoreServer Configuration – NFS* page, click **Next** to display the *Notification Setting* page.



The screenshot shows a web browser window titled "Setup Wizard -- Web Page Dialog". The main content area is titled "Setup Wizard" and "Notification Setting". Below the title, there is a descriptive text: "This step enables you to define the email address & SNMP manager to which notifications are sent when alerts are generated by this appliance." There are three input fields: "Email address:", "Mail server host name:", and "SNMP notification host:". At the bottom of the window, there are four buttons: "Cancel", "< Back", "Next >", and "Finish".

**Figure 3-13: Notification Setting Page**

- 2 In the **Email address** field, enter the address to which notifications about this gateway are sent.

- 3 In the **Mail server host name** field, enter the name of the mail server host.

**NOTE:**



The email address defined in the Setup Wizard applies to events generated by all gateway components. In the Gateway Manager, you can define different email addresses for each specific component (role) defined for the gateway, if required, as described in *Chapter 4, Gateway Management*.

- 4 In the **SNMP notification host** field, enter the name or address of the SNMP manager (such as HP Open View™ or IBM Tivoli NetView™) that will receive trap notifications from the appliances in the ActaStor network.

**NOTE:**



For more information about the SNMP parameters exported by ActaStor gateways, refer to *SNMP Support* in *Chapter 2, Getting Started*.

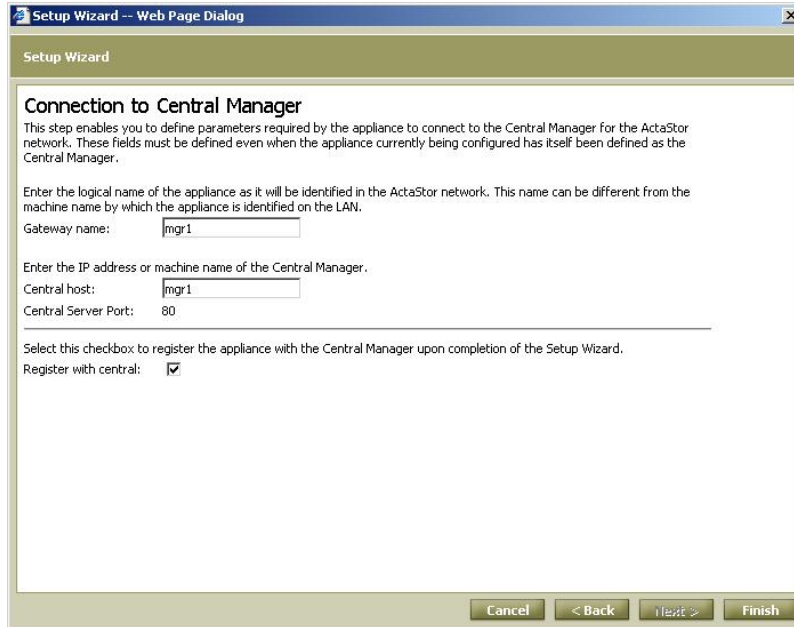
- 5 Click **Next**. The *Central Manager Connection* page is displayed, as described in the following section.

## Registering to the Central Manager

This step enables you to define parameters required by the gateway to register to the Central Manager of the ActaStor network. These fields must be defined even when the gateway currently being configured has itself been defined as the Central Manager.

➤ **To register the gateway to the Central Manager:**

- 1 From the *Notification Setting* page, click **Next** to display the *Connection to Central Manager* page.



Setup Wizard -- Web Page Dialog

Setup Wizard

### Connection to Central Manager

This step enables you to define parameters required by the appliance to connect to the Central Manager for the ActaStor network. These fields must be defined even when the appliance currently being configured has itself been defined as the Central Manager.

Enter the logical name of the appliance as it will be identified in the ActaStor network. This name can be different from the machine name by which the appliance is identified on the LAN.

Gateway name:

Enter the IP address or machine name of the Central Manager.

Central host:

Central Server Port:

---

Select this checkbox to register the appliance with the Central Manager upon completion of the Setup Wizard.

Register with central:

Cancel < Back Next > Finish

**Figure 3-14: Connection to Central Manager Page**

- 2 In the **Gateway name** field, enter the logical name of the gateway as it will be identified in the ActaStor network. This name can be different from the machine name by which the gateway is identified on the LAN, as described on page 3-8.
- 3 In the **Central host** field, enter the IP address or machine name of the Central Manager.

- 4 Select the **Register with central** checkbox to register the gateway currently being configured with the Central Manager upon completion of the Setup Wizard. If this checkbox is not selected, the gateway will not be seen by the Central Manager.

**NOTE:**



Alternatively, you can register the gateway at a later time in the **Registration** tab of the *Gateway Control* page of the Gateway Manager. In addition, re-registration must be performed whenever changes are made to the list of file servers exported by the CoreServer. For more information, refer to *Chapter 4, Gateway Management*.

- 5 Click **Finish**. If the **Register with central** checkbox was selected, the gateway is registered on the ActaStor network in the Central Manager.

**NOTE:**



If the time zone or clock setting has been changed, as described on page 3-9, clicking **Finish** automatically restarts the ActaStor components configured for the gateway. A page is then displayed that includes a link for logging back in to the Gateway Manager.

- 6 If an installation console was used during the installation and deployment process, you may now remove the crossover cable connecting the installation console to the gateway.

- 7 Close the front panel and tighten the two thumbscrews.

After the new gateway has been installed and registered in the ActaStor network, it can be managed remotely from any location on the network via Internet Explorer, as described in *Chapter 4, Gateway Management* and *Chapter 5, Central Management*.

The license file, which defines the components that can be run on the gateway and for how long, can now be installed using the Central Manager, as described in the section that follows.

## Step 4: Installing the License

Activating specific components inside a gateway requires a license file obtained from Actona. The Central Manager must be directed to this file, whose information is then distributed to the relevant gateway.

For more information, refer to *Managing Licenses* in *Chapter 5, Central Management*.

## Step 5: Starting Components

After installing the license, the components inside the gateway can be started, enabling it to become a fully functioning part of the ActaStor network.

For more information about starting the components inside the gateway, refer to *Starting and Stopping Components* in *Chapter 4, Gateway Management*. To perform this action for all gateways simultaneously, refer to *Performing Operations on All Gateways* in *Chapter 5, Central Management*.

## Step 6: Defining Connectivity

Use the **Connectivity** option in the Central Manager to connect it to other gateways according to its assigned role. For more information, refer to *Defining Connections Between EdgeServers and CoreServers* in *Chapter 5, Central Management*.

**NOTE:**

Refer to *Appendix A, Sample Installation*, for a step-by-step guide to installing a complete ActaStor network.

# Chapter 4

## Gateway Management

### ABOUT THIS CHAPTER

This chapter describes the Gateway Manager, and includes the following sections:

- **Launching the Gateway Manager**, beginning on page 4-3, describes how to launch the Gateway Manager.
- **Gateway Manager Quick Tour**, beginning on page 4-4, describes the Gateway Manager graphic user interface (GUI).
- **Gateway Management Workflow**, beginning on page 4-6, describes what to do after a gateway has been deployed.
- **Managing the Gateway**, beginning on page 4-7, describes how to manage the gateway using the Gateway Manager.
- **Managing the CoreServer Component**, beginning on page 4-27, describes how to manage the CoreServer component of the gateway.
- **Managing the EdgeServer Component**, beginning on page 4-34, describes how to manage the EdgeServer component of the gateway.



- **Managing the Replication Component**, beginning on page 4-44, enables you to monitor the progress, and optionally terminate, replication policies created in the Central Manager.
- **Monitoring the Gateway**, beginning on page 4-49, describes how to view connectivity statistics regarding CoreServers and EdgeServers, and how to generate graphs containing information about each gateway component.
- **Viewing Gateway Logs**, beginning on page 4-63, describes how to view the logs of the various gateway components.

# Launching the Gateway Manager

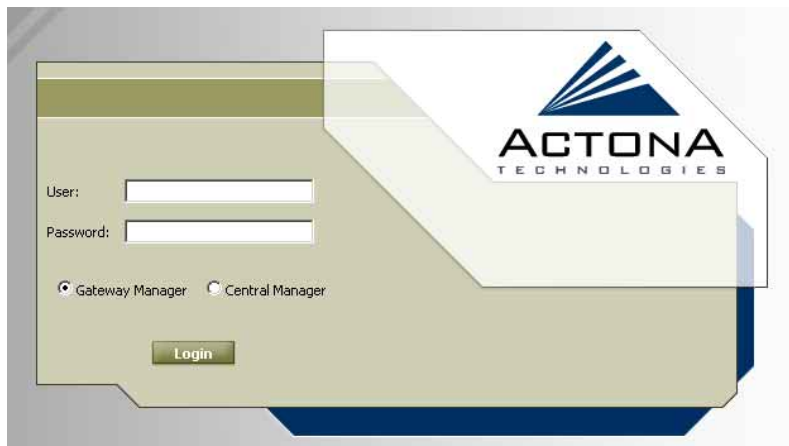
Each gateway is managed separately, via an accessible Web-based interface enabling remote management of that gateway. You can launch the Gateway Manager remotely from any location on the ActaStor network via Internet Explorer.

➤ **To launch the Gateway Manager:**

- 1 Open Internet Explorer 5.5 or above, and enter the ActaStor Management address:

**http://<Gateway\_Manager\_IP\_Address>/mgr.**

The *Login* page of the ActaStor Manager is displayed:



**Figure 4-1: Login Page – Gateway Manager**

- 2 Enter your user name and password in the fields provided. The default user name is **admin** and the default password is **actona**.
- 3 Select the **Gateway Manager** option and click **Login** to display the Gateway Manager interface, as shown in Figure 4-2.

# Gateway Manager Quick Tour

The Gateway Manager interface is divided into two sections. The area on the left displays the navigation area. The display area on the right displays information relevant to the options you have selected from the navigation area.

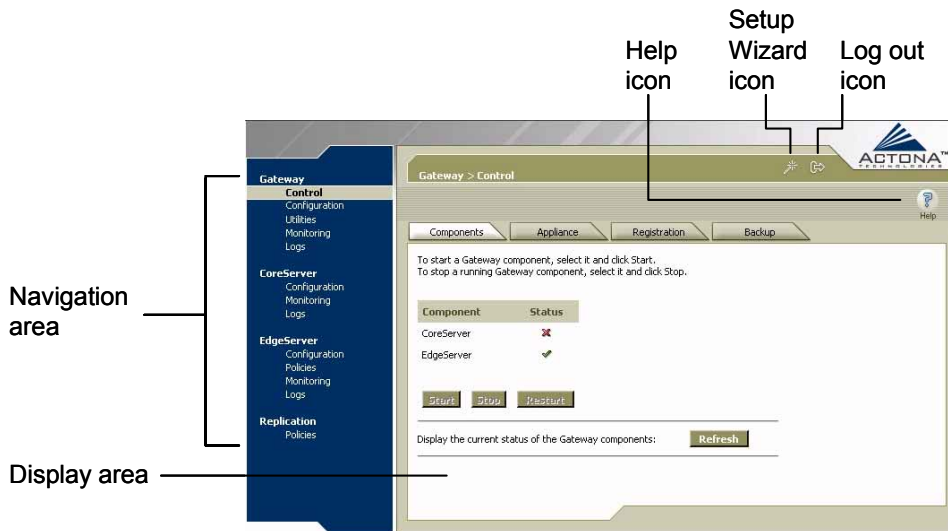


Figure 4-2: Gateway Manager

The navigation area enables you to navigate the management screens for different gateway components. It includes the following options:


- **Gateway:** Enables you to control gateway components, register/unregister the gateway, backup/restore configuration files and use various gateway utilities. For more information, refer to *Managing the Gateway*, page 4-7.
- **CoreServer:** Enables you to select the file servers to which the CoreServer will connect. For more information, refer to *Managing the CoreServer Component*, page 4-27.

- ▶ **EdgeServer:** Enables you to set the default coherency age for directory listings and other CIFS settings, perform name registrations and view CoreServer connections. For more information, refer to *Managing the EdgeServer Component*, page 4-34.
- ▶ **Replication:** Enables you to monitor the progress, and optionally terminate, replication policies created in the Central Manager. For more information, refer to *Managing the Replication Component*, page 4-44.

#### NOTES:




The component options displayed for a particular gateway are determined by the roles that were selected and configured in the Setup Wizard, as described in *Chapter 3, Installation and Deployment*.

To open the Setup Wizard, click the  icon on the upper-right side of the display area.

The options in the navigation area include suboptions, which when selected, display additional tabs in the display area. Mandatory fields in the display area are indicated with an asterisk. If you click **Save** without entering a value in a mandatory field, an error message is displayed. Click the **Back** link to return to the page where the error occurred.

Information displayed in tables can be sorted by clicking the column headers. Clicking the header a second time sorts the information in reverse order.

As you navigate in the Gateway Manager, your current location is always displayed across the top of the display area.

To log out of the Gateway Manager, click the  icon on the upper-right side of the display area.

#### IMPORTANT NOTE:



JavaScripts, cookies and popup windows must be enabled in the Web browser in order to use the Gateway Manager.

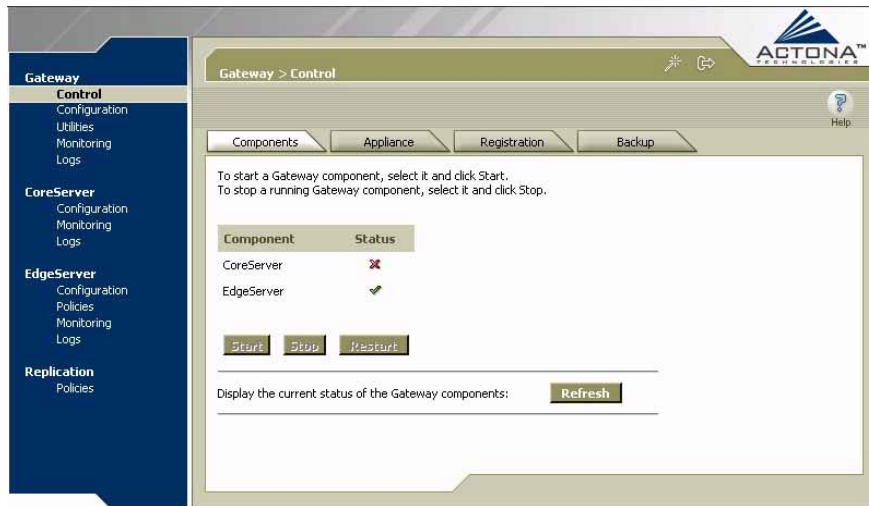
# Gateway Management Workflow

After gateways have been deployed and registered, as described in *Chapter 3, Installation and Deployment*, use the Gateway Manager to modify settings defined in the Setup Wizard, as well as to:

- ▶ Start and stop components, as described in *Starting and Stopping Components*, page 4-8.
- ▶ Reboot the gateway, as described in *Rebooting the Gateway*, page 4-11.
- ▶ Register/unregister the gateway, as described in *Registering the Gateway*, page 4-12.
- ▶ Back up and restore configuration files, as described in *Backing Up and Restoring Configuration Files*, page 4-13.
- ▶ Configure the gateway to provide print services to its clients, as described in *Configuring Print Services*, page 4-18.
- ▶ Define component-specific notification recipients, as described in *Defining Notification Settings*, page 4-23.
- ▶ Run gateway maintenance utilities, as described in *Utilities Option*, page 4-24.
- ▶ View the details, current status and history of pre-position tasks performed on EdgeServer components, as described in *Policies Option*, page 4-39.
- ▶ Manage replication tasks, as described in *Managing the Replication Component*, page 4-44.
- ▶ View SNMP-generated information and graphs about each gateway component, as described in *Monitoring the Gateway*, page 4-49.
- ▶ View the logs for each gateway component, as described in *Viewing Gateway Logs*, page 4-63.

# Managing the Gateway

The **Gateway** option in the navigation area is used to perform basic gateway operations, as well as to view the status of gateway components.



**Figure 4-3: Gateway Control Page**

The Gateway component includes the following options:

- **Control:** Enables you to control the gateway and its components, as described in *Control Option*, page 4-8.
- **Configuration:** Enables you to perform basic configuration tasks, as described in *Configuration Option*, page 4-14.
- **Utilities:** Enables you to run various maintenance utilities on the gateway, as described in *Utilities Option*, page 4-24.
- **Monitoring:** Enables you to view tables and graphs related to CPU and disk utilization in the gateway, as described in *Monitoring the Gateway*, page 4-49.
- **Logs:** Enables you to view event logs for various gateway subsystems, as described in *Viewing Gateway Logs*, page 4-63.

## Control Option

The **Control** option displays the following tabs:

- **Components:** Enables you to view the working status of each Gateway component. You can start, stop and restart any component, as required. For more information, refer to *Starting and Stopping Components*, below.
- **Appliance:** Enables you to shut down and reboot the gateway, as described in *Rebooting the Gateway*, page 4-11.
- **Registration:** Enables you to register or unregister the gateway on the ActaStor network. For more information, refer to *Registering the Gateway*, page 4-12.
- **Backup:** Enables you to download and save gateway configuration files, and to restore these files back to the gateway, if required. For more information, refer to *Backing Up and Restoring Configuration Files*, page 4-13.

## Starting and Stopping Components

The **Components** tab enables you to view which components defined for the gateway are running and which are not, as well as start, stop and restart components, as required.

Only licensed components may be started. For more information about managing licenses, refer to *Chapter 5, Central Management*.

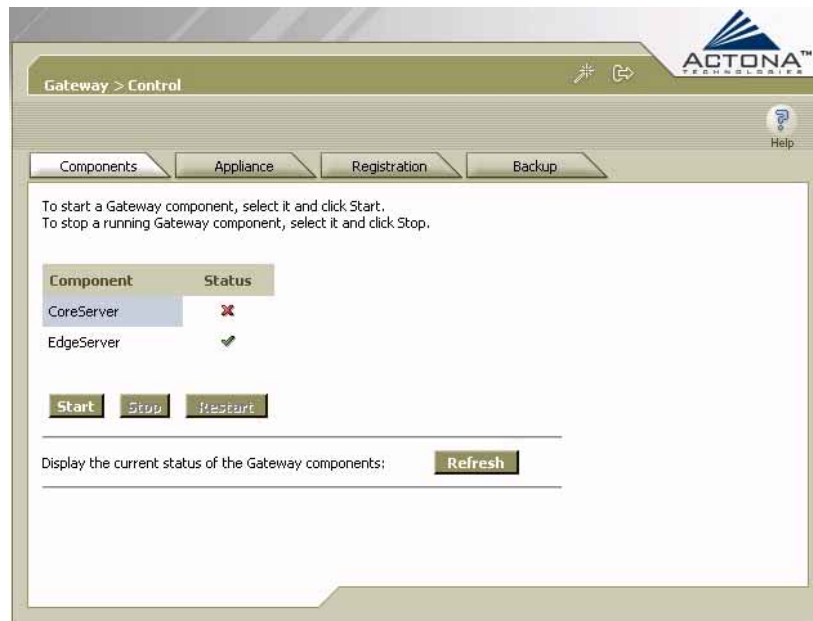
### NOTE:



If a component is not running, most of its configuration can be performed offline. However, any configuration changes made to the component will take effect only after it is restarted.

➤ **To start and stop components:**

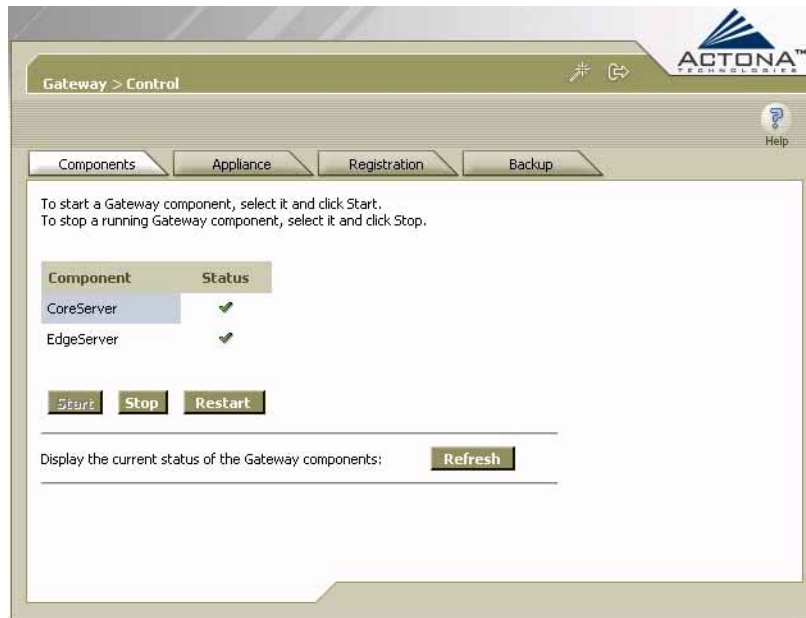
- 1 In the **Components** tab of *Gateway Control* page, select the component you want to activate and click **Start**. After a few seconds, a green checkmark ✓ will appear next to the selected component, indicating its status as "running", as shown below.



**Figure 4-4: Components Tab – Starting Components**



- 2 To stop a component, select it from the list and click **Stop**. After a few seconds, a red **X** will appear next to the selected component, indicating that it is no longer running, as shown below.



**Figure 4-5: Components Tab – Stopping Components**

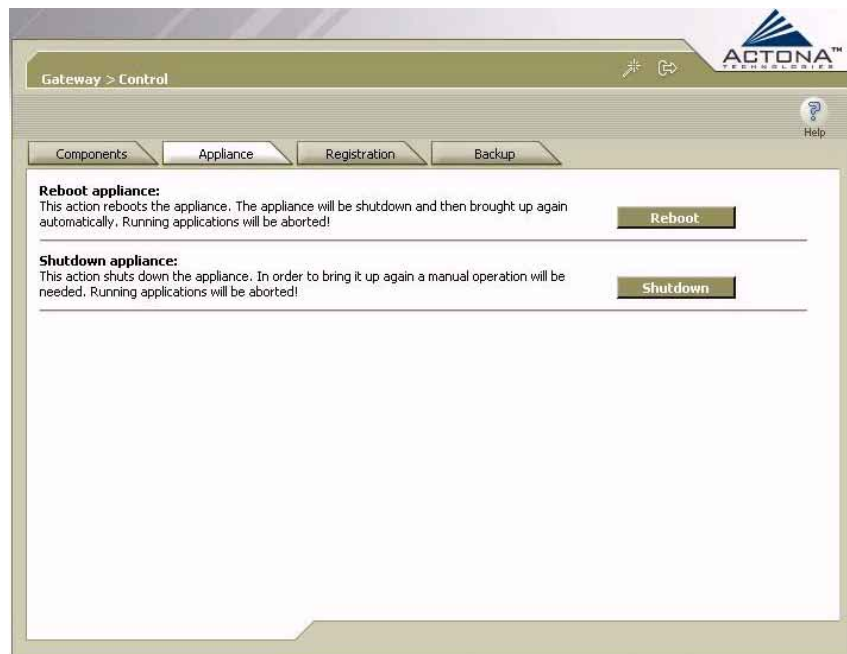
- 3 To restart a Gateway component, select it from the list and click **Restart**.
- 4 To display the current status of the Gateway components, click **Refresh**.

## Rebooting the Gateway

The **Appliance** tab enables you to shut down and reboot the gateway, if required. Shutting down or rebooting the gateway aborts any operations that may be running, including your Manager session.

### ➤ To shut down and reboot the appliance:

- 1 In the *Gateway Control* page, click the **Appliance** tab to display the following:



**Figure 4-6: Gateway Control – Appliance Tab**

- 2 To reboot the gateway, click **Reboot**.
- 3 To shut down the gateway, click **Shutdown**.

## Registering the Gateway

The **Registration** tab enables you to register the gateway as part of the ActaStor network, or unregister it, as required. After the gateway is registered, it can be managed using the Central Manager.

➤ **To register the gateway:**

- 1 In the *Gateway Control* page, click the **Registration** tab to display the following:



**Figure 4-7: Gateway Control – Registration Tab**

- 2 To register the gateway as part of the ActaStor network, click **Register**. If successful, the message, **Appliance registered successfully**, is displayed.

- 3** To unregister the gateway as part of the ActaStor network, click **Unregister**. If successful, the message, **Appliance unregistered successfully**, is displayed.



**NOTE:**

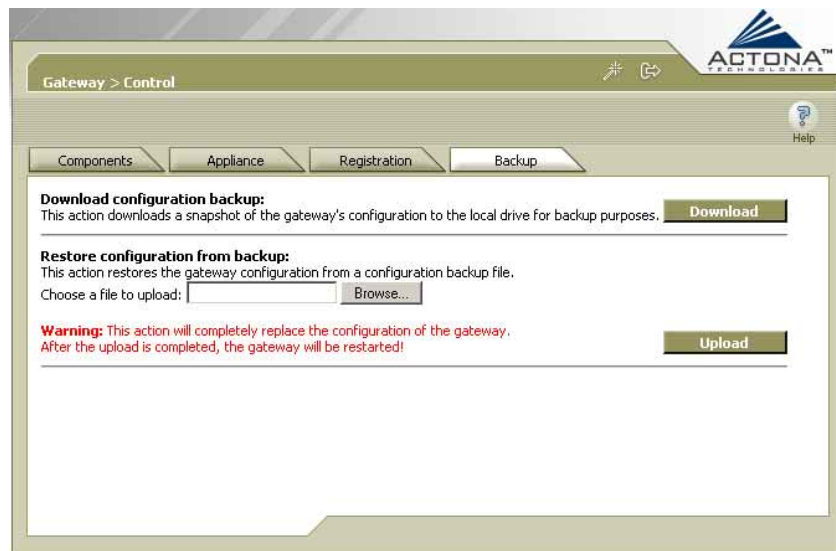
Unregistering a gateway removes any policies defined for it in the Central Manager.

## Backing Up and Restoring Configuration Files

The **Backup** tab enables you to backup and restore the configuration files of the gateway, as required. Restoring the configuration returns the gateway to its previous state when the backup was performed.

### ➤ To back up the gateway configuration:

- 1** In the *Gateway Control* page, click the **Backup** tab to display the following:



**Figure 4-8: Gateway Control – Backup Tab**

- 2 In the **Download configuration backup** area, click **Download**.
- 3 In the *File Download* window, click **Save**.
- 4 In the *Save As* window, browse to where you want to save the file. You can also change the file name, if needed.
- 5 Click **Save**. The gateway configuration files are downloaded to the selected destination folder and stored in a single, compressed file.

➤ **To restore the configuration files:**

- 1 In the **Restore configuration from backup** area, click **Browse** to navigate to the location of the backup file that you want to restore.
- 2 Click **Upload** to restore the selected configuration files.

## Configuration Option

The **Configuration** option for the Gateway component displays the following tabs:

- **Manager:** Enables you to define the logical name of the gateway as it will be identified in the ActaStor network. For more information, refer to *Defining the Manager Configuration*, page 4-15.
- **SNMP:** Enables you to define the SNMP manager that receives SNMP Inform (trap) messages from the gateway. For more information, refer to *Defining the SNMP Manager*, page 4-16.
- **Networking:** Enables you to view gateway settings defined in the Setup Wizard. For more information, refer to *Viewing Connection Settings*, page 4-17.
- **Print Services:** Enables you to define the settings required by the gateway to provide print services to the network. For more information, refer to *Configuring Print Services*, page 4-18.

- ▶ **Notifier:** Enables you to define the email address to which notifications are sent when alerts are generated by the gateway. For more information, refer to *Defining Notification Settings*, page 4-23.

**NOTE:**  
 ↩ The same **Notifier** option is available in the Replication, EdgeServer and CoreServer components.

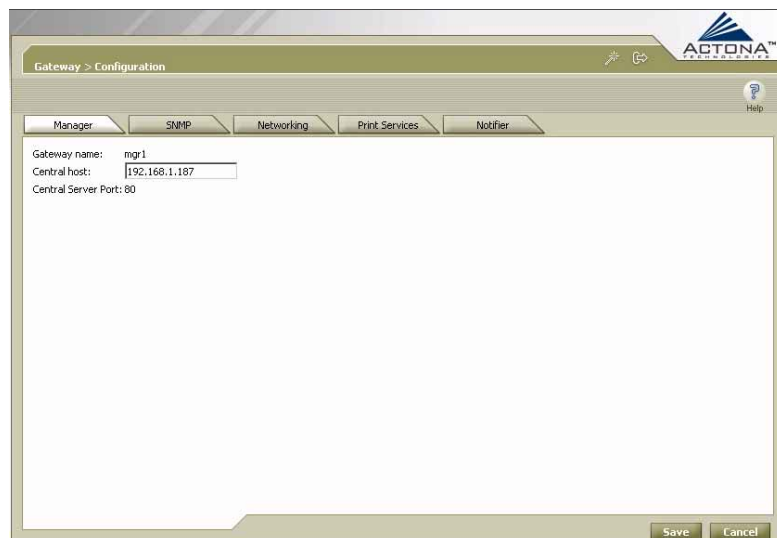
## Defining the Manager Configuration

The **Manager** tab enables you to modify the connection of the gateway to the Central Manager.

**NOTE:**  
 ↩ This parameter is typically defined in the Setup Wizard during deployment, as described in *Chapter 3, Installation and Deployment*.

### ▶ To configure the Manager component:

- 1 In the *Configuration* page, click the **Manager** tab to display the following:



**Figure 4-9: Gateway Configuration – Manager Tab**

- 2 In the **Central host** field, enter the IP address or machine name of the Central Manager to which this gateway reports.

**NOTE:**

If the gateway currently being configured is itself the Central Manager, enter the name of the machine.

- 3 Click **Save**.

## Defining the SNMP Manager

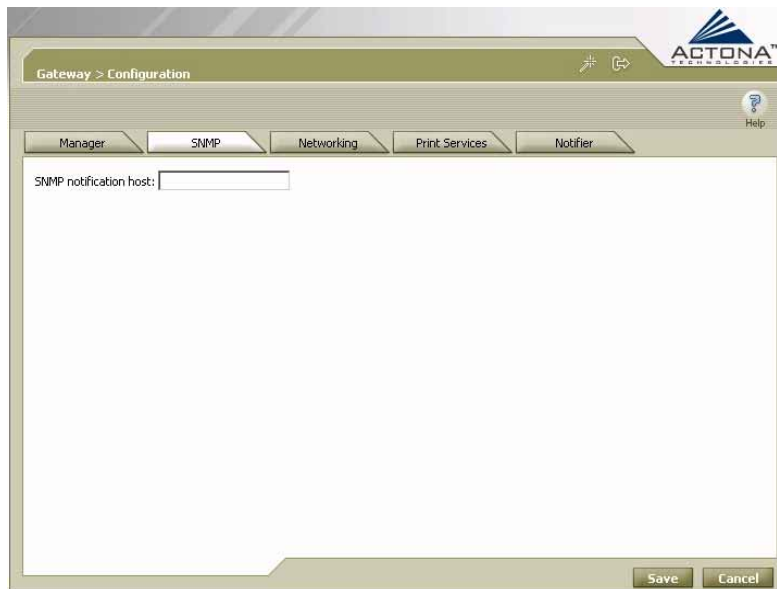
The SNMP tab enables you to define the SNMP manager used to receive traps generated by the gateway.

**NOTE:**

For more information, refer to *SNMP Support* in *Chapter 2, Getting Started*.

### ➤ To define the SNMP manager:

- 1 In the *Configuration* page, click the **SNMP** tab to display the following:



**Figure 4-10: Gateway Configuration – SNMP Tab**

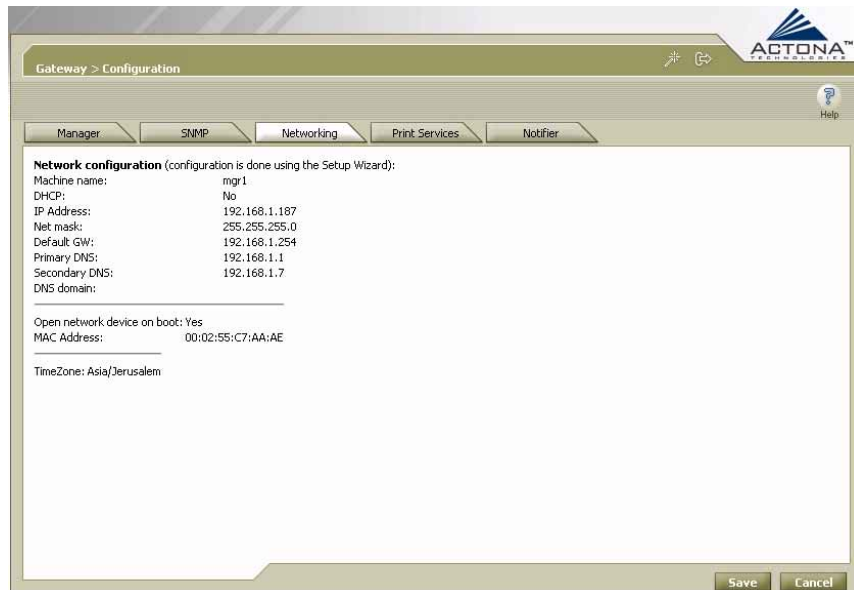
- 2 In the **SNMP notification host** field, enter the name or IP address of the SNMP manager that will receive SNMP Inform (trap) messages generated by the gateway.
- 3 Click **Save**.

## Viewing Connection Settings

The **Networking** tab enables you to view the connection parameters between the gateway and the LAN that were defined in the Setup Wizard.

➤ **To view the gateway connection settings:**

In the *Configuration* page, click the **Networking** tab to display the following:



**Figure 4-11: Gateway Configuration – Networking Tab**



The **Networking** tab contains the following information:

- ▲ **Machine name:** The name of the gateway as it is known by the LAN. This name may be different from the one the gateway is known by in the ActaStor network.
- ▲ **DHCP:** Whether a DHCP server is available on the network.
- ▲ **IP address**
- ▲ **Net mask**
- ▲ **Default GW**
- ▲ **Primary DNS**
- ▲ **Secondary DNS**
- ▲ **DNS domain**
- ▲ **MAC address**
- ▲ **Time zone**

## Configuring Print Services

The **Print Services** tab enables you to configure print services for Windows clients who access the gateway. Any gateway can be configured to act as a print server, regardless of its role.

When configuring print services, you must configure addressing information for the print server. You also must choose whether CUPS (the third-party application that interfaces with the printer) can be configured from any location or only from a specific IP address. In addition, a link is provided to the CUPS administration page.

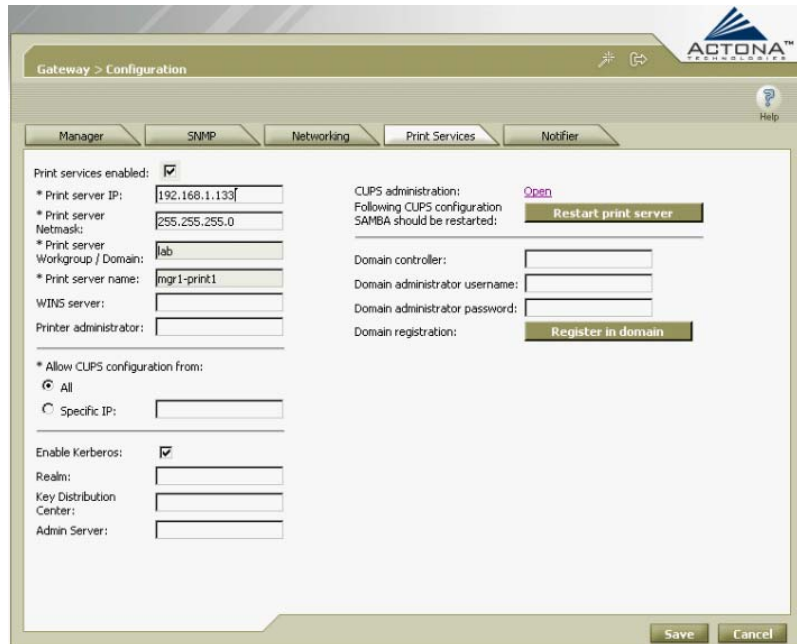
### **NOTE:**



Print services for UNIX clients are not supported in the current version. For more information about print services, refer to *Print Services* in *Chapter 2, Getting Started*.

➤ **To configure print services on the gateway:**

- 1 In the *Configuration* page, click the **Print Services** tab to display the following:



The screenshot shows the 'Print Services' configuration tab in the Gateway Management interface. The 'Print services enabled' checkbox is checked. The configuration fields are as follows:

- \* Print server IP: 192.168.1.133
- \* Print server Netmask: 255.255.255.0
- \* Print server Workgroup / Domain: lab
- \* Print server name: mgr1-print1
- WINS server: (empty)
- Printer administrator: (empty)
- \* Allow CLUPS configuration from:
  - All
  - Specific IP: (empty)
- Enable Kerberos: 
  - Realm: (empty)
  - Key Distribution Center: (empty)
  - Admin Server: (empty)

Additional options and buttons include:

- CLUPS administration: [Open](#)
- Following CLUPS configuration SAMBA should be restarted: **Restart print server**
- Domain controller: (empty)
- Domain administrator username: (empty)
- Domain administrator password: (empty)
- Domain registration: **Register in domain**

At the bottom right, there are **Save** and **Cancel** buttons.

**Figure 4-11: Gateway Configuration – Print Services Tab**

- 2 Select the **Print services enabled** checkbox. A series of fields are displayed beneath the checkbox.
- 3 Enter the following addressing information for the print server in the fields provided:
  - IP address (must differ from the IP of the gateway itself)
  - Net mask
  - Workgroup/domain
  - NetBIOS name of the print server
  - WINS server (if any)
  - Printer administrator

- 4 In the **CUPS administration** field, click the **Open** link. The administration page of the CUPS application is displayed, enabling you to configure printer options, as required. This includes the name and IP address of the printer, as well as the complete set of printing options available for that printer.

**NOTES:**

In order to access the CUPS administration page, make the following configuration change in Internet Explorer: **Tools** → **Internet Options** → **Connections** → **LAN Settings** and deselect the **Automatically detect settings** checkbox.

When you have finished printer configuration in CUPS, click **Restart print server** to reboot Samba, which is the platform on which ActaStor's print services are based. For more information about CUPS, refer to <http://www.easysw.com/> and <http://www.cups.org/>.

- 5 In the **Allow CUPS configuration from** field, select **All** to enable print service settings to be configured from any IP on the network, or **Specific IP** to enable configuration only from a specific address. Enter the address in the field provided.

**NOTE:**

Administrator credentials are required to register the print server in the selected domain. These credentials are discarded when you log out or the session expires.

- 6 Select the **Enable Kerberos** checkbox to enable Kerberos authentication, an additional domain security level used to avoid impersonation.

If this option is selected, enter the required information in the following fields:

- **Realm:** Security key used by Kerberos.
- **Key Distribution Center:** Hostname of the key distribution center (kdc).
- **Admin Server:** Hostname of admin server.

- 7 Click **Save**. The print server settings are saved.

- 8 If the NetBIOS name of the print server is being entered for the first time (as described in step 3), you must register the print server with the domain. To do this, enter information about the domain controller in the following fields:
- **Domain controller:** Name of the server acting as the domain controller.
  - **Domain administrator username:** User name of the domain controller administrator (without the domain name).
  - **Domain administrator password:** Password of the domain controller administrator.

The domain controller authenticates the credentials of users wishing to access print services.

- 9 Click **Register in domain**. The print server is registered in the defined domain.

**NOTE:**



The printer server must be re-registered after any change to the NetBIOS name of the print server. To do this, enter the domain controller, domain administrator username and password, and click **Register in Domain**.

You must now configure the necessary printer drivers in order to use the print services of the gateway, as described in the section that follows.

**NOTE:**



The printer driver can be configured only by an administrator. For additional information, contact Actona Support.

## Configuring Printer Drivers

After configuring the printer settings in the CUPS administration page and the print services in the **Print Services** tab, you must upload the necessary printer drivers to enable users to begin using the print service. This is done via the Network Neighborhood in Windows.

### ➤ **To configure printer drivers:**

- 1** Open the Network Neighborhood.
- 2** Browse to the Samba host, meaning, the NetBIOS name of the configured printer.
- 3** Open the **Printer & Faxes** folder.
- 4** Double-click the printer icon and then select **Printer** → **Properties**.
- 5** In the **Advanced** tab, click **New Driver**. The Add Printer Driver wizard is displayed.
- 6** Continue with the wizard as when normally adding a printer driver. The necessary driver can be uploaded either from the list of currently available drivers or from a disk.

## Defining Notification Settings

The **Notifier** tab enables you to define the email address to which notifications are sent when alerts are generated by the gateway.

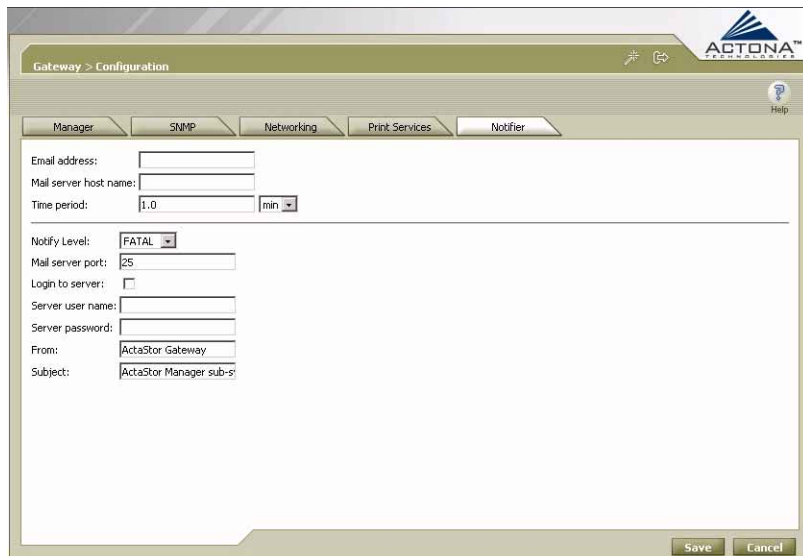
### NOTE:



Any changes implemented in the **Notifier** tab for a specific component override settings configured in the Setup Wizard. For more information, refer to *Chapter 3, Installation and Deployment*.

### ➤ To define notification settings:

- 1 In the *Configuration* page, click the **Notifier** tab to display the following:



Gateway > Configuration

Manager | SNMP | Networking | Print Services | **Notifier** | Help

Email address:

Mail server host name:

Time period:  min

---

Notify Level:

Mail server port:

Login to server:

Server user name:

Server password:

From:

Subject:

Save Cancel

**Figure 4-13: Notifier Tab**

- 2 In the **Email address** field, enter the address to which notifications about this gateway are sent.
- 3 In the **Mail server host name** field, enter the name of the mail server host.

- 4 In the **Time period** field, enter the time interval for notifications to accumulate until they are sent via email and select the relevant time unit from the dropdown list, **min** or **sec**.
- 5 From the **Notify Level** dropdown list, select the minimum event severity level for generating notifications.
- 6 In the **Mail server port** field, enter the port number for connecting with the mail server.
- 7 Select the **Login to server** checkbox if the gateway must log in to the mail server to send notifications. If this option is selected, additional fields are enabled, as described below.
- 8 In the **Server user name** field, enter the user name for accessing the mail server.
- 9 In the **Server password** field, enter the password for accessing the mail server.
- 10 In the **From** field, enter the text that should appear in the From field of each email notification.
- 11 In the **Subject** field, enter the text that should appear as the subject of each notification.
- 12 Click **Save**.

## Utilities Option

The **Utilities** option displays the following tabs:

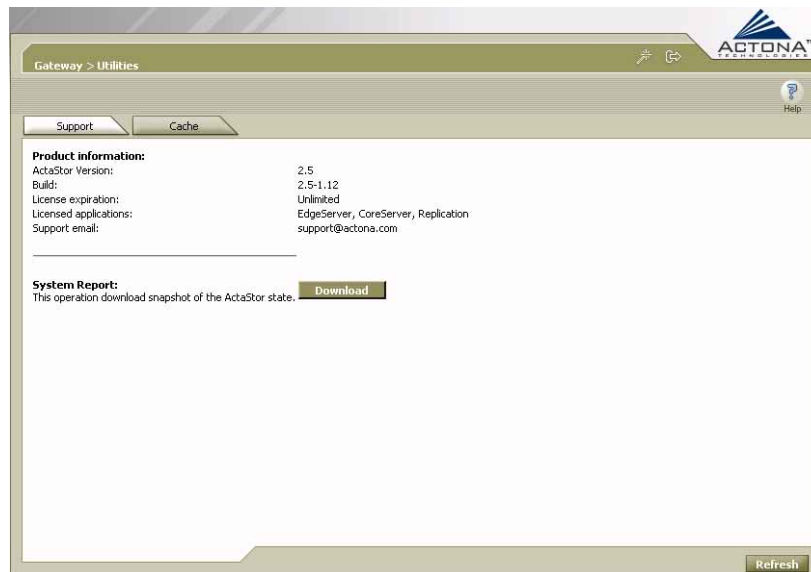
- ▲ **Support:** Enables you to dump gateway data to an external location for support purposes. For more information, refer to *Running Support Utilities*, page 4-25.
- ▲ **Cache:** Enables you to synchronize the gateway cache. For more information, refer to *Running the Cache Removal Utility*, page 4-26.

## Running Support Utilities

The **Support** tab displays product information about ActaStor, including the version and build numbers, as well as licensing information, including the expiration date and the applications covered by the license. It also enables you to capture a snapshot of the current state of the gateway and its operation, including the configuration log files of various components. This report can then be sent to Actona Support when in need of assistance.

### ➤ To download ActaStor system information:

- 1 In the *Utilities* page, click the **Support** tab to display the following:



**Figure 4-14: Utilities – Support Tab**

- 2 In the **System Report** field, click **Download** to start the collection process.



- 3 In the *File Download* window, click **Save**.
- 4 In the *Save As* window, browse to where you want to save the file. (You can also change the file name, if needed.) Click **Save**. The file is saved in tar gzip format.

## Running the Cache Removal Utility

The **Cache** tab enables you to activate the Cache Removal utility, which clears the contents of the EdgeServer cache. The EdgeServer must be stopped, as described on page 4-8, before the utility is run.

➤ **To run the cache removal utility:**

- 1 In the *Utilities* page, click the **Cache** tab to display the following:



**Figure 4-15: Utilities – Cache Tab**

- 2 In the **Cache Removal** field, click **Run** to erase the contents of the cache.

# Managing the CoreServer Component

When managing gateways with a CoreServer component, you must define the file servers to which the gateway will be connected. These parameters are typically defined in the Setup Wizard during deployment, as described in *Chapter 3, Installation and Deployment*, but may be modified here.

The CoreServer component includes the following options:

- ▶ **Configuration:** Enables you to select the file servers to which the CoreServer will connect. It also enables you to define notification settings for the CoreServer component. For more information, refer to *Configuration Option*, below.
- ▶ **Monitoring:** Enables you to view CoreServer statistics in tables and graphs, as described in *Monitoring the Gateway*, page 4-49.
- ▶ **Logs:** Enables you to view the event log related to the CoreServer component. For more information, refer to *Viewing Gateway Logs*, page 4-63.

## Configuration Option

The **Configuration** option for the CoreServer component displays the following tabs:

- ▶ **NFS Servers:** Enables you to define the NFS file servers to which the CoreServer will connect. For more information, refer to *Selecting NFS Servers*, page 4-28.
- ▶ **CIFS Servers:** Enables you to define the CIFS file servers to which the CoreServer will connect. For more information, refer to *Selecting CIFS Servers*, page 4-30.

- ▶ **Notifier:** Enables you to define the email address to which notifications are sent when alerts are generated by the CoreServer component. For more information, refer to *Defining Notification Settings*, page 4-23.

## Selecting NFS Servers

You can modify the list of NFS servers to which the CoreServer gateway will connect.

### ▶ To select NFS servers:

- 1 In the *CoreServer Configuration* page, click the **NFS Servers** tab to display the following:



CoreServer > Configuration

NFS Servers | CIFS Servers | Notifier

File server access UID:  (Used in browsing)

File server access GID:

List of NFS servers:

Server Name	Using TCP	Using UDP
Empty list		

**Figure 4-16: CoreServer – NFS Servers Tab**

- 2 In the **File server access UID** field, enter the user ID the CoreServer will use for browsing NFS file servers. This user ID is used for all NFS servers connected to this CoreServer.

- 3 In the **File server access GID** field, enter the group ID the CoreServer will use for browsing NFS file servers. This group ID is used for all NFS servers connected to this CoreServer.

**NOTE:**



The UID and GID are used for browsing during policy definition in the Central Manager.

- 4 In the **List of NFS servers** field, click **Add** to display the following:



**Figure 4-17: New NFS File Server Window**

- 5 Define the new file server, as follows:
  - In the **Server Name** field, enter the name of the file server.
  - Select the checkboxes for the appropriate connections used by the file server, **Using TCP** or **Using UDP**. At least one option must be selected.
  - Click **Ok**. The file server is added to the list in the **NFS Servers** tab.
- 6 Repeat steps 4 and 5 to add more NFS file servers, if required.
- 7 Click **Save**.

## Deleting NFS Servers

You can delete an NFS file server from the list of servers to which the CoreServer is connected at any time, as described below.

➤ **To delete an NFS file server:**

Select the file server from the list displayed in the **NFS Servers** tab and then click **Delete**.

## Selecting CIFS Servers

You can modify the list of CIFS servers to which the CoreServer gateway will connect.

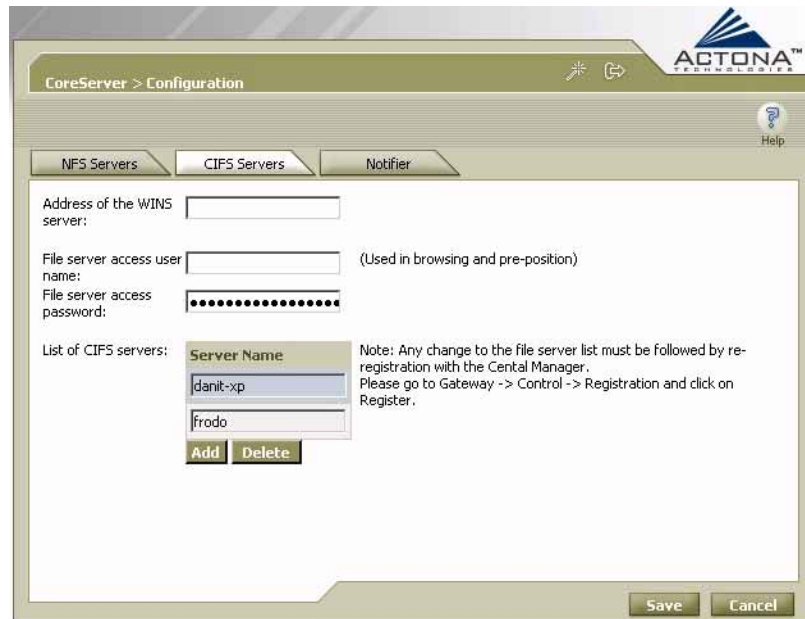
**NOTE:**



The gateway must be re-registered with the Central Manager after making changes to the server list. Refer to *Registering the Gateway*, page 4-12.

➤ **To select CIFS servers:**

- 1 In the *CoreServer Configuration* page, click the **CIFS Servers** tab to display the following:



CoreServer > Configuration

NFS Servers | **CIFS Servers** | Notifier

Address of the WINS server:

File server access user name:  (Used in browsing and pre-position)

File server access password:

List of CIFS servers:

Server Name
danit-xp
frodo

Add Delete

Note: Any change to the file server list must be followed by re-registration with the Central Manager. Please go to Gateway -> Control -> Registration and click on Register.

Save Cancel

**Figure 4-18: CoreServer – CIFS Servers Tab**

- 2 In the **Address of the WINS server** field, enter the name or IP address of the WINS server, if any.
- 3 In the **File server access user name** field, enter the user name the CoreServer will use for browsing CIFS file servers. This user name is used for all CIFS servers connected to this CoreServer. The format of the user name is: **[domain]\<user name>**. (Enter the domain if this is not a local user.)

- 4 In the **File server access password** field, enter the password the CoreServer will use for browsing CIFS file servers. This password is used for all CIFS servers connected to this CoreServer.

**NOTE:**

The user name and password are required for browsing during policy definition in the Central Manager and for executing pre-position policies in the EdgeServer.

- 5 In the **List of CIFS servers** field, click **Add** to display the following:



**Figure 4-19: New CIFS File Server Window**

- 6 Define the new file server, as follows:
  - In the **Server Name** field, enter the name of the file server.
  - Click **Ok**. The file server is added to the list in the **CIFS Servers** tab.
- 7 Repeat steps 5 and 6 to add more CIFS file servers, if required.
- 8 Click **Save**.

- 9 Re-register the gateway with the Central Manager, as described in *Registering the Gateway*, page 4-12.

## Deleting CIFS Servers

You can delete a CIFS file server from the list of servers to which the CoreServer is connected at any time, as described below.

### ➤ To delete a CIFS file server:

- 1 Select the file server from the list displayed in the **CIFS Servers** tab and then click **Delete**.
- 2 Re-register the gateway with the Central Manager, as described in *Registering the Gateway*, page 4-12.



# Managing the EdgeServer Component

The **EdgeServer** option in the navigation area enables you to modify selected EdgeServer settings defined in the Setup Wizard. In addition, you can set the maximum age for information stored in the cache and define a specific recipient for notifications generated by the EdgeServer component of the gateway.

The EdgeServer component includes the following options:

- **Configuration:** Enables you to configure the EdgeServer component. For more information, refer to *Configuration Option*, below.
- **Policies:** Enables you to monitor the progress of pre-position policies created in the Central Manager. In addition, you can optionally terminate policy tasks, if required. For more information, refer to *Policies Option*, page 4-39.
- **Monitoring:** Enables you to view EdgeServer statistics in tables and graphs, as described in *Monitoring the Gateway*, page 4-49.
- **Logs:** Enables you to view the event log related to the EdgeServer component. For more information, refer to *Viewing Gateway Logs*, page 4-63.

## Configuration Option

The **Configuration** option for the EdgeServer component displays the following tabs:

- **General:** Enables you to set the default coherency age of the EdgeServer and to view data about cache size and usage. For more information, refer to *Setting the Default Coherency Age*, page 4-35.

- ▶ **Connectivity:** Enables you to view read-only information about the CoreServers to which the EdgeServer is connected. For more information, refer to *Viewing CoreServer Connections*, page 4-37.
- ▶ **CIFS:** Enables you to define the name registration parameters required by the EdgeServer to connect to the Windows environment correctly. For more information, refer to *Modifying CIFS Settings*, page 4-38.
- ▶ **Notifier:** Enables you to define the email address to which notifications are sent when alerts are generated by the EdgeServer component. For more information on email notifications, refer to *Defining Notification Settings*, page 4-23.

## Setting the Default Coherency Age

The Central Manager is used to define the coherency policies used by each EdgeServer, as described in *Chapter 5, Central Management*. However, an additional coherency parameter is defined for each EdgeServer with the Gateway Manager – default coherency age. This parameter defines the maximum age of the information stored in the EdgeServer cache. (ActaStor uses age-based coherency for NFS files, as well as for CIFS/NFS files and directories.)

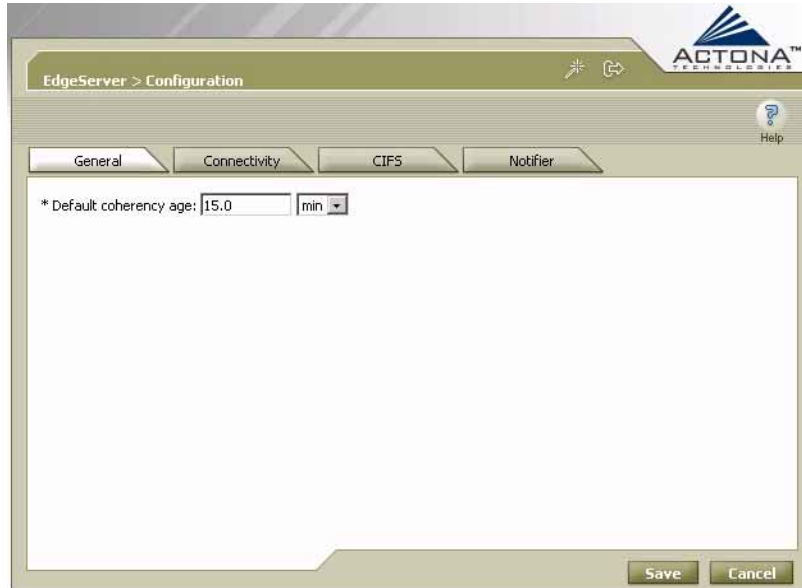
After a file has resided in the cache for longer than this interval, the EdgeServer will verify whether the file has been updated before responding to read requests from users.

### NOTE:

For more information about coherency, refer to *Chapter 2, Getting Started*.

➤ **To set the default coherency age:**

- 1 In the *EdgeServer Configuration* page, click the **General** tab to display the following:



EdgeServer > Configuration

ACTONA™  
TECHNOLOGIES

Help

General Connectivity CIFS Notifier

\* Default coherency age: 15.0 min

Save Cancel

**Figure 4-20: EdgeServer – General Tab**

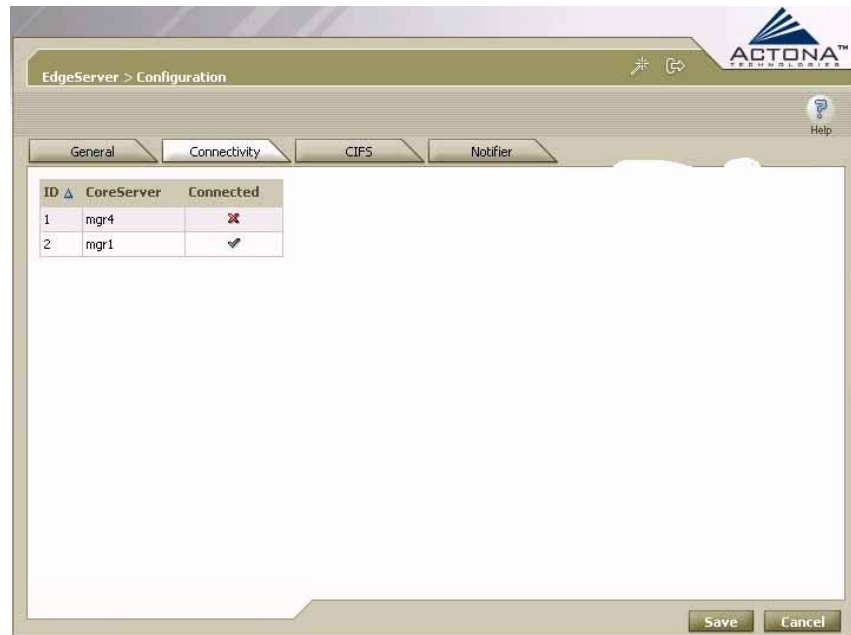
- 2 In the **Default coherency age** field, enter the time interval for age-based validation. (Select the time unit from the dropdown list.)
- 3 Click **Save**.

## Viewing CoreServer Connections

The **Connectivity** tab enables you to view read-only information about the CoreServer connections for this EdgeServer, as defined in the Central Manager.

➤ **To view CoreServer connections:**

In the *EdgeServer Configuration* page, click the **Connectivity** tab to display the following:



**Figure 4-21: EdgeServer – CoreServers Tab**

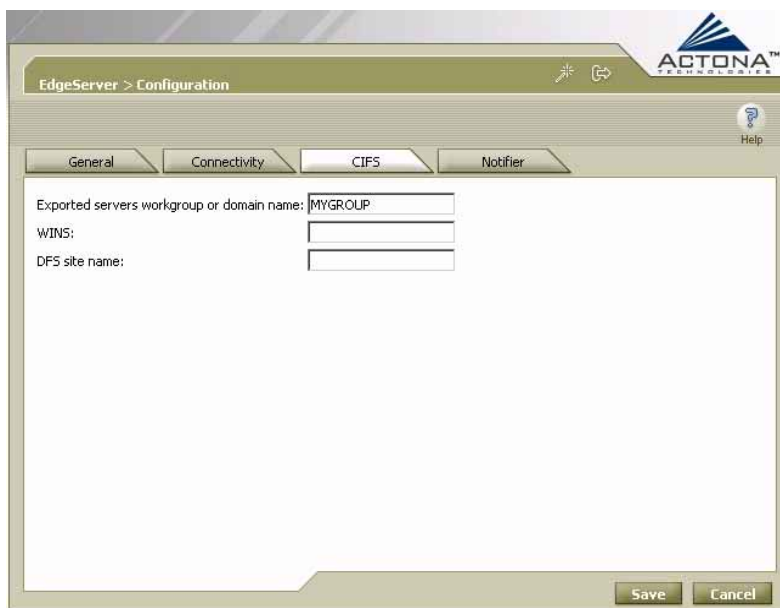
The **Connectivity** tab contains a table listing each CoreServer related to the selected EdgeServer and its current connection status.

## Modifying CIFS Settings

The **CIFS** tab enables you to modify parameters defined in the Setup Wizard regarding the Windows environment to which the EdgeServer is connected, including the name of the Windows workgroup to which the gateway will belong, the name or IP address of the WINS server, as well as the default prefix for all file servers accessed through this gateway.

➤ **To modify CIFS settings:**

- 1 In the *EdgeServer Configuration* page, click the **CIFS** tab to display the following:



The screenshot shows the EdgeServer Configuration page with the CIFS tab selected. The page has a header with the Actona logo and the text "EdgeServer > Configuration". Below the header are four tabs: "General", "Connectivity", "CIFS", and "Notifier". The "CIFS" tab is active. The main content area contains three input fields: "Exported servers workgroup or domain name:" with the value "MYGROUP", "WINS:", and "DFS site name:". At the bottom right of the form are "Save" and "Cancel" buttons.

**Figure 4-22: EdgeServer – CIFS Tab**

- 2 In the **Exported servers workgroup or domain name** field, enter the name of the Windows workgroup or domain to which the EdgeServer will belong. When end users connect to the EdgeServer to view information on the file servers, these servers will appear to the users as members of this workgroup.
- 3 In the **WINS** field, enter the name or IP address of the WINS server on the LAN, if any.
- 4 [If DFS is being used] In the **DFS site name** field, enter the name of the site where the EdgeServer is located. This site name, which is typically found in the Active Directory database, is used in DFS target selection.

**NOTE:**



For more information about how ActaStor interacts with DFS, refer to *Chapter 2, Getting Started*.

- 5 Click **Save**.

## Policies Option

The **Policies** option for the EdgeServer component enables you to view the details and current status of pre-position policies created in the Central Manager. These policies define which files are proactively placed in the EdgeServer cache according to a pre-arranged schedule. Pre-positioning enables system administrators to strategically place large, frequently accessed files at the network edge during off-peak hours, increasing efficiency and providing end users with quick first-time access of those files.

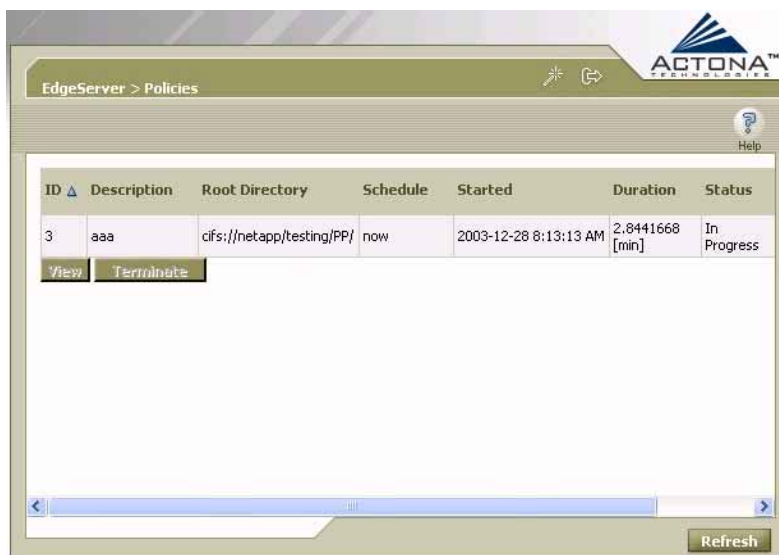
You can view information such as the root directory containing the files being pre-positioned, the schedule for each policy and the status of the most recent task for each policy. You can also view a detailed task history for each policy, and manually terminate any tasks in progress, if required.

**NOTE:**

For more information about pre-position policies, refer to *Defining Pre-position Policies* in *Chapter 5, Central Management*.

**➤ To view pre-position policies for this gateway:**

- 1 In the navigation area, click **Policies** to display the following:



The screenshot shows the EdgeServer web interface. The breadcrumb navigation is 'EdgeServer > Policies'. The ACTONA logo is in the top right corner. A 'Help' icon is also present. The main content area contains a table with the following data:

ID ▲	Description	Root Directory	Schedule	Started	Duration	Status
3	aaa	cifs://netapp/testing/PP/	now	2003-12-28 8:13:13 AM	2.8441668 [min]	In Progress

Below the table, there are two buttons: 'View' and 'Terminate'. At the bottom right of the interface is a 'Refresh' button.

**Figure 4-23: EdgeServer – Policies**

The *Policies* page contains a table displaying all the pre-position policies assigned to this EdgeServer. For each policy, the following information is displayed:

- **ID:** The ID number of the selected policy.
- **Description:** The descriptive name assigned to the policy.
- **Root Directory:** The source directory for the content being pre-positioned.
- **Schedule:** The defined schedule for the policy.
- **Started:** When this policy was last invoked by the system.
- **Duration:** The elapsed time of the latest task.
- **Status:** The current status of the policy, updated every 60 seconds. If the task defined by the policy is currently being run, its status is **In Progress**. A pre-position task in progress can be terminated, as described on page 4-43.

- 2 To view a detailed task history (that is, iterations of a selected policy), select a policy in the table and click **View** to display the following popup window:

Preposition Policy 3 - aaa

Create Date: 2003-12-28 7:42:36 AM    Status: enabled  
 Last Modified: 2003-12-28 8:12:02 AM  
 Root Dir: cifs://netapp/testing/PP/  
           [Include sub directories]  
 Schedule: now  
 Total size:                                  Duration:  
 Min file size: 20.0 KB                      Perform on: Files changed since last preposition  
 Max file size:

Started <span style="font-size: small;">▲</span>	Duration	Total data	# matching files	Amount copied	# files copied	Throughput [KB/sec]	Status	Termination reason
2003-12-28 8:13:13 AM	3.1678834 [min]	2.112595 [GB]	2640	149.1206 [MB]	6	822.6539	In Progress	

Close

**Figure 4-24: Pre-position Task Details**



The upper half of the *Pre-position Policy* window displays the following additional details about the selected policy:

- **Create Date:** When the policy was created.
- **Last Modified:** When the policy was last modified.
- **Total size:** The limit placed on the total size of the files being pre-positioned, if any.
- **Min file size:** The minimum size of files in the root directory that are affected by the policy.
- **Max file size:** The maximum size of files in the root directory that are affected by the policy.
- **Perform on:** Which files to pre-position from the selected location – those that have changed since last pre-position, those changed during a defined interval, or all files.

The lower half of the *Pre-position Policy* window contains a table displaying the most recent tasks performed by the selected policy (up to the last 10 iterations), including the following information:

- **Total data:** The total amount of data to be transferred by the policy.
- **# matching files:** The number of files matching the defined filter of the policy.
- **Amount copied:** The total amount of data copied by the policy during its most recent run. (This amount may be less than the amount in the **Total data** field if the policy is currently in progress, or if the policy did not complete its run, for example, due to time constraints placed on its operation.)
- **# files copied:** The number of files copied by the policy during its most recent run.

- **Throughput:** The throughput achieved by the policy in KB/sec.
- **Termination reason:** The reason the policy was terminated, if relevant. Policies can be terminated due to time or space constraints placed on the policy, or to a decision by the administrator to manually terminate its operation.

3 Click **Close** to return to the *Policies* page.

**NOTE:**



To update the information displayed in the *Policies* page, click **Refresh**.

## Terminating a Pre-position Task

You can terminate a pre-position task that is in progress at any time. This action does not delete the pre-position policy that generated the task; the system will still perform the task described by the policy when the next scheduled time arrives.

### ➤ To terminate a pre-position task:

- 1 In the *Policies* page, select a pre-position policy with a status of **In Progress** and click **Terminate**. A confirmation message is displayed.
- 2 Click **Yes** to terminate the task. If **View** is clicked to display the *Pre-position Policy* window, the table displaying the task history contains a message indicating that the latest task was terminated by the administrator.

# Managing the Replication Component

The **Replication** option in the navigation area enables you to view the details and current status of replication policies that define this gateway as the replication target. For example, you can see the status of those policies that physically copy files from a source site to this gateway in order to back up data locally.

You can view information such as the source gateway for the data being replicated to this gateway, the schedule for each policy and the status of the most recent task for each policy. You can also view a detailed task history for each policy, and manually terminate any tasks in progress, if required.

## NOTES:

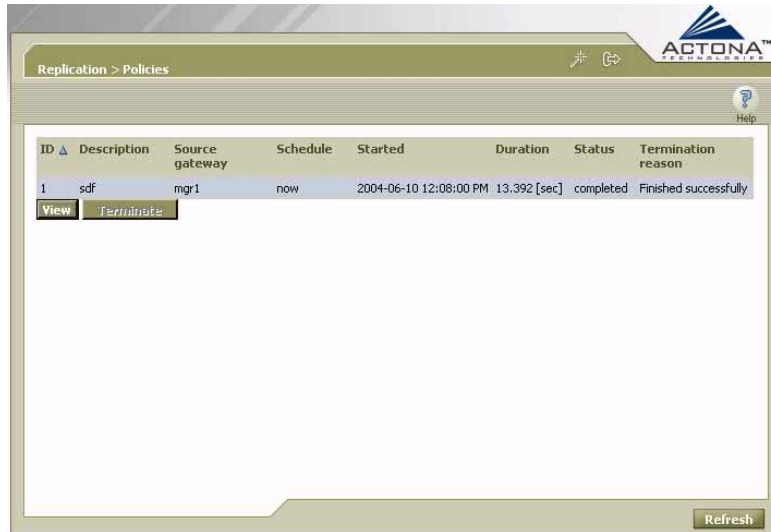


To view replication policies that have this gateway defined as the source, you must open the Gateway Manager for the defined target gateway.

Replication policies are defined in the Central Manager, as described in *Defining Replication Policies* in *Chapter 5, Central Management*.

➤ **To view replication policies that define this gateway as the target:**

- 1 In the **Replication** component of the navigation area, click **Policies** to display the following:



ID	Description	Source gateway	Schedule	Started	Duration	Status	Termination reason
1	sdf	mgr1	now	2004-06-10 12:08:00 PM	13.392 [sec]	completed	Finished successfully

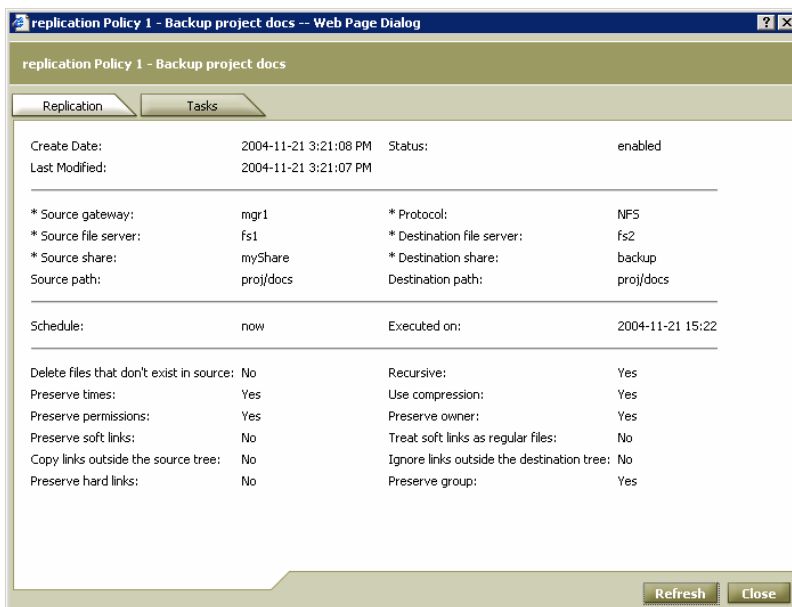
Buttons: View, Terminate, Refresh

**Figure 4-25: Replication Policies**

The *Policies* page contains a table displaying all the replication policies that define this gateway as the replication target. For each policy, the following information is displayed:

- **ID:** The ID number of the selected policy.
- **Description:** The descriptive name assigned to the policy.
- **Source gateway:** The gateway providing the files to be replicated.
- **Schedule:** The defined schedule for the policy.
- **Started:** When this policy was last invoked by the system.
- **Duration:** The elapsed time of the latest task.

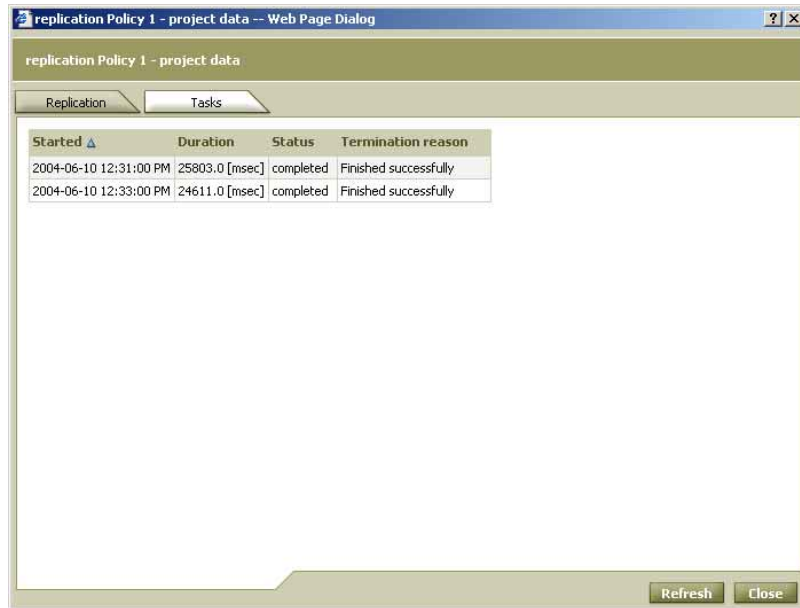
- **Status:** The current status of the policy, updated every 60 seconds. If the task defined by the policy is currently being run, its status is **In Progress**. A replication task in progress can be terminated, as described on page 4-48.
- 2 To view the policy configuration, select a policy in the table and click **View** to display the *Replication Policy* window.



**Figure 4-26: Replication Task Details**

The **Replication** tab displays complete configuration information for the selected policy. For more information about these parameters, refer to *Defining Replication Policies* in *Chapter 5, Central Management*.

- 3 To view a detailed task history (that is, iterations of the selected policy), click the **Tasks** tab to display the following:



Started	Duration	Status	Termination reason
2004-06-10 12:31:00 PM	25803.0 [msec]	completed	Finished successfully
2004-06-10 12:33:00 PM	24611.0 [msec]	completed	Finished successfully

**Figure 4-27: Replication Task History**

The **Tasks** tab contains a table displaying the most recent tasks performed by the selected policy (up to the last 10 iterations), including the following information:

- **Started:** The start time of each task.
- **Duration:** The duration of the task.
- **Status:** The current status of the task (updated by clicking **Refresh**).
- **Termination reason:** The reason the policy was terminated, if relevant. Tasks can be terminated manually (as described in *Terminating a Replication Task*, page 4-48) or due to an error.

- 4 Click **Close** to return to the *Replication* page.

**NOTE:**

To update the information displayed in the *Replication Policy* window, click **Refresh**.

## Terminating a Replication Task

You can terminate a replication task that is in progress at any time. This action does not delete the replication policy that generated the task; the system will still perform the task described by the policy when the next scheduled time arrives.

➤ **To terminate a replication task:**

- 1 In the *Replication* page, select a replication policy with a status of **In Progress** and click **Terminate**. A confirmation message is displayed.
- 2 Click **Yes** to terminate the task. The status of the task changes to **terminated by admin**.

# Monitoring the Gateway

The **Monitoring** option located in each gateway component enables you to view detailed tables describing the current state of the gateway. It also provides graphs that display a wide range of historical data about selected components. This information enables you to track gateway statistics over the course of a day, several weeks, several months, or even an entire year.

 **NOTE:**

Gateway statistics and graphs are generated by the freeware MRTG utility. For details, browse to <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>.

The monitoring options differ for each gateway component, as follows:

- **Gateway:** Enables you to monitor CPU and disk utilization, as described in *Monitoring the Gateway Component*, page 4-52.
- **CoreServer:** Enables you to monitor connectivity statistics, count EdgeServer connections and measure total traffic, as described in *Monitoring the CoreServer Component*, page 4-53.
- **EdgeServer:** Enables you to monitor connectivity and cache statistics, count CoreServer connections and measure various aspects of EdgeServer traffic, as described in *Monitoring the EdgeServer Component*, page 4-56.



## Viewing Monitoring Graphs

ActaStor provides the following four monitoring graphs for each available graph type:

- ▲ Daily (5-minute average)
- ▲ Weekly (30-minute average)
- ▲ Monthly (2-hour average)
- ▲ Yearly (1-day average)

When displaying graphs, you have the option of viewing all four graphs of a particular type (for example, connected sessions) at once, or viewing an index page of daily graphs for all graph types available for that component.

A sample set of graphs for a selected type is shown below.

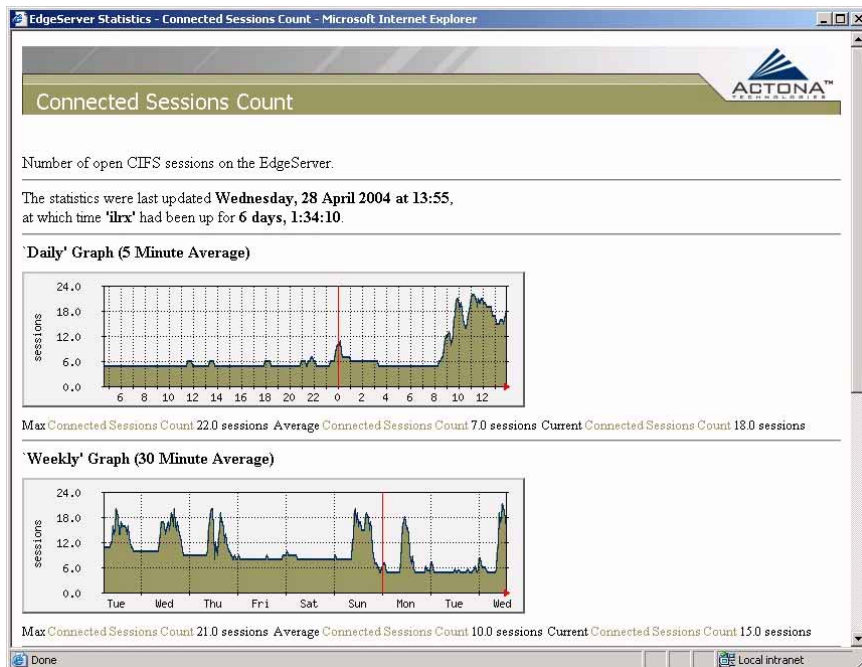
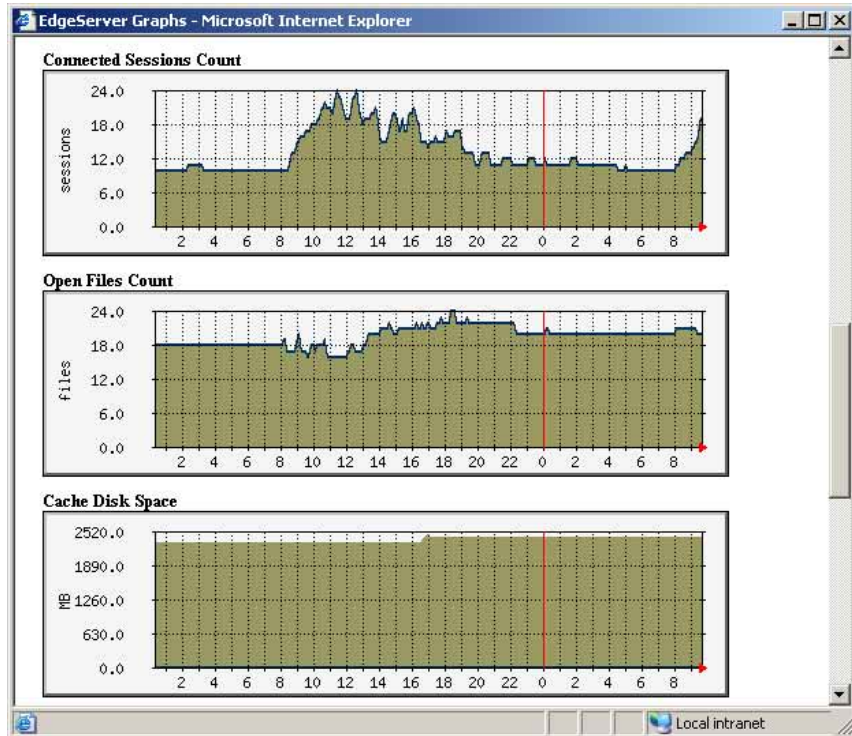


Figure 4-28: Sample Graph Window

A sample set of index graphs for the selected component is shown below.



**Figure 4-29: Sample Index Graph Window**

Each daily graph displayed in an index window acts as a link. Clicking the graph displays all four graphs of the selected type. For example, clicking the Open Files Count graph in the EdgeServer graphs index window displays the daily, weekly, monthly and yearly Open Files Count graphs. Clicking the **Back** button in the browser returns you to the index graphs.

**NOTE:**



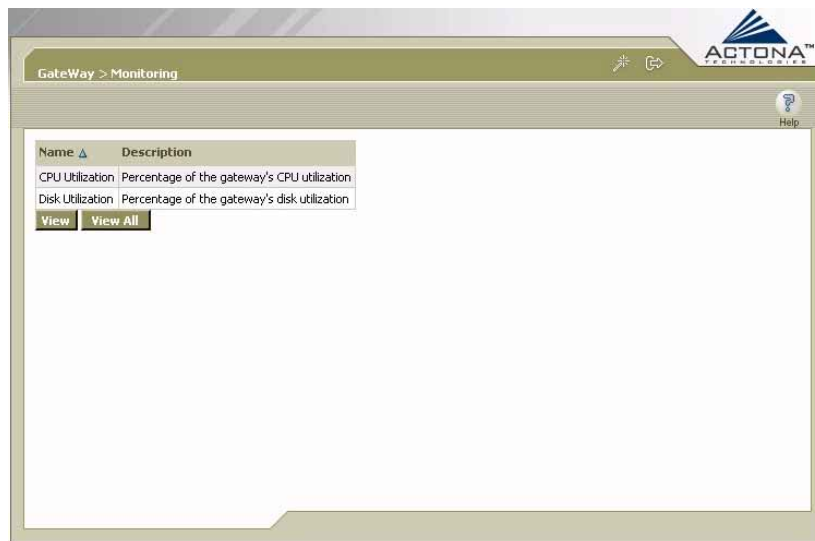
Graphs can be printed using the Print command in your browser.

## Monitoring the Gateway Component

The **Monitoring** option for the Gateway component enables you to display graphs that indicate the CPU utilization and disk utilization of the gateway.

➤ **To monitor the Gateway component:**

- 1 In the navigation area, click **Monitoring** under the Gateway component to display the following:



**Figure 4-30: Gateway Component Monitoring Page**

The following graphs are available for the Gateway component:

- **CPU Utilization:** The CPU utilization percentage in the gateway.
- **Disk Utilization:** The disk utilization percentage in the gateway.

- 2 Do one of the following:
  - Select a graph in the table and then click **View** to display a popup window with all four graphs of the selected type (daily, weekly, monthly, yearly).
  - Click **View All** to display the index window with the daily graphs for the gateway component.

**NOTE:**



For more information, refer to *Viewing Monitoring Graphs*, page 4-50.

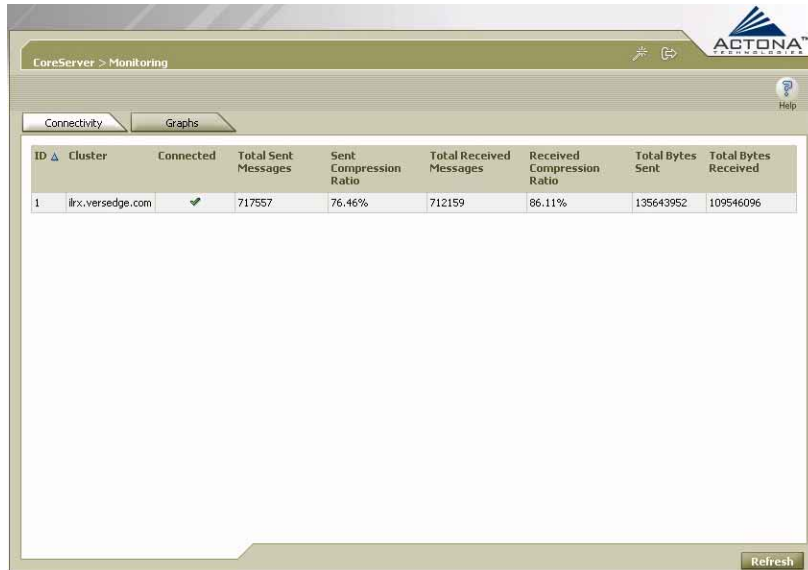
## Monitoring the CoreServer Component

The **Monitoring** option for the CoreServer component contains the following two tabs:

- ▀ **Connectivity:** Displays a table of connectivity statistics for the CoreServer component.
- ▀ **Graphs:** Displays a list of graphs that are available for the CoreServer component.

➤ **To monitor the CoreServer component:**

- 1 In the navigation area, click **Monitoring** under the CoreServer component to display the following:



ID	Cluster	Connected	Total Sent Messages	Sent Compression Ratio	Total Received Messages	Received Compression Ratio	Total Bytes Sent	Total Bytes Received
1	ilrx.versedge.com	✔	717557	76.46%	712159	86.11%	135643952	109546096

**Figure 4-31: CoreServer Monitoring – Connectivity Tab**

The table in the **Connectivity** tab displays the following data about the CoreServer component:

- **Cluster:** Name of the CoreServer cluster to which this CoreServer belongs, if any.
- **Connected:** Whether the CoreServer is currently connected ✔ or disconnected ✘ from its EdgeServers.
- **Total Sent Messages:** Total number of messages sent from this CoreServer since activation.
- **Sent Compression Ratio:** Compression ratio of messages sent from this CoreServer to each of the EdgeServers connected to it. Compression is used to reduce the amount of WAN bandwidth required by the gateway.

- **Total Received Messages:** Total number of messages received by this CoreServer since activation.
- **Received Compression Ratio:** Compression ratio of messages received by this CoreServer from each of the EdgeServers connected to it.
- **Total Bytes Sent:** Total number of bytes sent from this CoreServer since activation.
- **Total Bytes Received:** Total number of bytes received from this CoreServer since activation.

2 Click the **Graphs** tab to display the following:



**Figure 4-32: CoreServer Monitoring – Graphs Tab**

The following historical graphs are available for the CoreServer component:

- **Connected EdgeServers counts:** The number of EdgeServers currently connected to the selected CoreServer. This graph is useful for detecting EdgeServers disconnections.


- **CoreServer traffic:** The total volume of traffic (in KB) between the CoreServer and each of the EdgeServers connected to it. The green line represents transmitted traffic; the blue line represents received traffic.
- 3** Do one of the following:
- Select a graph in the table and then click **View** to display a popup window with all four graphs of the selected type (daily, weekly, monthly, yearly).
  - Click **View All** to display the index window with the daily graphs for the CoreServer component.

**NOTE:** For more information, refer to *Viewing Monitoring Graphs*, page 4-50.

## Monitoring the EdgeServer Component

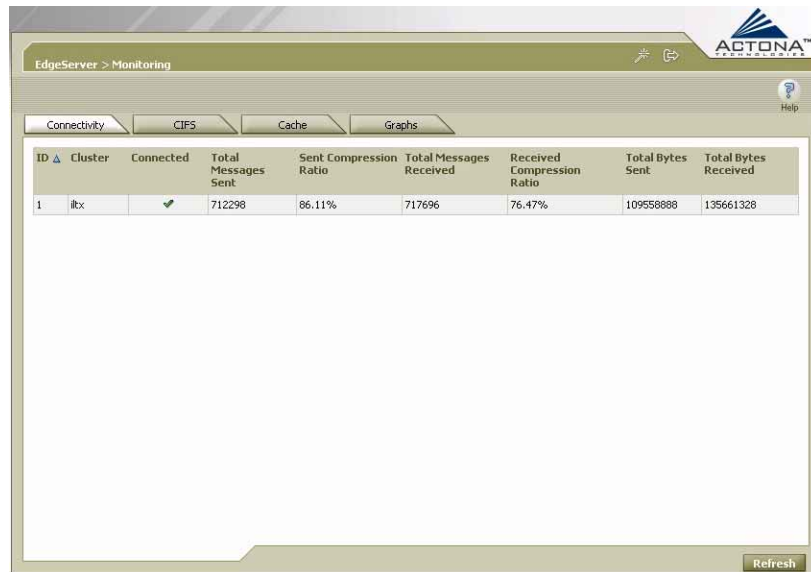
The **Monitoring** option for the EdgeServer component contains the following four tabs:

- ▀ **Connectivity:** Displays a table of connectivity statistics for the EdgeServer component.
- ▀ **CIFS:** Displays data regarding the status of the CIFS protocol and the selected EdgeServer.
- ▀ **Cache:** Displays data related to the EdgeServer cache.
- ▀ **Graphs:** Displays a list of graphs that are available for the EdgeServer component.

**NOTE:** The SNMP parameters displayed in the CIFS and Cache tabs are contained in a special MIB file. For more information, refer to *SNMP Support* in *Chapter 2, Getting Started*.

➤ **To monitor the EdgeServer component:**

- 1 In the navigation area, click **Monitoring** under the EdgeServer component to display the following:



ID	Cluster	Connected	Total Messages Sent	Sent Compression Ratio	Total Messages Received	Received Compression Ratio	Total Bytes Sent	Total Bytes Received
1	iltx	✔	712298	86.11%	717696	76.47%	109558888	135661328

**Figure 4-33: EdgeServer Monitoring – Connectivity Tab**

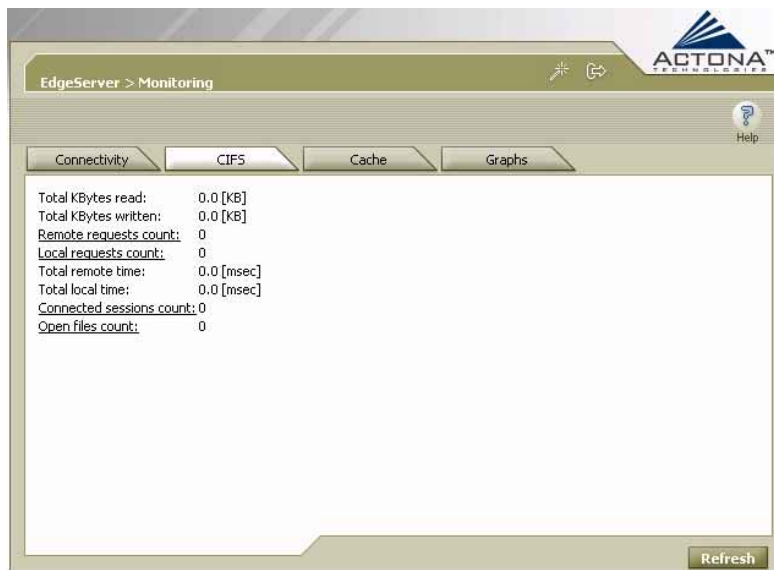
The table in the **Connectivity** tab displays the following data about the EdgeServer component:

- **Cluster:** Name of the CoreServer cluster to which this EdgeServer is connected, if any.
- **Connected:** Whether the EdgeServer is currently connected ✔ or disconnected ✘ from the CoreServer.
- **Total Sent Messages:** Total number of messages sent from this EdgeServer since activation.
- **Sent Compression Ratio:** Compression ratio of messages sent from this EdgeServer. Compression is used to reduce the amount of WAN bandwidth required by the gateway.
- **Total Received Messages:** Total number of messages received by this EdgeServer since activation.



- **Received Compression Ratio:** Compression ratio of messages received by this EdgeServer.
- **Total Bytes Sent:** Total number of bytes sent from this EdgeServer since activation.
- **Total Bytes Received:** Total number of bytes received by this EdgeServer since activation.

2 Click the **CIFS** tab to display the following:



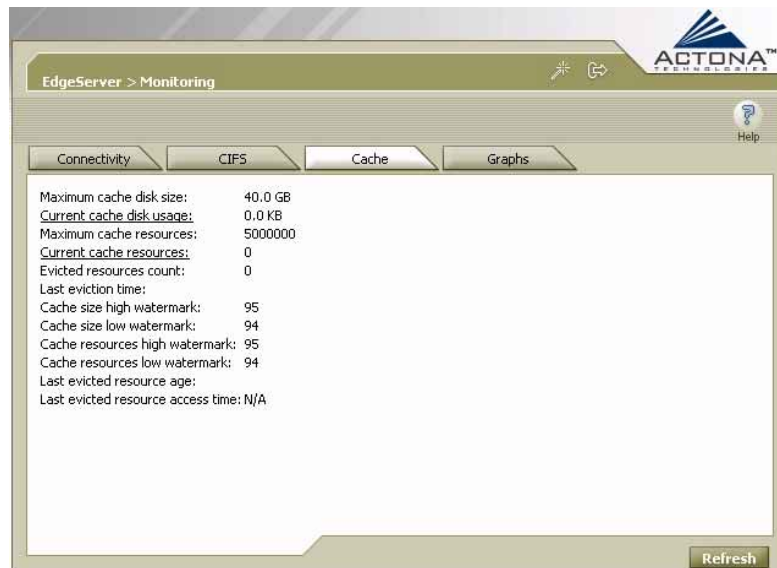
**Figure 4-34: EdgeServer Monitoring – CIFS Tab**

The **CIFS** tab displays the following CIFS-related information:

- **Total KBytes read:** The total number of kilobytes read by clients (both via the cache and remotely) from this EdgeServer using the CIFS protocol.
- **Total KBytes written:** The total number of kilobytes written by clients to this EdgeServer using the CIFS protocol.
- **Remote requests count:** Click the link to display a graph indicating the total number of client CIFS requests that were forwarded remotely over the WAN to the CoreServer.

- **Local requests count:** Click the link to display a graph indicating the total number of client CIFS requests handled locally by this EdgeServer.
- **Total remote time:** The total duration of all client CIFS requests sent remotely to the CoreServer from this EdgeServer.
- **Total local time:** The total duration of all client CIFS requests handled locally by this EdgeServer.
- **Connected sessions count:** Click the link to display a graph indicating the total number of connected CIFS sessions on this EdgeServer.
- **Open files count:** Click the link to display a graph indicating the total number of open CIFS files on this EdgeServer.

**3** Click the **Cache** tab to display the following:

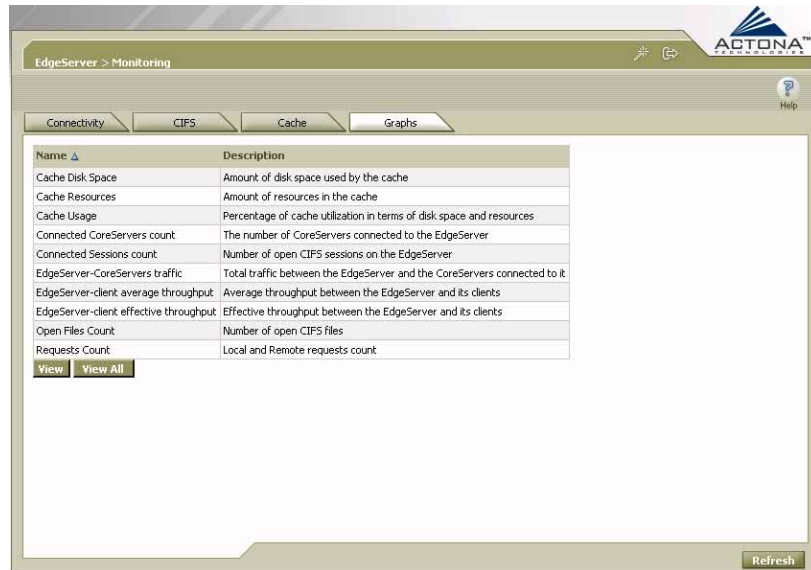


**Figure 4-35: EdgeServer Monitoring – Cache Tab**

The **Cache** tab displays the following information:

- **Maximum cache disk size:** The maximum amount of disk space allocated to the EdgeServer cache.
- **Current cache disk usage:** Click the link to display a graph indicating the amount of space used by the EdgeServer cache.
- **Maximum cache resources:** The maximum number of resources (files and directories) allowed in the EdgeServer cache.
- **Current cache resources:** Click the link to display a graph indicating the number of resources contained in the EdgeServer cache.
- **Evicted resources count:** The number of resources that have been evicted from the cache since the EdgeServer was started.
- **Last eviction time:** The time when cache eviction last occurred.
- **Cache size high watermark:** The disk usage percentage that causes the EdgeServer to begin evicting resources.
- **Cache size low watermark:** The disk usage percentage that causes the EdgeServer to stop evicting resources.
- **Cache resources high watermark:** The percentage of total cache resources that causes the EdgeServer to begin evicting resources.
- **Cache resources low watermark:** The percentage of total cache resources that causes the EdgeServer to stop evicting resources.
- **Last evicted resource age:** The amount of time spent in the EdgeServer cache by the last-evicted resource.
- **Last evicted resource access time:** The last access time of the last-evicted resource.

4 Click the **Graphs** tab to display the following:



**Figure 4-36: EdgeServer Monitoring – Graphs Tab**

The following historical graphs are available for the EdgeServer component:

- **Cache Disk Space:** The amount of disk space used by the EdgeServer cache.
- **Cache Hit Rate:** The percentage of user requests answered by the cache (as opposed to forwarding the request remotely over the WAN to the file server).
- **Cache Resources:** The total number of cache resources (files and directories) consumed by the cache.
- **Cache Usage:** The percentage of disk space and of resources used by the cache, based on defined limits.

- **Connected CoreServers count:** The number of CoreServers connected to the selected EdgeServer.

**NOTE:**

The EdgeServer could be connected to multiple CoreServers to provide for high availability. For more information, refer to *Clustering and Failover in Chapter 2, Getting Started*.

- **Connected Sessions count:** The number of open CIFS sessions on the selected EdgeServer.
  - **EdgeServer-CoreServers traffic:** The total volume of traffic (in KB) between the EdgeServer and each of the CoreServers connected to it. The green line represents transmitted traffic; the blue line represents received traffic.
  - **EdgeServer-client average throughput:** The total volume of traffic between the EdgeServer and the clients it serves, divided by total uptime (including idle time).
  - **EdgeServer-client effective throughput:** The total volume of traffic between the EdgeServer and the clients it serves, divided by total uptime, excluding idle time.
  - **Open Files Count:** The total number of open CIFS files.
  - **Requests Count:** The number of local requests (client requests answered via the EdgeServer cache) and the number of remote requests (client requests answered via the remote file server), in requests per second.
- 5 Do one of the following:
- Select a graph in the table and then click **View** to display a popup window with all four graphs of the selected type (daily, weekly, monthly, yearly).
  - Click **View All** to display the index window with the daily graphs for the EdgeServer component.

**NOTE:**

For more information, refer to *Viewing Monitoring Graphs*, page 4-50.

# Viewing Gateway Logs

Each gateway component maintains one or more logs containing a description of the events that have taken place in that component, as follows:

- ▲ **Gateway:** Contains tabs for the following three logs:
  - **Manager:** Displays events related to the Gateway Manager and Central Manager components, such as configuration changes, gateway registrations and notifications that other gateway components were started or stopped.
  - **Watchdog:** Displays events related to the watchdog utility, which monitors the other application files inside the gateway and restarts them, if necessary.
  - **Utilities:** Displays events related to the Cache Removal utility.
- ▲ **CoreServer:** Displays events related to the CoreServer component.
- ▲ **EdgeServer:** Displays events related to the EdgeServer component.

Each log entry contains the date and time, the severity level of the event and a description containing the log message. The severity levels are as follows:

- ▲ **Info:** Information regarding the proper functioning of the component.
- ▲ **Warning:** Indicates a minor problem that the component was able to overcome without user intervention.
- ▲ **Error:** Indicates a problem in the functioning of the component.
- ▲ **Fatal:** Indicates a severe problem in the component that may have caused it to stop functioning.

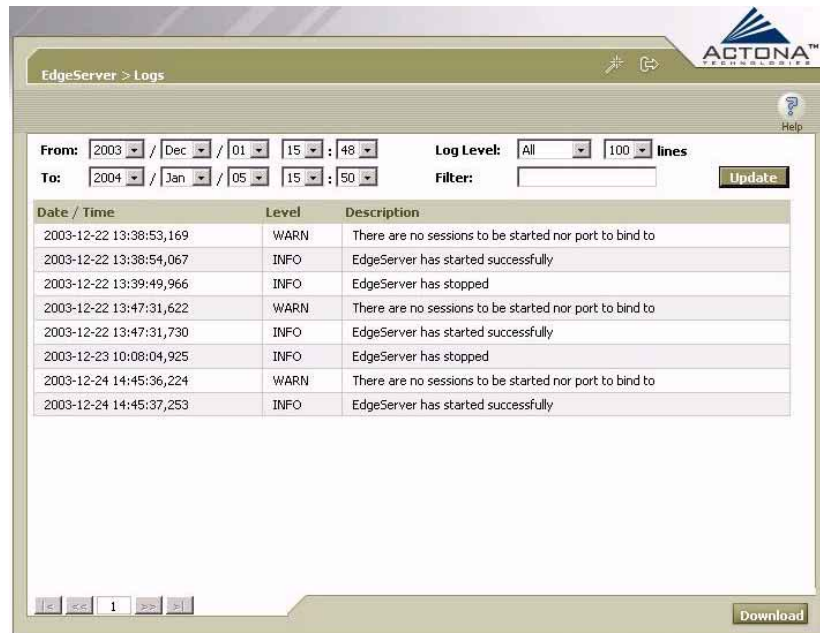
You can set the criteria by which the log is viewed using the following options:

- **Date:** Enables you to specify the date range of the log (year, month and date).
- **Time:** Enables you to specify the time period of the log (hour and minutes using a 24-hour clock format).
- **Log Level:** Enables you to select the minimum severity level of events to display.
- **Lines:** Enables you to set the number of (event) lines that appear on a single page of the log.
- **Filter:** Enables you to enter free text by which the log can be further filtered.

You can also save a log as a text file and download it to your local drive.

➤ **To view gateway logs:**

- 1 In the navigation area, click the **Logs** option of any component. The *Logs* page for that component will be displayed, as in the following example:




**Figure 4-37: Gateway Component Logs Page**

- 2 In the **From** and **To** fields, enter the date ranges and time periods for viewing the log.
- 3 From the **Log Level** dropdown list, select the minimum severity level of events to include in the log:
  - All
  - Info
  - Warning
  - Error
  - Fatal



- 4 From the **lines** dropdown list, select the number of (event) lines you want to appear on a single page of the log:
  - **100**
  - **200**
  - **300**
  - **400**
- 5 [Optional] If you want to filter the log so that only events containing specific words or phrases will be displayed, enter the relevant free text in the **Filter** text box.
- 6 Click **Update**. The *Logs* page is refreshed according to your selected criteria.
- 7 Click **Download** to save the displayed log entries as a text file and download it to your local drive.

**NOTE:**

Navigation arrows  appear at the bottom of each page when events fill more than one page.

The navigation arrows shown are a set of five buttons: a left-pointing arrow, a double left-pointing arrow, a box containing the number '1', a double right-pointing arrow, and a right-pointing arrow.

# Chapter 5

## Central Management

### ABOUT THIS CHAPTER

This chapter describes the Central Manager, and includes the following sections:

- ▶ **Launching the Central Manager**, beginning on page 5-2, describes how to launch the Central Manager.
- ▶ **Central Manager Quick Tour**, beginning on page 5-3, describes the Central Manager graphic user interface (GUI).
- ▶ **Central Management Workflow**, beginning on page 5-5, describes what you configure in the Central Manager after gateways have been deployed and registered. It also describes how to manage licenses and distributions.
- ▶ **Managing Tasks**, beginning on page 5-10, describes how to manage the operations performed by the gateways in the ActaStor network using the Central Manager.
- ▶ **Managing Groups**, beginning on page 5-66, describes how to manage groups using the Central Manager.
- ▶ **Managing Users**, beginning on page 5-82, describes how to manage users using the Central Manager.

# Launching the Central Manager

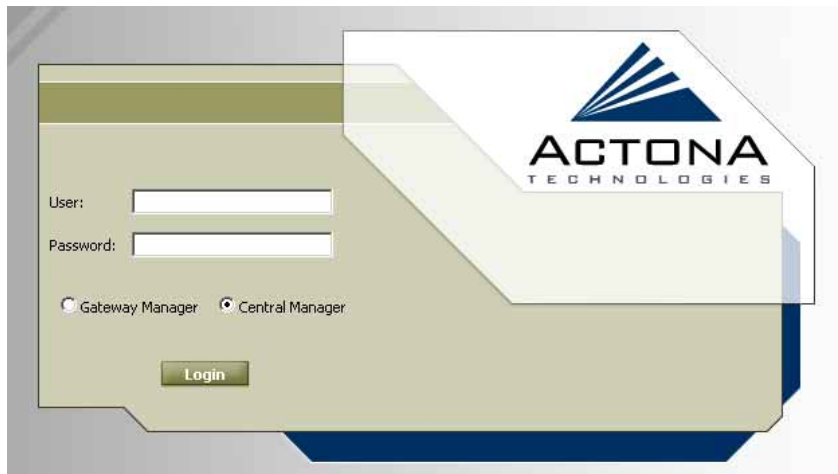
After the gateway designated as the Central Manager has been deployed, you can launch the Central Manager remotely from any location on the ActaStor network via Internet Explorer.

➤ **To launch the Central Manager:**

- 1 Open Internet Explorer 5.5 or above, and enter the ActaStor Management address:

**http://<Central\_Manager\_IP\_Address>/mgr.**

The *Login* page of the ActaStor Manager is displayed:



**Figure 5-1: Login Page – Central Manager**

- 2 Enter your user name and password in the fields provided. The default user name is **admin** and the default password is **actona**.

- 3 Select the **Central Manager** option (it is the default option) and click **Login** to display the Central Manager interface, as shown in the section that follows.

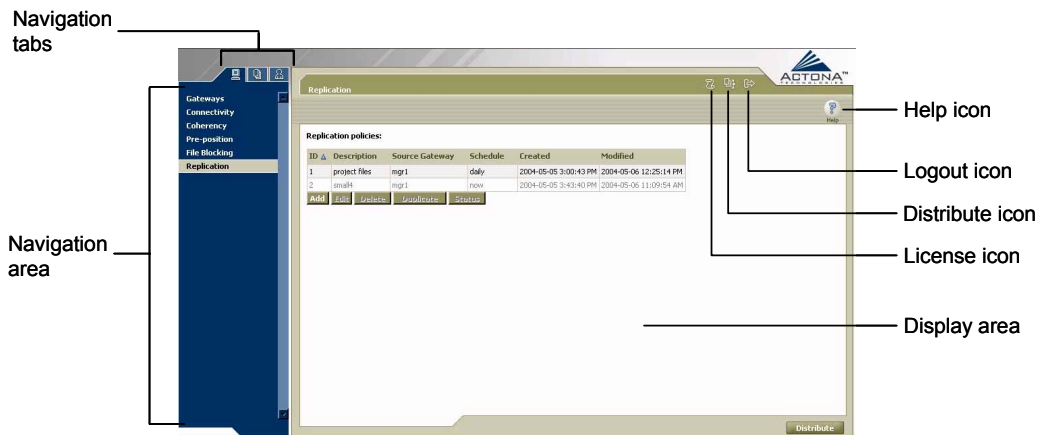


**NOTE:**

When accessing the Central Manager for the first time, a popup window is displayed containing the license agreement. Review the text of the agreement and then click **Accept** to continue.

## Central Manager Quick Tour

The Central Manager interface is divided into three sections. The area on the left contains a navigation area, which is divided into tabs used to navigate between the different Central Manager views. The display area on the right displays information relevant to the options you have selected from the navigation area. In addition to these sections, there are action icons on the upper-right side of the page.



**Figure 5-2: Central Manager Interface**


The Central Manager navigation tabs enable you to navigate to different views and management screens. It includes the following options:

- **Tasks:** Enables you to manage the gateways currently registered on the ActaStor network, which includes defining their connectivity and the policies that govern the actions they will perform. For more information, refer to *Managing Tasks*, page 5-10.
- **Groups:** Enables you to view and manage a list of all the groups of gateways defined in the Central Manager. For more information, refer to *Managing Groups*, page 5-66.
- **Users:** Enables you to view and manage a list of all ActaStor management users. For more information, refer to *Managing Users*, page 5-82.

Some of the options in the navigation area include suboptions, which are displayed as toolbar icons in the display area. Mandatory fields in the display area are indicated with an asterisk. If you click **Save** without entering a value in a mandatory field, an error message is displayed. Click the **Back** link to return to the page where the error occurred.

Information displayed in tables can be sorted by clicking the column headers. Clicking the header a second time sorts the information in reverse order.

As you select options in the navigation area, your current location in the manager is always displayed across the top of the display area.

To log out of the Central Manager, click the  icon on the upper-right side of the bar above the display area.

#### **IMPORTANT NOTE:**

JavaScripts, cookies and popup windows must be enabled in the Web browser in order to use the Central Manager.



# Central Management Workflow


After gateways have been deployed and registered, as described in *Chapter 3, Installation and Deployment*, you use the Central Manager to:

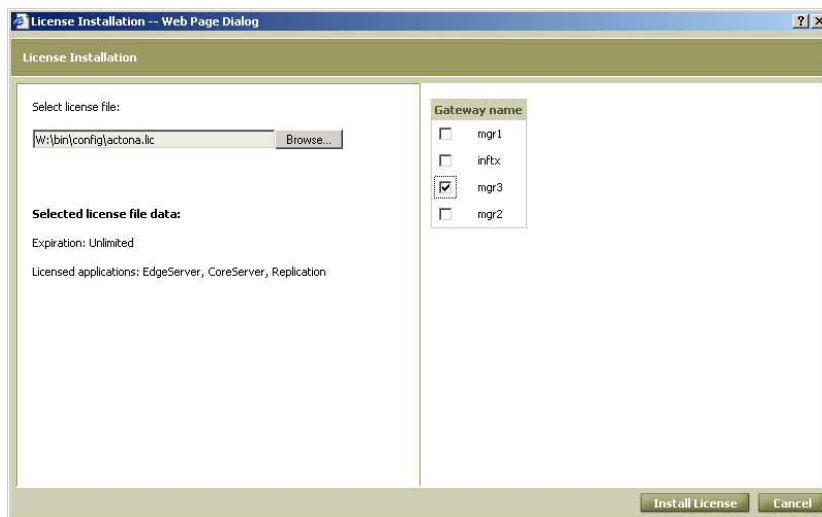
- Install ActaStor licenses, as described in *Managing Licenses*, page 5-6.
- Monitor gateways and access the Gateway Manager of a selected gateway, as described in *Gateways Option*, page 5-11.
- Define connectivity between gateways, as described in *Defining Connections Between EdgeServers and CoreServers*, page 5-17.
- Define policies that govern the behavior of gateways in the network, including:
  - Coherency policies, as described in *Defining Coherency Policies*, page 5-29.
  - Pre-position policies, as described in *Defining Pre-position Policies*, page 5-37.
  - File blocking policies, as described in *Defining File Blocking Policies*, page 5-49.
  - Replication policies, as described in *Defining Replication Policies*, page 5-54.
- Manage EdgeServer groups and CoreServer clusters, as described in *Managing Groups*, page 5-66.
- Manage users, as described in *Managing Users*, page 5-82.

## Managing Licenses

Activating specific ActaStor gateway components requires a valid license file obtained from Actona. This license specifies the licensed components as well as an expiration date. Licenses are distributed to the relevant gateways using the Central Manager. This is done by placing the license file in a secure location accessible from the workstation used for management, directing the Central Manager to the appropriate file and selecting the gateway to which the license applies. The appropriate information is then distributed to that gateway.

### ➤ To install a license:

- 1 Click the  icon on the upper-right side of the bar above the display area to display the following:



**Figure 5-3: License Installation Window**

- 2 In the **Select license file** field, click **Browse** and in the popup window displayed navigate to the location of the license file. (The license file will have an .LIC extension.)

- 3 Click **OK**. The path to the license file appears in the *License Installation* window. The details of the license are displayed in the **Selected license file data** area.
- 4 On the right side of the window, select the checkbox next to the gateway to which the license applies.
- 5 Click **Install License**. The license information is distributed to the selected gateways. You can confirm the results in the *Distribution Tasks* window, as described in *Managing Distributions*, below.

 **NOTE:**

After distributing the license, the components of all the registered gateways can be started at once, as described in *Performing Operations on All Gateways*, page 5-15.

## Managing Distributions

The data managed by the Central Manager is stored in a database. To take effect, this data must be sent to the relevant gateways. The distribution process compiles a list of changes that are made using the Central Manager and sends it to each relevant gateway whenever you click the **Distribute** button located at the bottom of each Central Manager page.

 **NOTE:**

To perform a general distribution of all Central Manager database information to all registered gateways, refer to page 5-15.


The *Distribution Tasks* window displays the status of all active and completed distributed tasks. You can view details of problematic tasks by clicking the relevant link.

 **NOTE:**

If a gateway component is stopped, and changes were made to it in the Central Manager, those changes can still be distributed, but will only take effect after that component is restarted.



➤ **To view distribution tasks:**

- 1 Click the  icon on the upper-right side of the bar above the display area to display the following:



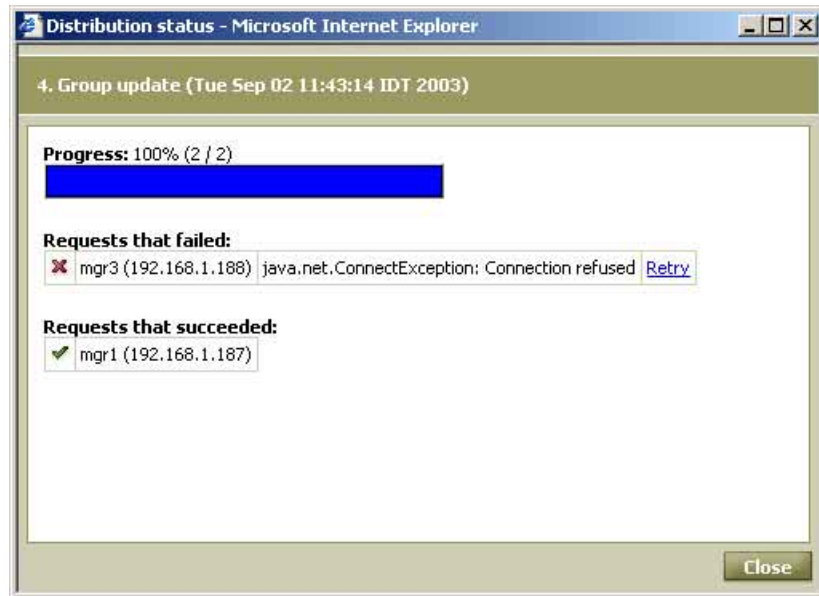
Task name	Progress	Control
<a href="#">1. Group update (Tue Sep 02 11:12:36 IDT 2003)</a>	Done ✓	<a href="#">Clear</a>
<a href="#">2. Group update (Tue Sep 02 11:13:33 IDT 2003)</a>	Done ✓	<a href="#">Clear</a>
<a href="#">3. License Installation (Tue Sep 02 11:37:16 IDT 2003)</a>	Done ✓	<a href="#">Clear</a>
<a href="#">4. Group update (Tue Sep 02 11:43:14 IDT 2003)</a>	Done ✘	<a href="#">Clear</a>

**Figure 5-4: Distribution Tasks Window**

This window includes the following information:

- **Task name:** Describes the task. The name is assigned to the task by the system.
- **Progress:** Indicates the current distribution percentage of the task. When a task is completed, it is marked as **Done**, with a status indicator of ✓ or ✘.
- **Control:** Includes a link for canceling the task during distribution, or clearing it from the list after its completion.

- 2 Click a task name to view its details, as shown below.




**Figure 5-5: Distribution Status**

Requests that have been successfully distributed have a checkmark ✔ next to them. Failed requests have an ✘ next to them. You can resend a failed request by clicking the **Retry** link.

# Managing Tasks

The Tasks view enables you to manage the operations and policies affecting gateways in the ActaStor network. This includes the connectivity between EdgeServers and CoreServers, as well as the coherency and pre-position policies assigned to various gateways. In addition, you can view basic information about each gateway and access specific Gateway Managers.

To access the Tasks view, click the **Tasks**  tab. The following page is displayed:



Gateway Name	IP	Applications	Status	Updated
mgr4	192.168.1.46	CoreServer, EdgeServer	✓	needs update
mgr3	192.168.1.188	CoreServer, EdgeServer	✗	updated

**Figure 5-6: Gateways Page**

The navigation area of the Tasks view includes the following options:

- **Gateways:** Enables you to view information about registered gateways and access their Gateway Managers, as described in *Gateways Option*, page 5-11.
- **Connectivity:** Enables you to define the connectivity between gateways, as described in *Defining Connections Between EdgeServers and CoreServers*, page 5-17.

- ▶ **Coherency:** Enables you to define coherency policies for CoreServers and the EdgeServers connected to them, as described in *Defining Coherency Policies*, page 5-29.
- ▶ **Pre-position:** Enables you to define pre-position policies that place files on designated EdgeServers according to a set schedule, as described in *Defining Pre-position Policies*, page 5-37.
- ▶ **File Blocking:** Enables you to define file blocking policies that prevent users connected to an EdgeServer from manipulating files that match a predefined pattern, as described in *Defining File Blocking Policies*, page 5-49.
- ▶ **Replication:** Enables you to define replication policies that copy files from one site to another via gateways at each site, as described in *Defining Replication Policies*, page 5-54.

## Gateways Option

The **Gateways** option displays the following tabs:

- ▶ **Gateways:** Enables you to view basic information about each registered gateway, as well as update and unregister selected gateways, as described in *Viewing and Managing Gateways*, page 5-12.
- ▶ **Operations:** Enables you to update the information in all registered gateways, as well as start and stop all gateway components in the network, as described in *Performing Operations on All Gateways*, page 5-15.

## Viewing and Managing Gateways

The **Gateways** tab displays a table of all registered gateways in the display area, including:

- **Status:** The current status of the gateway: ✓ (running) or ✗ (not running properly).
- **Gateway Name:** The name of the gateway.
- **IP:** The IP address of the gateway.
- **Applications:** The roles assigned to the gateway (CoreServer, EdgeServer and so on).
- **Distribution:** Whether the information in the gateway requires updating. (Click **Distribute** to send the latest information to any gateways requiring updating.)



The screenshot shows the 'Gateways' tab in the Actona management console. It features a table with columns for Status, Gateway Name, IP, Applications, and Distribution. Two gateways are listed: 'mgr1' with a red 'X' status and 'mgr4' with a green checkmark status. The 'mgr1' gateway has a 'required' distribution status, while 'mgr4' is 'up-to-date'. A 'view' button is located below the first row. At the bottom of the interface, there are 'Distribute' and 'Refresh' buttons.

Status	Gateway Name	IP	Applications	Distribution
✗	mgr1	192.168.1.187	CoreServer, EdgeServer	required
✓	mgr4	192.168.1.46	CoreServer, EdgeServer	up-to-date

Figure 5-7: Table of Registered Gateways

Each gateway name in the table acts as a link that can be clicked to display the Gateway Manager for that gateway.

**NOTES:**



An **X** displayed in the **Status** column indicates that at least one of the components of that gateway is not running.

To update the information displayed in the table, click **Refresh**.

➤ **To view additional gateway information:**

- 1 Select the row for the gateway in the table and click **View** to display the following popup window:



**Figure 5-8: Gateway Information Window**

The *Gateway information* window includes the following information:

- **Logical name:** The logical name of the gateway as it is identified in the Central Manager.
- **IP:** The IP address of the gateway.

- **Status:** The current status of the gateway (running or stopped).
  - **Last distribution:** The time when distribution was last performed on this gateway.
  - **Last change:** The time when any data relevant for this gateway was last updated in the Central Manager.
  - **Distribution status:** Whether the gateway requires a new distribution.
- 2 To open the Gateway Manager for the gateway, click **Open**. For more information, refer to *Chapter 4, Gateway Management*.
  - 3 For additional options, click **Advanced** to display the following:



**Figure 5-9: Gateway Information Page – Advanced**

- 4 To update the gateway with the latest information from the Central Manager database, click **Distribute**.

**NOTE:**



For information about performing a distribution to all gateways, refer to *Performing Operations on All Gateways*, below.

- 5 To unregister the gateway, click **Remove**. The gateway is removed from the Central Manager database. Any data that was defined for the gateway is deleted.



**CAUTION:**

Use this option with extreme care – deleted data cannot be recovered!

## Performing Operations on All Gateways

The **Operations** tab enables you to perform a **Distribute All** operation that updates the information contained in all the registered gateways in the ActaStor network.

In addition, the **Operations** tab enables you to start or stop all the components in each gateway with a single click. The **Start All** option is used after distributing a license to each gateway, as described in *Managing Licenses*, page 5-6. The **Stop All** option is used when a system shutdown is required, for example during network maintenance.

**NOTE:**

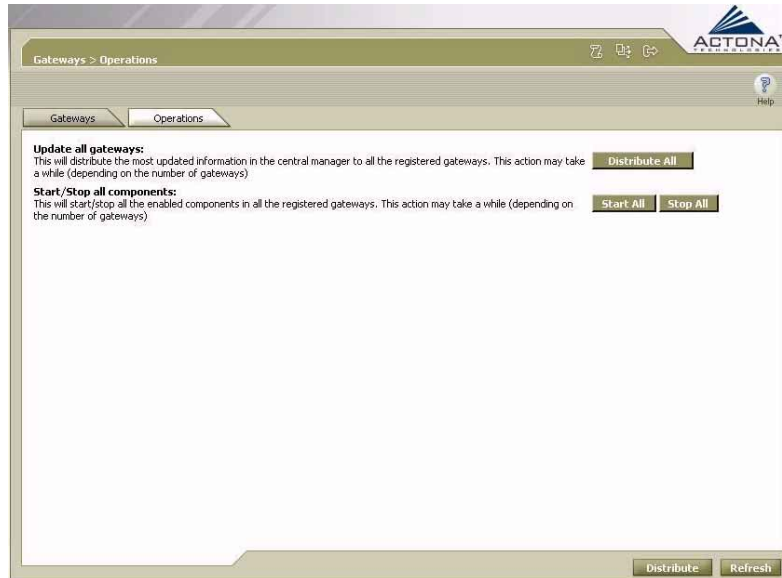


These operations may take time to perform, depending on the number of gateways.



➤ **To perform operations on all gateways:**

- 1 In the *Gateways* page, click the **Operations** tab to display the following:



**Figure 5-10: Gateway Operations Page**

- 2 To send an update to all gateways, regardless of their current distribution status, click **Distribute All**.

**NOTE:**



For more information about distributions, refer to *Managing Distributions*, page 5-7.

- 3 To start the components (EdgeServer, CoreServer, Replication) inside each gateway, click **Start All**.
- 4 To stop the components inside each gateway, click **Stop All**.

## Defining Connections Between EdgeServers and CoreServers

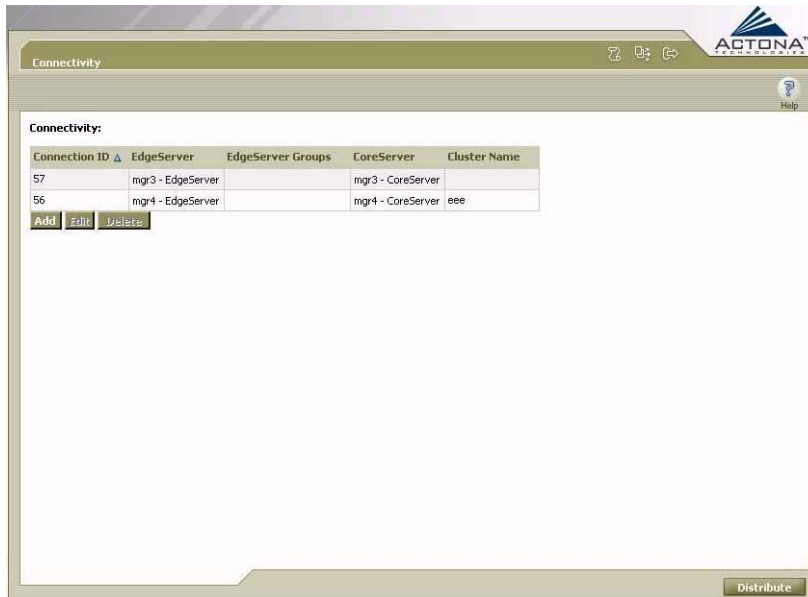
The **Connectivity** option in the Tasks view enables you to define connections between CoreServers and EdgeServers. Connections are defined using various combinations of individual gateways, EdgeServer groups and CoreServer clusters (a group of CoreServers that access the same file servers and act as a single, logical CoreServer). Without the proper connections, you cannot define policies.

When defining a connection that includes multiple CoreServers and EdgeServers, it is important to confirm beforehand that each CoreServer-EdgeServer link has the same connection parameters, such as allocated bandwidth and roundtrip delay, as well as identical aliasing and NFS parameters. If this is not the case, a separate connection must be defined for each link.

### NOTE:

It is recommended to define EdgeServer groups and CoreServer clusters before defining any connections involving those groups and clusters. For more information, refer to *Managing Groups*, page 5-49.

When you select **Connectivity** in the navigation area of the Tasks view, the *Connectivity* page, showing a list of existing connections in the ActaStor network, is displayed, as shown below.



**Figure 5-11: Connectivity Page**

The following information is displayed about each connection:

- **Connection ID:** The number assigned by the Central Manager to the connection.
- **EdgeServer:** The name of the EdgeServer(s) included in the connection (if the list is long, only the first few are displayed).
- **EdgeServer Groups:** The name of the EdgeServer group(s) included in the connection, if any.
- **CoreServer:** The name of the CoreServer(s) included in the connection.
- **Cluster Name:** The name of the CoreServer cluster(s) included in the connection, if any.

➤ **To define a new connection:**

- 1 From the *Connectivity* page, click **Add** to display the following:



**Figure 5-12: Selecting CoreServers for Connection**

Connectivity parameters are divided into the following tabs:

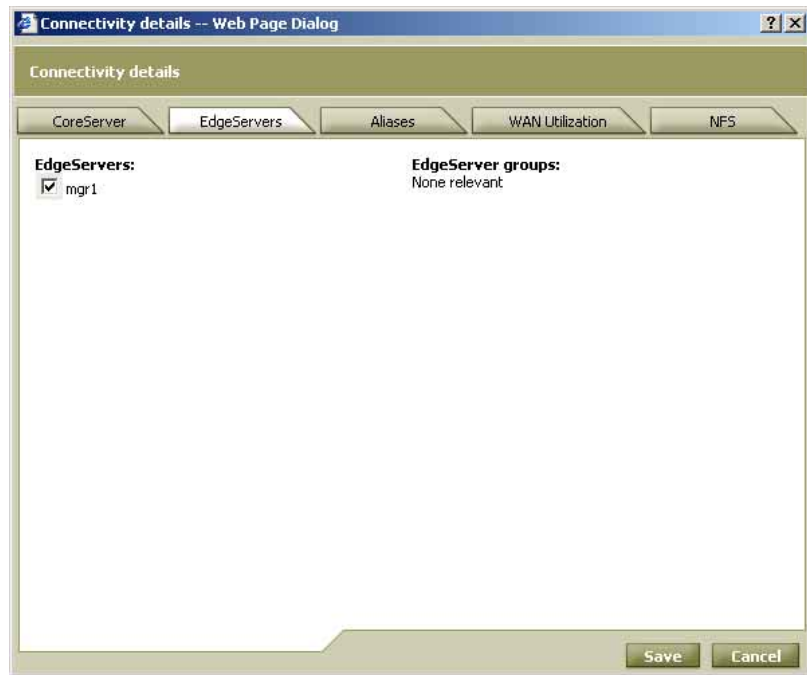
- **CoreServer:** Specifies the CoreServers or CoreServer clusters in the connection.
- **EdgeServers:** Specifies the EdgeServers and/or EdgeServer groups in the connection.
- **Aliases:** Specifies which file servers are exported for the connection and defines the naming convention that is used.
- **WAN Utilization:** Defines parameters related to the WAN connection between the CoreServer and the EdgeServers.
- **NFS:** Defines the NFS connection parameters used to access the file servers (applies to NFS file servers only).

- 2 In the **CoreServer** tab, select **Standalone CoreServers**, or select **CoreServer Cluster** and then select one of the clusters listed below the option.
- 3 Do one of the following:
  - If **Standalone CoreServers** was selected, select one CoreServer from the list displayed on the right.
  - If a CoreServer cluster was selected, select the CoreServers within the cluster to which the EdgeServer may connect from the list displayed on the right. This selection of multiple CoreServers is for failover purposes, as described in *Clustering and Failover in Chapter 2, Getting Started*.

**NOTE:**

When connecting to a cluster, it is generally recommended to connect the EdgeServer to multiple CoreServers in the cluster in order to make proper use of ActaStor's failover mechanism.

- 4 Click the **EdgeServer** tab to display the following:



**Figure 5-13: Selecting EdgeServers for Connection**

- 5 Select the checkboxes next to each individual EdgeServer or EdgeServer group to include the connection.

6 Click the **Aliases** tab to display the following:



The screenshot shows a web page dialog titled "Connectivity details" with several tabs: CoreServer, EdgeServers, Aliases, WAN Utilization, and NFS. The "Aliases" tab is active. It contains radio buttons for "Original file server name", "Prefix: AS-", and "Suffix:". Below is a table with columns "Exported", "File server", "Alias", and "Exported as".

Exported	File server	Alias	Exported as
<input checked="" type="checkbox"/>	frodo	newFs	newFs
<input type="checkbox"/>	netapp.lab.actona.com		
<input checked="" type="checkbox"/>	win3srv		AS-win3srv

Buttons for "Export all" and "Export none" are located below the table. "Save" and "Cancel" buttons are at the bottom right of the dialog.

**Figure 5-14: Defining File Server Aliases**

The **Aliases** tab enables you to decide which of the file servers exported by the CoreServers (as selected in the CoreServer tab) should be made available to the clients connected to the selected EdgeServers.

In addition, this tab enables 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 **as-** is defined as a prefix, and the name of the file server is **win3srv**, users will see this file server as **as-win3srv**.

- 7 Select one of the following file server naming options:
  - **Original file server name:** The name of each exported file server should be based on its original name.
  - **Prefix:** A prefix should be appended to the name of each exported file server. Enter the prefix in the field provided.
  - **Suffix:** A suffix should be appended to the name of each exported file server. Enter the suffix in the field provided.
- 8 The table in the **Aliases** field lists each file server exported by the selected CoreServers. Select the checkbox next to each file server that should be made available to the users of this connection.

**NOTE:**

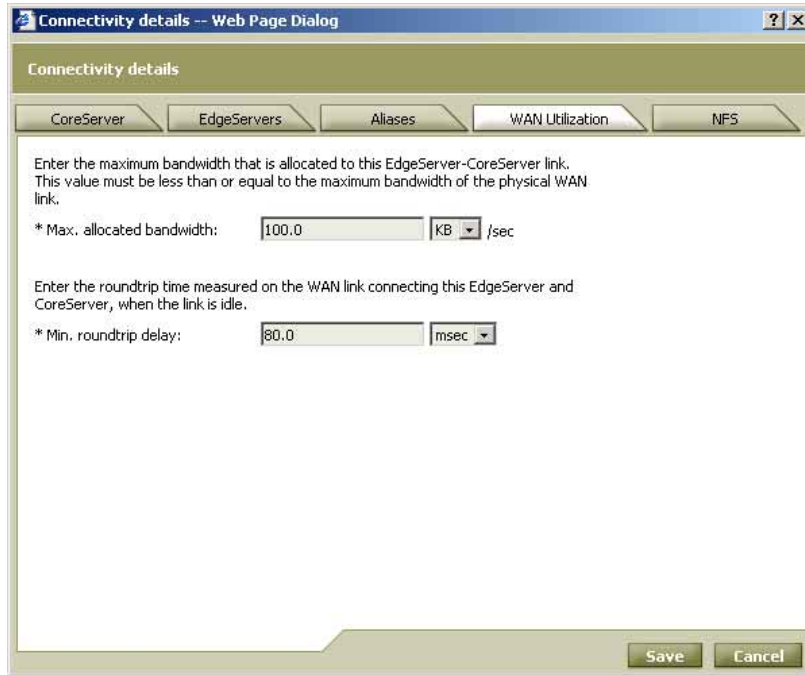


Click **Export all** to select all file servers or **Export none** to clear all the checkboxes.

- 9 [Optional] If required, enter an alias for selected file servers in the **Alias** column. An alias, which can be any name (max. 15 characters), overrides the default prefix/suffix setting defined in step 7. The **Exported as** column displays the name of each exported file server as it will appear to users.



10 Click the **WAN Utilization** tab to display the following:



The screenshot shows a web browser window titled "Connectivity details -- Web Page Dialog". The main content area is titled "Connectivity details" and contains five tabs: "CoreServer", "EdgeServers", "Aliases", "WAN Utilization", and "NFS". The "WAN Utilization" tab is selected. The content of the tab includes the following text and form fields:

Enter the maximum bandwidth that is allocated to this EdgeServer-CoreServer link.  
This value must be less than or equal to the maximum bandwidth of the physical WAN link.

\* Max. allocated bandwidth:   /sec

Enter the roundtrip time measured on the WAN link connecting this EdgeServer and CoreServer, when the link is idle.

\* Min. roundtrip delay:

At the bottom right of the dialog, there are "Save" and "Cancel" buttons.

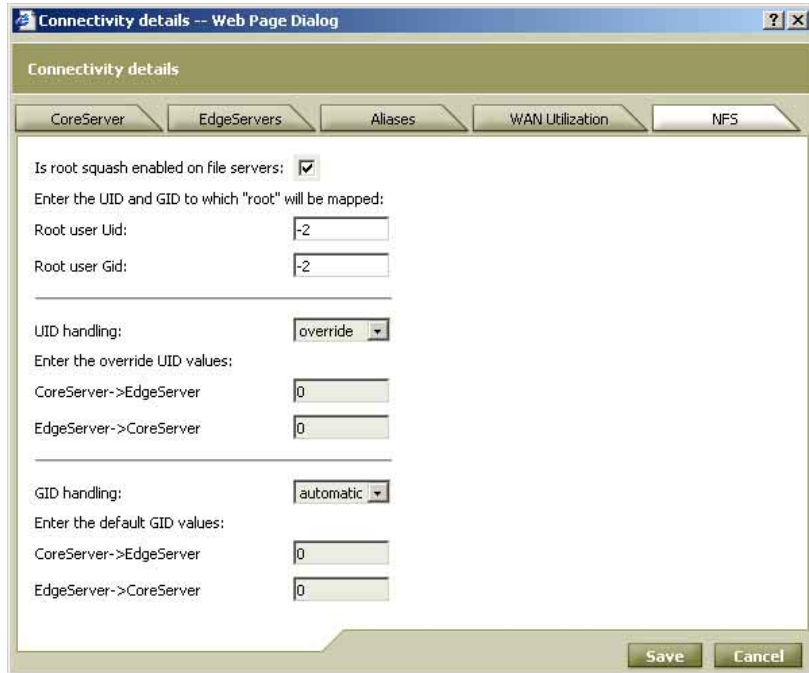
**Figure 5-15: Defining WAN Utilization Parameters**

The **WAN Utilization** tab contains parameters regarding the WAN connection between the CoreServer and EdgeServers in the connection.

11 Define the following network parameters:

- **Max. allocated bandwidth:** Enter the maximum bandwidth allocated to the connection (select the measurement unit from the dropdown list). This value must be less than or equal to the maximum bandwidth of the physical WAN link between the gateways.
- **Min roundtrip delay:** Enter the length of time it takes a bit to travel roundtrip from one gateway to the other end and back when the link is idle (select the measurement unit from the dropdown list).

- 12** If the connection is being used to export NFS file servers, click the **NFS** tab to display the following:



**Figure 5-16: Defining NFS Parameters**

- 13** Select the **Is root squash enabled on file servers** checkbox if root squashing has been enabled on the file servers to which the CoreServer is connected. This is a common security feature used to prevent root users from bypassing authentication procedures, and is the default mode on most file servers.

**NOTE:**

Root squash is enabled by default on Solaris and Red Hat Linux file servers.

- 14** If you selected the **Is root squash enabled on file servers** checkbox, fields for entering both a UID (user ID) and GID (group ID) are displayed. In the **Root user UID** and **Root user GID** fields, enter the user and group ID that replaces the root user for accessing the file server.
- 15** From the **UID handling** dropdown list, select how to handle the UID of files being transferred between the EdgeServer and CoreServer from the following options:
- **original:** Maintains the original UID defined in the file server. Use this option if the remote site has the same user list as the core site. This option runs the risk that a UID will not be defined in the EdgeServer. In this case, the file may not be accessible.
  - **override:** Replaces the existing UID with a new UID. If you select this option, additional fields for entering the new UIDs are displayed:
    - **CoreServer -> EdgeServer:** Enter a new UID for files accessed by the EdgeServer from the CoreServer.
    - **EdgeServer -> CoreServer:** Enter a new UID for new files created at the EdgeServer and then written back to the CoreServer.
  - **automatic:** Matches the UID by name instead of number. If this option is selected, you are prompted to enter the default UID values to use in case the user name cannot be found.

**NOTE:**

If the **automatic** option is used, NIS (Network Information Service) should be configured at both the core and remote sites.

- 16** From the **GID handling** dropdown list, select how to handle the GID of files being transferred between the EdgeServer and CoreServer from the following options:
- **original:** Maintains the original GID defined in the CoreServer. Use this option if the remote site has the same group list as the core site. This option runs the risk that a GID will not be defined in the EdgeServer. In this case, the file may not be accessible.
  - **override:** Replaces the existing GID with a new GID. If you select this option, additional fields for entering the new GIDs are displayed:
    - **CoreServer -> EdgeServer:** Enter a new GID for files accessed by the EdgeServer from the CoreServer.
    - **EdgeServer -> CoreServer:** Enter a new GID for new files written back to the CoreServer from the EdgeServer.
  - **automatic:** Matches the GID by name instead of number. If this option is selected, you are prompted to enter the default GID values to use in case the group name cannot be found.

**NOTE:**

If the **automatic** option is used, NIS should be configured at both the core and remote sites.

- 17** Click **Save**. The new connection is added to the table on the *Connectivity* page.
- 18** Repeat steps 1 through 17 for each new connection you want to configure.
- 19** Click **Distribute** to update the affected gateways.

## Editing a Connection

The properties of a connection may be modified at any time. Modifications must be distributed in order to take effect.

### ➤ To edit a connection:

- 1 From the *Connectivity* page, select a connection from the list and click **Edit**. The *Connectivity details* window is displayed, as shown on page 5-19.
- 2 Edit the properties of the connection as required.
- 3 Click **Save**. The modified connection is saved.
- 4 Click **Distribute** to update the affected gateways.

## Deleting a Connection

Connections may be deleted at any time. Deletions must be distributed in order to take effect.

### ➤ To delete a connection:

- 1 From the *Connectivity* page, select a connection from the list and click **Delete**. The selected connection is deleted from the list.
- 2 Click **Distribute** to update the affected gateways.

## Defining Coherency Policies

The **Coherency** option in the Tasks view enables you to define coherency policies that determine the overall coherency between the files in the EdgeServer cache and the files located on the file server.


There are three levels of coherency – local, global and strict, as described in *Chapter 2, Getting Started*. If a coherency policy is not defined for a particular set of data on a file server, the default coherency (global for CIFS, local for NFS) is applied.

No restrictions are placed on the ability to define different coherency levels to different folders, sub-folders and even specific file types on the same file server. For example, a file server can be assigned a global coherency policy and a particular folder on that server can be assigned a local coherency policy. Policy conflicts are resolved in favor of the policy with the most specific path. For example, if one coherency policy applies to an entire file server (such as a strict coherency policy for all files with the extension PPT) and a local policy applies to a folder on that server, the latter policy is applied to all the files in that folder, even those with a PPT extension.

After defining coherency policies, they must be distributed to the appropriate EdgeServers. This is because policies are defined at the CoreServer level, but implemented at the EdgeServer level. This enables consistent policy enforcement for all users connected to the CoreServer. You can edit and delete coherency policies, as required.

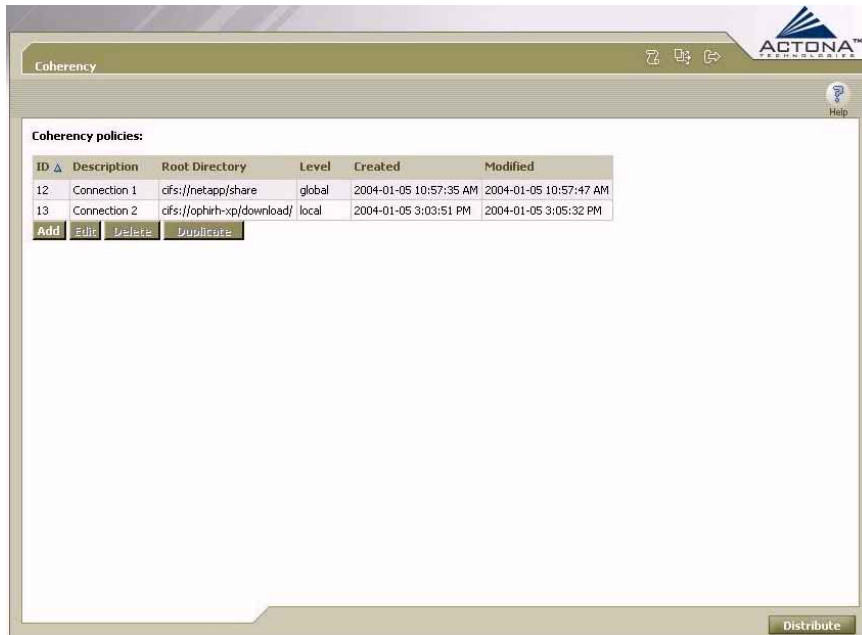
For more information about coherency, refer to *Chapter 2, Getting Started*, and *Managing the EdgeServer Component* in *Chapter 4, Gateway Management*.

### NOTE:



A warning message is displayed if the required connections do not exist for defining coherency policies, as described on page 5-17.

When you select **Coherency** in the navigation area of the Tasks view, the *Coherency* page, showing a list of existing coherency policies in the ActaStor network, is displayed, as shown below.



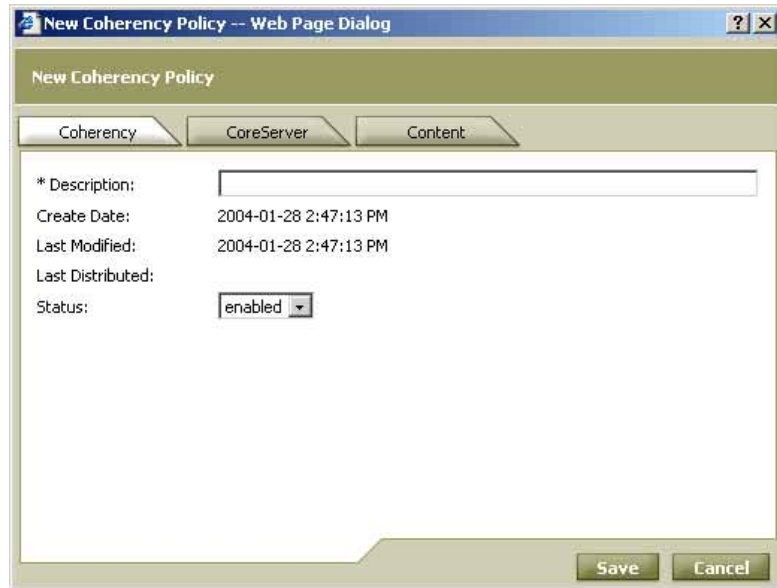
**Figure 5-17: Coherency Page**

The following information is displayed about each coherency policy:

- ▲ **ID:** The number assigned by the Central Manager to the coherency policy.
- ▲ **Description:** A brief description of the policy.
- ▲ **Root Directory:** The source directory for the content affected by the policy.
- ▲ **Level:** The level of coherency applied by this policy.
- ▲ **Created:** The date the policy was created.
- ▲ **Modified:** The date the policy was last modified.

➤ **To define coherency policies:**

- 1 From the *Coherency* page, click **Add** to display the following popup window:



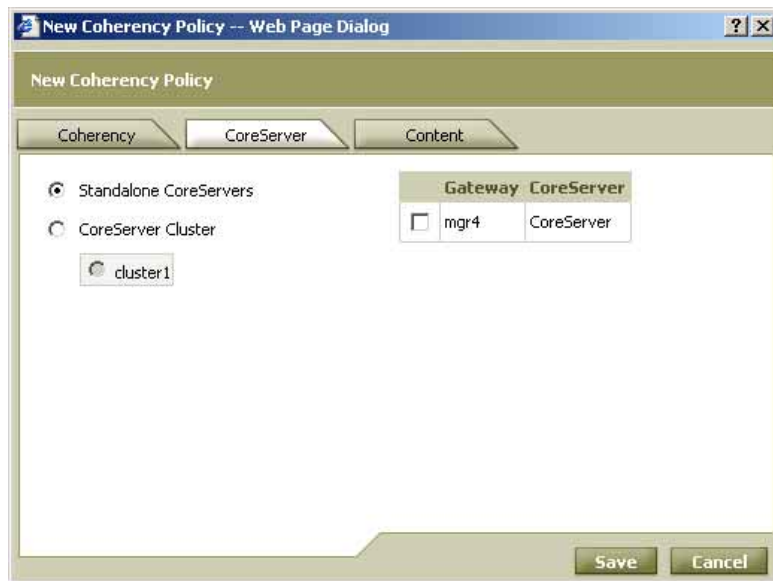
**Figure 5-18: New Coherency Policy Window – Coherency Tab**

The *New Coherency Policy* window contains the following tabs:

- **Coherency:** For entering a description of the policy and selecting its status.
- **CoreServer:** For selecting the CoreServers included in the policy.
- **Content:** For selecting the content to which the policy applies.



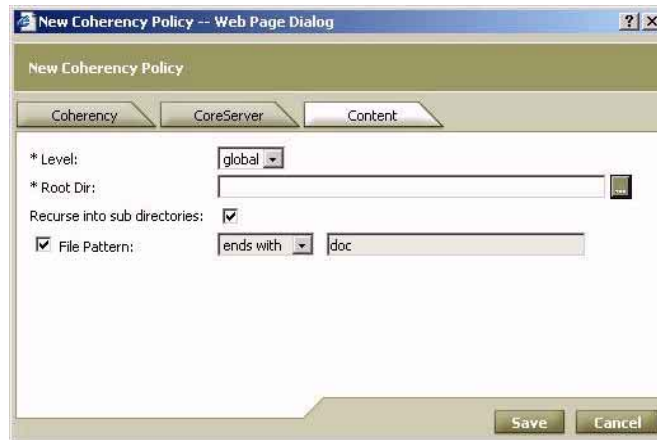
- 2 Define the following information in the **Coherency** tab:
  - In the **Description** field, enter a short description for the policy.
  - From the **Status** dropdown list, select the status of the policy: **enabled** or **disabled**. Disabled policies are not put into effect and therefore do not affect coherency.
- 3 Click the **CoreServer** tab to display the following:



**Figure 5-19: New Coherency Policy Window – CoreServer Tab**

- 4 Define the following information:
  - Select **Standalone CoreServers** or **CoreServer Cluster**.
  - If **Standalone CoreServers** was selected, select one of the CoreServers listed on the right. If **CoreServer Cluster** was selected, select one of the clusters listed below the option.

5 Click the **Content** tab to display the following:

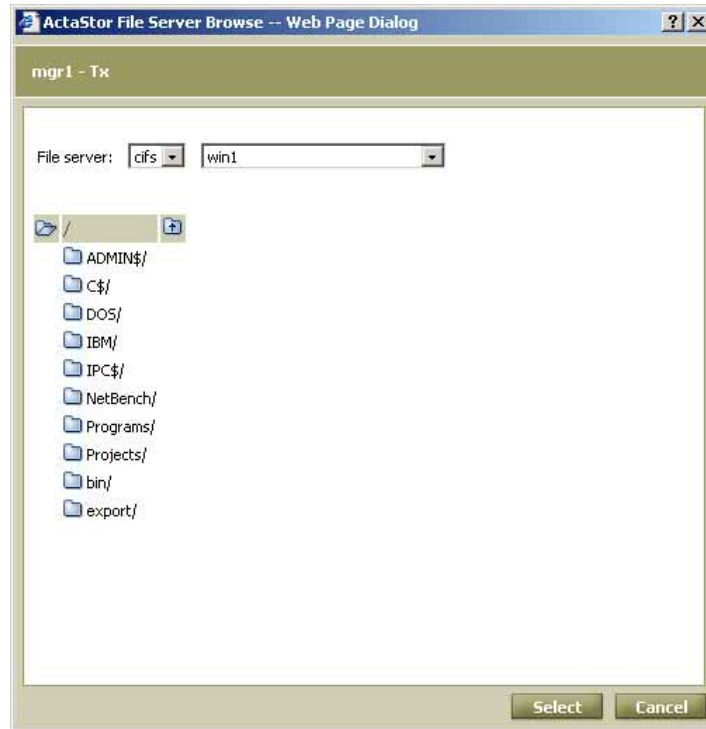


**Figure 5-20: New Coherency Policy Window – Content Tab**

6 Define the following information:

- From the **Level** dropdown list, select the coherency level for the new policy: **local**, **global** or **strict**.
  - **local**: Used for intra-site access (default for NFS)
  - **global**: Standard coherency level, used for inter-site access (default for CIFS)
  - **strict**: Highest coherency level

- In the **Root Dir** field, click  to display the following window:



**Figure 5-21: Defining the Root Directory**

- From the **File server** dropdown lists, select the file system type, either **cifs** or **nfs**, and then select the name of the file server containing the files to which the coherency policy will apply.
- In the tree beneath the **File server** dropdown lists, navigate the directory tree (click the folder icons to drill down to sub-folders), select the required directory by clicking its name and click **Select**. The popup window closes, and the path of the selected root directory is displayed in the **Root Dir** field.

- [Optional] Select the **Recurse into sub directories** checkbox to include all subdirectories of the selected folder in the coherency policy. If this option is not selected, only the files in the selected root directory are included in the policy.
- [Optional] To narrow the policy definition to a particular type of file, select the **File Pattern** checkbox, select a pattern operator from the dropdown list, and in the adjacent text box, enter free text describing the pattern. For example, **ends with .doc**.

- 7 Click **Save**. The policy is added to the table on the *Coherency* page.

**NOTE:**



The new policy takes effect only when distributed to the relevant EdgeServers. For more information, refer to *Managing Distributions*, page 5-7.

- 8 Repeat steps 1 through 7 for each new policy you want to define.
- 9 Click **Distribute** to update the affected gateways.

## Editing a Coherency Policy

The properties of a coherency policy may be modified at any time. Modifications must be distributed in order to take effect.

### ➤ To edit a coherency policy:

- 1 From the *Coherency* page, select a coherency policy from the list and click **Edit**. The *Edit Coherency Policy* window is displayed. (This resembles the *New Coherency Policy* window, as shown on page 5-31.)
- 2 Edit the properties of the policy, as required.
- 3 Click **Save**. The modified policy is saved.
- 4 Click **Distribute** to update the affected gateways.

## Duplicating a Coherency Policy

An existing coherency policy can be duplicated in order to use it as a base for a new policy.

### ➤ To duplicate a coherency policy:

- 1 From the *Coherency* page, select a policy from the list and click **Duplicate**. The *Edit Coherency Policy* window is displayed. The fields are predefined based on the properties of the policy that was duplicated.
- 2 Edit the properties of the policy as required.
- 3 Click **Save**. The new policy is saved.
- 4 Click **Distribute** to update the affected gateways.

## Deleting a Coherency Policy

Coherency policies may be deleted at any time. Deletions must be distributed in order to take effect.

### ➤ To delete a coherency policy:

- 1 From the *Coherency* page, select a coherency policy from the list and click **Delete**. The selected policy is deleted from the list.
- 2 Click **Distribute** to update the affected gateways.

## Defining Pre-position Policies

The **Pre-position** option in the Tasks view enables you to define one or more pre-position policies that determine which files should be proactively copied from CIFS file servers to the cache of selected EdgeServers, according to a pre-defined schedule. Pre-positioning enables you to take advantage of idle time on the WAN to transfer frequently accessed files to selected EdgeServers, where users can benefit from cache-level performance even during first-time access of these files.

When defining a pre-position policy, you must select the CoreServers (or CoreServer clusters) and EdgeServers (or EdgeServer groups) involved in the file transfers. Next, you specify the content to be pre-positioned, including the root directory and a specific file pattern, if required. Since the policy may call for the task to be repeated on a regular basis, you also 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.

Pre-position policies can be scheduled to run either once or on a recurring basis, based on time of day, days of the week or days of the month. In addition, time and size limits can be placed on the policy, to prevent the task from consuming too much bandwidth on the WAN or too much space on the EdgeServer cache. It is strongly recommended to use these limits in order to optimize network efficiency and prevent misuse of this feature.

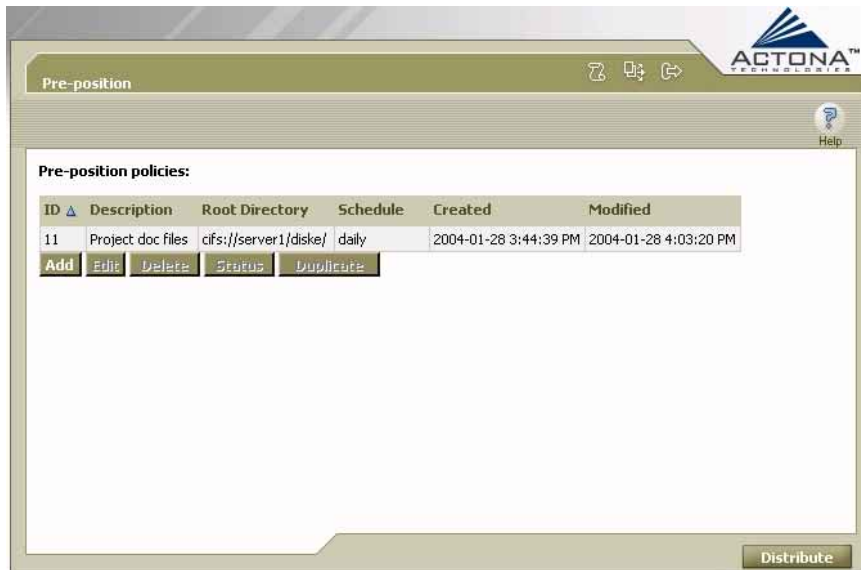
When the activation time of a policy arrives, a pre-position task is initiated in each EdgeServer to which it has been assigned. Each policy task can be monitored in either the Central Manager or the Gateway Manager, both during and after processing. Active tasks can be terminated if required, as described in *Chapter 4, Gateway Management*.

For more information about pre-positioning, refer to *Chapter 2, Getting Started*, and *Managing the EdgeServer Component in Chapter 4, Gateway Management*.

**NOTE:**

A warning message is displayed if the required connections do not exist for defining pre-position policies, as described on page 5-17.

When you select **Pre-position** in the navigation area of the Tasks view, the *Pre-position* page, showing a list of existing pre-position policies in the ActaStor network is displayed, as shown below.



Pre-position

ACTONA™  
TECHNOLOGIES

Help

Pre-position policies:

ID ▲	Description	Root Directory	Schedule	Created	Modified
11	Project doc files	cifs://server1/diske/	daily	2004-01-28 3:44:39 PM	2004-01-28 4:03:20 PM

Add Edit Delete Status Duplicate

Distribute

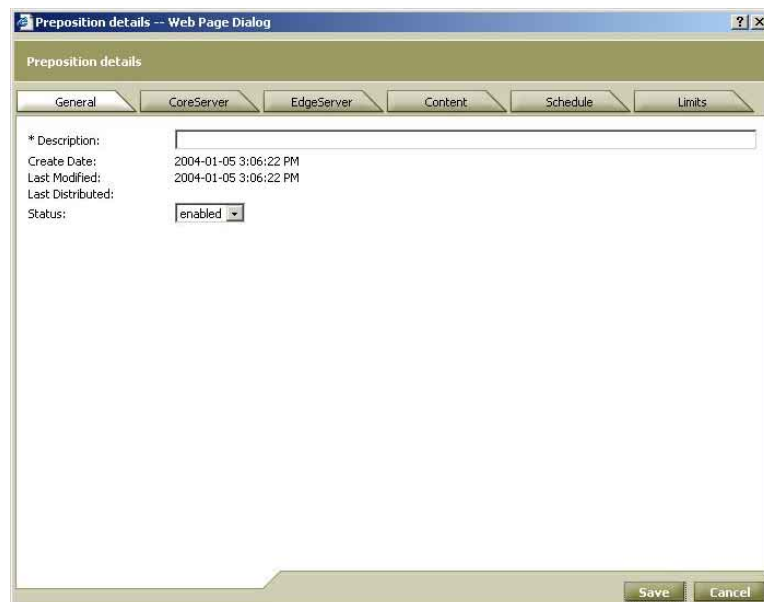
**Figure 5-22: Pre-position Page**

The following information is displayed about each pre-position policy:

- ▲ **ID:** The number assigned by the Central Manager to the pre-position policy.
- ▲ **Description:** A brief description of the policy.
- ▲ **Root Directory:** The location on the file server containing the files to be pre-positioned. Files are located in this directory, and optionally, in its subdirectories.
- ▲ **Schedule:** The type of schedule (daily, weekly, and so on) set for the policy.
- ▲ **Created:** The date when the policy was created.
- ▲ **Modified:** The date when the policy was last modified.

➤ **To define pre-position policies:**

- 1 From the *Pre-position* page, click **Add** to display the following popup window:



**Figure 5-23: Pre-position Details Window – General Tab**



The *Pre-position details* window contains the following tabs:

- **General:** For entering a description of the policy and selecting its status.
- **CoreServer:** For selecting the CoreServers included in the policy.
- **EdgeServer:** For selecting the EdgeServers included in the policy.
- **Content:** For selecting the content to which the policy applies.
- **Schedule:** For defining when and how often the policy is to be run.
- **Limits:** For setting size and time limits on each iteration of the pre-position task defined by the policy.

**2** Define the following information in the **General** tab:

- In the **Description** field, enter a name for the policy.
- From the **Status** dropdown list, select the status of the policy: **enabled** or **disabled**. Disabled policies are not put into effect.

- 3 Click the **CoreServer** tab to display the following:



**Figure 5-24: Pre-position Details Window – CoreServer Tab**

- 4 Define the following information:
  - Select **Standalone CoreServers** or **CoreServer Cluster**.
  - If **Standalone CoreServers** was selected, select one of the CoreServers listed on the right. If **CoreServer Cluster** was selected, select one of the clusters listed below the option.

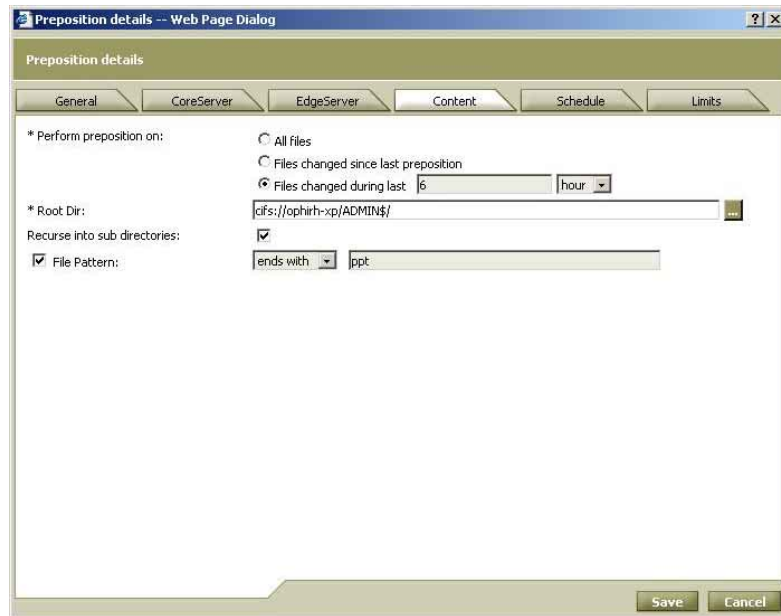
- 5 Click the **EdgeServer** tab to display the following:



**Figure 5-25: Pre-position Details Window – EdgeServer Tab**

- 6 From the dropdown list, select **All EdgeServers** (that is, all EdgeServers connected to the CoreServers selected in the previous tab) or **Selected EdgeServers**. If the policy applies only to selected EdgeServers, mark the checkboxes next to each relevant EdgeServer or EdgeServer group.

**7** Click the **Content** tab to display the following:



**Figure 5-26: Pre-position Details Window – Content Tab**

**8** Define the following information:

- In the **Perform pre-position on** field, select one of the following options:
  - **All files**
  - **Files changes since last pre-position**
  - **Files changed during last** (enter a value and select a time unit from the dropdown list)
- In the **Root Dir** field, click  to browse to the root directory path on the file server containing the files to be pre-positioned (see Figure 5-21).

- [Optional] Select the **Recurse into sub directories** checkbox to include all subdirectories of the selected folder in the pre-position policy. If this option is not selected, only the files in the selected root directory will be included in the policy.
  - [Optional] To narrow the policy definition to a particular type of file, select the **File Pattern** checkbox, select a pattern operator from the dropdown list, and in the adjacent text box, enter free text describing the pattern. For example, **ends with .doc**.
- 9 Click the **Schedule** tab to display the following:



Figure 5-27: Pre-position Details Window – Schedule Tab

- 10** From the **Schedule** dropdown list, select one of the following scheduling options:
- **now:** The task defined by the policy is run as soon as it is distributed to the relevant gateways.
  - **date:** The task is run once at a defined time and date.
  - **daily:** The task is run daily at a defined time.
  - **weekly:** The task is run on selected days of the week at a defined time.
  - **monthly, days:** The task is run on selected days of the month at a defined time.
  - **monthly, weekday:** The task is run on a defined day (as opposed to a defined date) and time during the month. For example, you can have the task run on the second Tuesday of every month, as shown below.



**Figure 5-28: Schedule Tab – Monthly, Weekday Option**

**11** Click the **Limits** tab to display the following:



The screenshot shows a web browser window titled "Preposition details -- Web Page Dialog". The window has a tabbed interface with tabs for "General", "CoreServer", "EdgeServer", "Content", "Schedule", and "Limits". The "Limits" tab is selected. Below the tabs, there is a section titled "Select the fields using the checkbox and then set their values:". This section contains four rows of settings, each with a checked checkbox, a text input field, and a unit dropdown menu:

- Total size: 10 % of cache size
- Duration: 3 hour
- Max file size: 300 MB
- Min file size: 20.0 KB

At the bottom right of the window, there are "Save" and "Cancel" buttons.

**Figure 5-29: Pre-position Details Window – Limits Tab**

**12** [Optional] Select one or more of the following checkboxes to define time and/or size limits for the pre-position task:

- **Total size:** The pre-positioned files cannot consume more than a defined percentage of the overall EdgeServer cache.
- **Duration:** The task cannot take longer than the amount of time entered here. Select a time unit from the dropdown list.
- **Max file size:** The maximum allowable size of each file being pre-positioned. Files larger than this are ignored.

- **Min file size:** The minimum size of each file being pre-positioned. Files smaller than this are ignored. (The default value is 20 KB. As a general rule, it is inefficient to pre-position files smaller than this, as they can be retrieved quickly enough over the WAN via ActaStor, as needed.)

**NOTE:**



If a limit is exceeded during a pre-position task, the task is terminated and a message is sent to the Administrator log. Any remaining files are transferred 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 via ActaStor as usual.

- 13** Click **Save**. The policy is added to the table on the *Pre-position* page.

**NOTE:**



The new policy takes effect only when distributed to the relevant EdgeServers. For more information, refer to *Managing Distributions*, page 5-7.

- 14** Repeat steps 1 through 13 for each new pre-position policy you want to define.

- 15** Click **Distribute** to update the affected gateways.

**NOTES:**



To view the current status and history of a selected pre-position policy, select it in the table on the *Pre-position* page and click **Status**.

The current status and history of pre-position policies assigned to a particular EdgeServer can also be viewed using the Gateway Manager. In addition, any pre-position tasks currently being run can be terminated, if required. For more information, refer to *Policies Option* in *Chapter 4, Gateway Management*.



## Editing a Pre-position Policy

The properties of a pre-position policy may be modified at any time. Modifications must be distributed in order to take effect.

### ➤ To edit a pre-position policy:

- 1 From the *Pre-position* page, select a pre-position policy from the list and click **Edit**. The *Pre-position details* window is displayed, as shown on page 5-39.
- 2 Edit the properties of the policy, as required.
- 3 Click **Save**. The modified policy is saved.
- 4 Click **Distribute** to update the affected gateways.

#### **NOTE:**



Changing the status of a pre-position policy to **disabled** terminates the current task generated by that policy.

## Duplicating a Pre-position Policy

An existing pre-position policy can be duplicated in order to use it as a base for a new policy.

### ➤ To duplicate a pre-position policy:

- 1 From the *Pre-position* page, select a policy from the list and click **Duplicate**. The *Pre-position details* window is displayed, as shown on page 5-39. The fields are predefined based on the properties of the policy that was duplicated.
- 2 Edit the properties of the policy as required.
- 3 Click **Save**. The new policy is saved.
- 4 Click **Distribute** to update the affected gateways.

## Deleting a Pre-position Policy

Pre-position policies may be deleted at any time. Deletions must be distributed in order to take effect.

➤ **To delete a pre-position policy:**

- 1 From the *Pre-position* page, select a policy from the list and click **Delete**. The selected policy is deleted from the list.
- 2 Click **Distribute** to update the affected gateways.



**NOTE:**

Deleting a pre-position policy terminates the current task generated by that policy.

## Defining File Blocking Policies

The **File Blocking** option in the Tasks view enables you to define one or more file blocking policies that prevent users from opening, creating or copying files that match a defined file pattern. These policies, which apply to all EdgeServers in the ActaStor network (and by extension, to all users connected to them), prevent precious bandwidth, as well as file server and cache space, from being wasted on files that system administrators decide to block. In addition, these policies can simplify file server management.

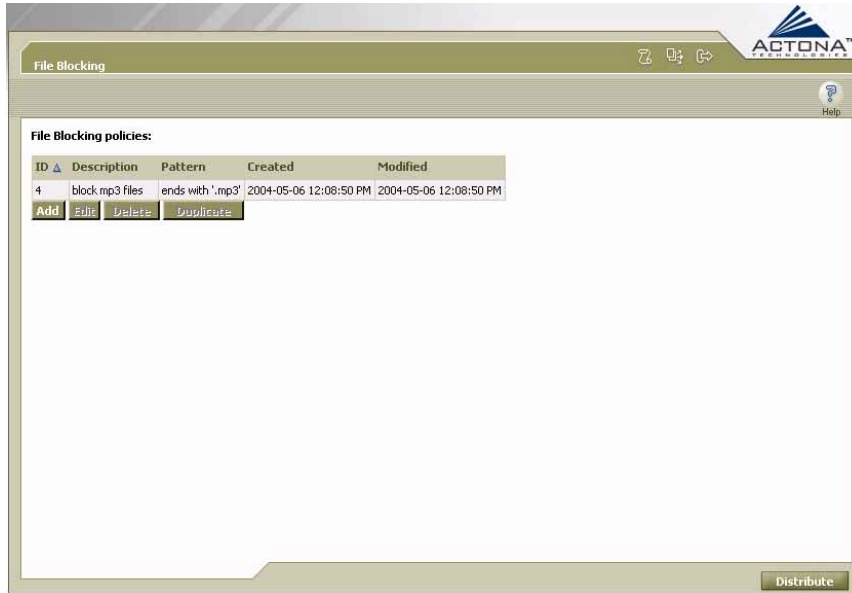
For example, if a file blocking policy regarding MP3 files is defined, all users connected to the ActaStor network will be unable to create, open or copy these files using the EdgeServer cache. The only action permitted to users is to delete these files.



**NOTE:**

Files blocked by ActaStor can be accessed only via direct access to the original file server.

When you select **File Blocking** in the navigation area of the Tasks view, the *File Blocking* page, showing a list of existing file blocking policies in the ActaStor network is displayed, as shown below.



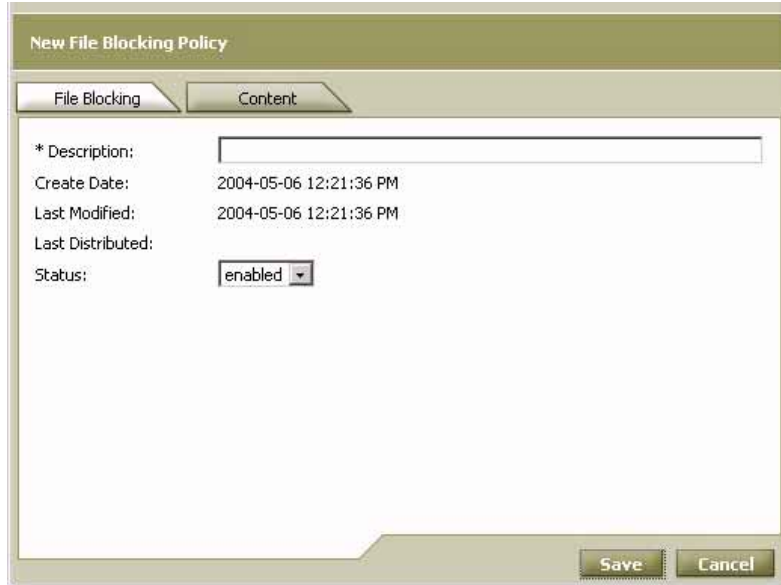
**Figure 5-30: File Blocking Page**

The following information is displayed about each file blocking policy:

- ▲ **ID:** The number assigned by the Central Manager to the file blocking policy.
- ▲ **Description:** A brief description of the policy.
- ▲ **Pattern:** The file pattern blocked by the policy.
- ▲ **Created:** The date when the policy was created.
- ▲ **Modified:** The date when the policy was last modified.

➤ **To define file blocking policies:**

- 1 From the *File Blocking* page, click **Add** to display the following popup window:



**New File Blocking Policy**

File Blocking | Content

\* Description:

Create Date: 2004-05-06 12:21:36 PM

Last Modified: 2004-05-06 12:21:36 PM

Last Distributed:

Status:

Save Cancel

**Figure 5-31: New File Blocking Policy Window**

The *New File Blocking Policy* window contains the following tabs:

- **File Blocking:** For entering a description of the policy and selecting its status.
  - **Content:** For selecting the file pattern to be blocked by the policy.
- 2 Define the following information in the **File Blocking** tab:
    - In the **Description** field, enter a name for the policy.
    - From the **Status** dropdown list, select the status of the policy: **enabled** or **disabled**. Disabled policies are not put into effect.

- 3 Click the **Content** tab to display the following:



**Figure 5-32: New File Blocking Policy Window – Content Tab**

- 4 Select one of the following matching patterns from the dropdown list:
  - **is**
  - **starts with**
  - **ends with**
  - **contains**
- 5 In the field to the right of the dropdown list, complete the file pattern definition. For example, if **ends with** is selected from the dropdown 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.

- 6 Click **Save**. The policy is added to the table on the *File Blocking* page.

**NOTE:**



The new policy takes effect only after it is distributed throughout the ActaStor network. For more information, refer to *Managing Distributions*, page 5-7.

- 7 Repeat steps 1 through 6 for each new file blocking policy you want to define.
- 8 Click **Distribute** to update the affected gateways.

## Editing a File Blocking Policy

The properties of a file blocking policy may be modified at any time. Modifications must be distributed in order to take effect.

### ➤ To edit a file blocking policy:

- 1 From the *File Blocking* page, select a pre-position policy from the list and click **Edit**. The *Edit File Blocking Policy* window is displayed. (This resembles the *New File Blocking Policy* window, as shown on page 5-51.)
- 2 Edit the properties of the policy, as required.
- 3 Click **Save**. The modified policy is saved.
- 4 Click **Distribute** to update the affected gateways.

## Duplicating a File Blocking Policy

An existing file blocking policy can be duplicated in order to use it as a base for a new policy.

➤ **To duplicate a file blocking policy:**

- 1 From the *File Blocking* page, select a policy from the list and click **Duplicate**. The *New File Blocking Policy* window is displayed, as shown on page 5-51. The fields are predefined based on the properties of the policy that was duplicated.
- 2 Edit the properties of the policy as required.
- 3 Click **Save**. The new policy is saved.
- 4 Click **Distribute** to update the affected gateways.

## Deleting a File Blocking Policy

File blocking policies may be deleted at any time. Deletions must be distributed in order to take effect.

➤ **To delete a file blocking policy:**

- 1 From the *File Blocking* page, select a policy from the list and click **Delete**. The selected policy is deleted from the list.
- 2 Click **Distribute** to update the affected gateways.

## Defining Replication Policies

The **Replication** option in the Tasks view enables you to define one or more replication policies that determine how to physically copy files from one site to another in order to back up local copies of the data. Replication is typically used in two scenarios. In one scenario, you replicate the data in a local file server to the central storage facility of your organization, where it can be backed up by existing backup services. In another scenario, you replicate files directly from the central storage facility that must be accessible locally and not accessed through the EdgeServer cache.

Replication is always performed by two ActaStor gateways working together, as follows:

- ▶ **Source gateway:** Provides the files for replicating data.
- ▶ **Target gateway:** Initiates the replication process and receives the files provided by the source gateway.

Any gateway, regardless of its other roles, can include the Replication component and act as either a source gateway, target gateway or both. For more information, refer to *Selecting Roles*, in *Chapter 3, Installation and Deployment*.

When defining a replication policy, you must select the replication-enabled gateways that will act as the source and target. You then select the source and destination file servers for the task, including the share, directory and any required identification information. The replication policy can then be scheduled to run at defined intervals.

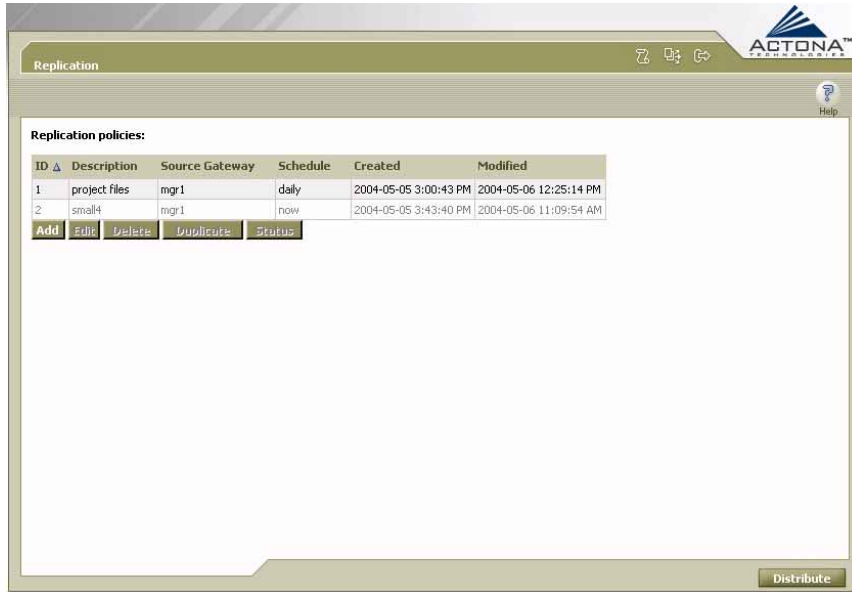
 **NOTE:**

The Replication component must be running on both the source gateway and the destination gateway before you can manage replication tasks.

Replication policies can be scheduled to run either once or on a recurring basis, based on time of day, days of the week or days of the month. When the activation time of a policy arrives, a replication task is initiated in the target gateways to which it has been assigned. Each policy task can be monitored in either the Central Manager or the Gateway Manager, both during and after processing. Active tasks can be terminated if required, as described in *Chapter 4, Gateway Management*. For more information about replication, refer to *Chapter 2, Getting Started*.



When you select **Replication** in the navigation area of the Tasks view, the *Replication* page, showing a list of existing replication policies in the ActaStor network is displayed, as shown below.



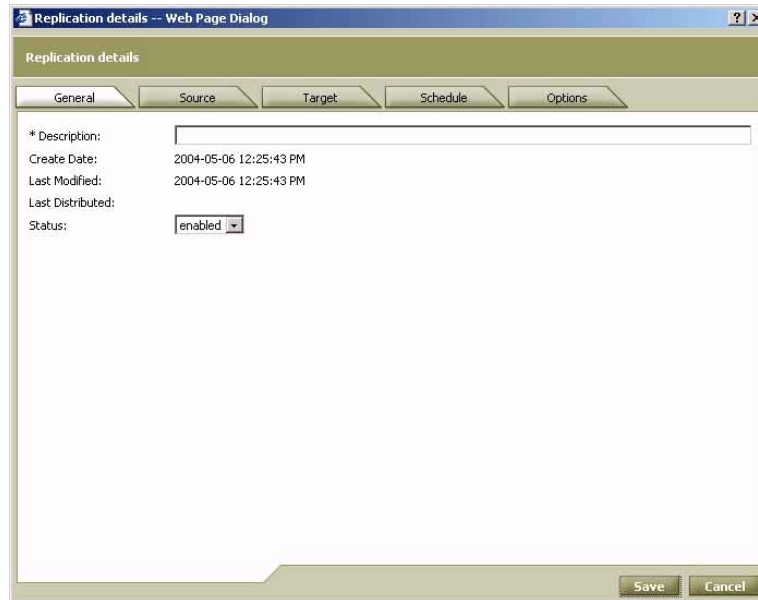
**Figure 5-33: Replication Page**

The following information is displayed about each replication policy:

- **ID:** The number assigned by the Central Manager to the pre-position policy.
- **Description:** A brief description of the policy.
- **Source Gateway:** The gateway providing the files to be replicated.
- **Schedule:** The type of schedule (daily, weekly, and so on) set for the policy.
- **Created:** The date when the policy was created.
- **Modified:** The date when the policy was last modified.

➤ **To define replication policies:**

- 1 From the *Replication* page, click **Add** to display the following popup window:

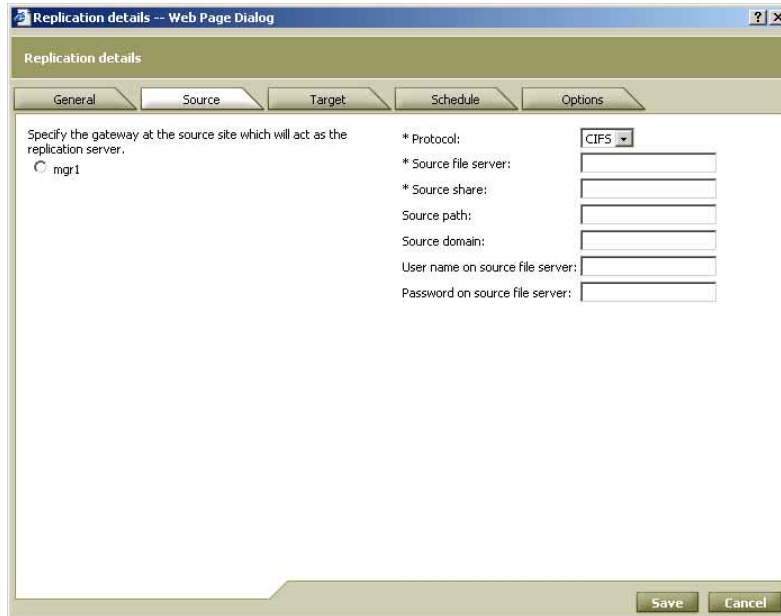


**Figure 5-34: Replication Details Window – General Tab**

The *Replication details* window contains the following tabs:

- **General:** For entering a description of the policy and selecting its status.
- **Source:** For selecting the gateway, file server and path at the source site that is the source for the replication task.
- **Target:** For selecting the gateway, file server and path at the target site that is the destination for the replication task.
- **Schedule:** For defining when and how often the policy is to be run.
- **Options:** For selecting various options affecting how the selected files are replicated.

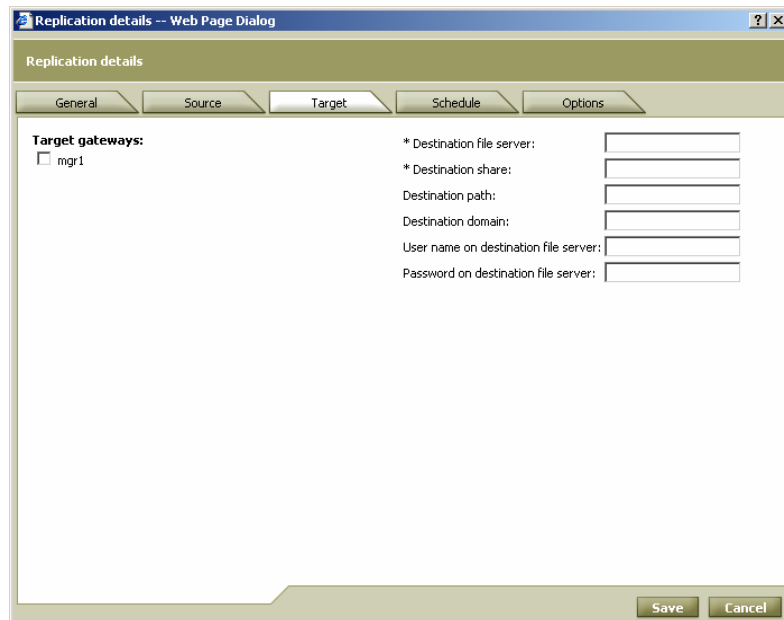
- 2 Define the following information in the **General** tab:
  - In the **Description** field, enter a name for the policy.
  - From the **Status** dropdown list, select the status of the policy: **enabled** or **disabled**. Disabled policies are not put into effect.
- 3 Click the **Source** tab to display the following:



**Figure 5-35: Replication Details Window – Source Tab**

- 4 On the left side of the tab, select the gateway that will act as the source gateway for the replication policy. Only gateways in the network that have been defined with a replication role are listed.
- 5 From the **Protocol** dropdown list, select the relevant file server protocol, **CIFS** (Windows) or **NFS** (UNIX).

- 6 Enter the following information about the source file server for the replication task in the fields provided:
  - **File server**
  - **Share**
  - **Path** (optional; if left blank, the whole share is replicated)
  - **Domain**
  - **User name** (CIFS only)
  - **Password** (CIFS only)
  
- 7 Click the **Target** tab to display the following:



**Figure 5-36: Replication Details Window – Target Tab**



**NOTE:**

Replication Share and Path names are case sensitive. When you set up the WAFS ActaStor replication directive, make sure that the Share and Path information in the Source and Target tabs is the same as the Share and Directory paths in Windows for case sensitivity. Otherwise, the replication will fail.

- 8 On the left side of the tab, select the gateway that will act as the target for the replication policy. Only gateways in the network that have been defined with a replication role are listed.
- 9 Enter the following information about the target file server for the replication task in the fields provided:
  - **File server**
  - **Share**
  - **Path** (optional; if left blank, the target is the root directory of the share)
  - **Domain**
  - **User name** (CIFS only)
  - **Password** (CIFS only)
- 10 Click the **Schedule** tab to display the following:

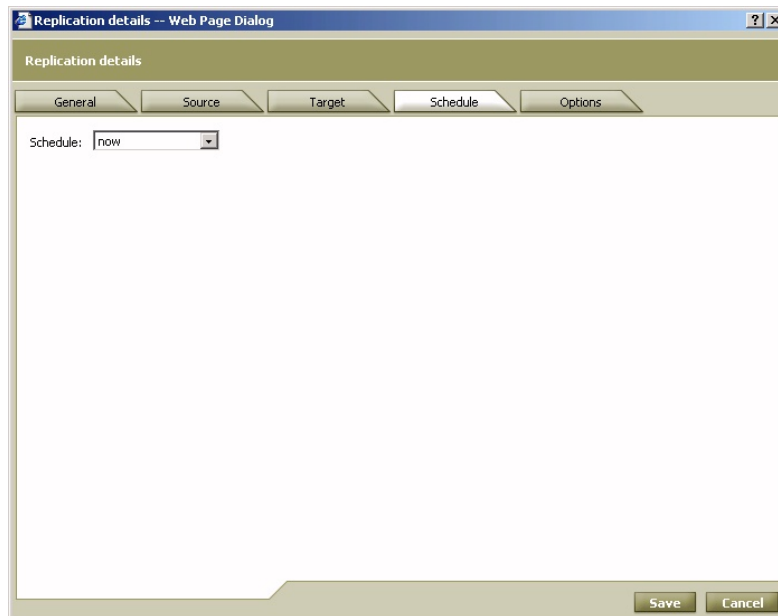


Figure 5-37: Replication Details Window – Schedule Tab

- 11 From the **Schedule** dropdown list, select one of the following scheduling options:
- **now:** The task defined by the policy is run as soon as it is distributed to the relevant gateways.
  - **date:** The task is run once at a defined time and date.
  - **daily:** The task is run daily at a defined time.
  - **weekly:** The task is run on selected days of the week at a defined time.
  - **monthly, days:** The task is run on selected days of the month at a defined time.
  - **monthly, weekday:** The task is run on a defined day (as opposed to a defined date) and time during the month.

**NOTE:**



The fields displayed in the **Schedule** tab reflect the choice selected from the **Schedule** dropdown list. For more information regarding policy scheduling, refer to page 5-45.

- 12 Click the **Options** tab to display the following:

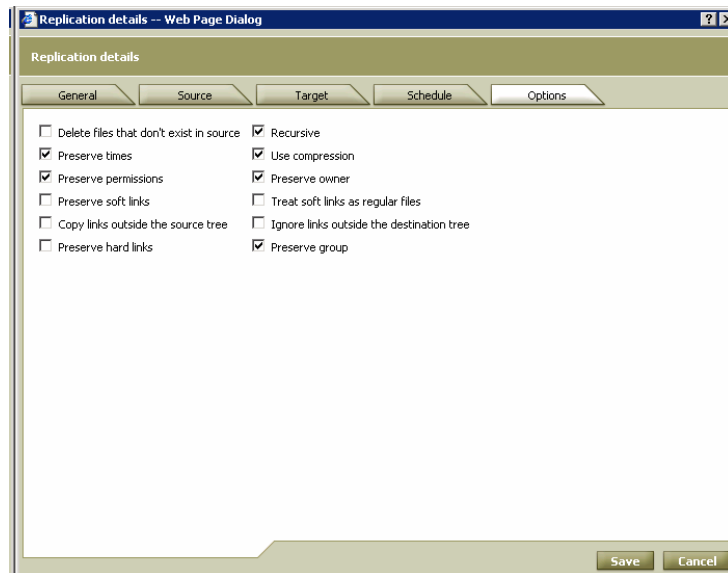


Figure 5-38: Replication Details Window – Options Tab

**13** In the **Options** tab, select any of the following checkboxes, as required:

<b>CIFS &amp; NFS Fields</b>	<b>Description</b>
Preserve times	Maintains the modification date and time of the content being replicated.
Recursive	Includes all subfolders of the selected folder in the replication.
Use compression	Uses file compression during the replication process.
Delete files that don't exist in source	Delete any files from the destination server that have been removed from the source. This is useful when content that has been replicated on a regular basis is deleted from the source.

<b>NFS-only Fields</b>	<b>Description</b>
Preserve permissions	Recreates the permissions to each file and folder on the destination server.
Preserve group	Recreates the group to which each file and folder belongs on the destination server.
Preserve owner	Recreates the owner of each file and folder on the destination server.
Preserve soft links	Recreates symbolic links on the destination server. If this option is not selected, the links are ignored.

NFS-only Fields	Description
Copy links outside the source tree	Treats symbolic links that point outside the source tree as ordinary files.
Preserve hard links	Recreates hard links on the destination server. If this option is not selected, the link is copied as an ordinary file.
Treat soft links as regular files	Treats symbolic links as ordinary files, that is, it copies the original file (whether within or outside of the source tree).
Ignore links outside the destination tree	Ignores any links in the source tree that point outside the destination tree, thus keeping the original destination tree intact.

**NOTES:**



Replicated files have the same replicating user as the owner. Permissions are not inherited; they are inherited from the parent NTFS folder in the destination server.

- 14** Click **Save**. The policy is added to the table on the *Replication* page.

**NOTE:**



The new policy takes effect only when distributed to the relevant EdgeServers. For more information, refer to *Managing Distributions*, page 5-7.

- 15** Repeat steps 1 through 14 for each new replication policy you want to define.



**16** Click **Distribute** to update the affected gateways.

#### NOTES:



To view the current status and history of a selected replication policy, select it in the table on the *Replication* page and click **Status**.

The current status and history of replication policies assigned to a particular EdgeServer can also be viewed using the Gateway Manager. In addition, any replication tasks currently being run can be terminated, if required. For more information, refer to *Managing the Replication Component* in *Chapter 4, Gateway Management*.

## Editing a Replication Policy

The properties of a replication policy may be modified at any time. Modifications must be distributed in order to take effect.

### ➤ To edit a replication policy:

- 1** From the *Replication* page, select a replication policy from the list and click **Edit**. The *Replication details* window is displayed, as shown on page 5-57.
- 2** Edit the properties of the policy, as required.
- 3** Click **Save**. The modified policy is saved.
- 4** Click **Distribute** to update the affected gateways.

#### NOTE:



Changing the status of a replication policy to **disabled** terminates the current task generated by that policy.

## Duplicating a Replication Policy

An existing replication policy can be duplicated in order to use it as a base for a new policy.

### ➤ To duplicate a replication policy:

- 1 From the *Replication* page, select a policy from the list and click **Duplicate**. The *Replication details* window is displayed, as shown on page 5-57. The fields are predefined based on the properties of the policy that was duplicated.
- 2 Edit the properties of the policy as required.
- 3 Click **Save**. The new policy is saved.
- 4 Click **Distribute** to update the affected gateways.

## Deleting a Replication Policy

Replication policies may be deleted at any time. Deletions must be distributed in order to take effect.

### ➤ To delete a replication policy:

- 1 From the *Replication* page, select a policy from the list and click **Delete**. The selected policy is deleted from the list.
- 2 Click **Distribute** to update the affected gateways.




#### NOTE:

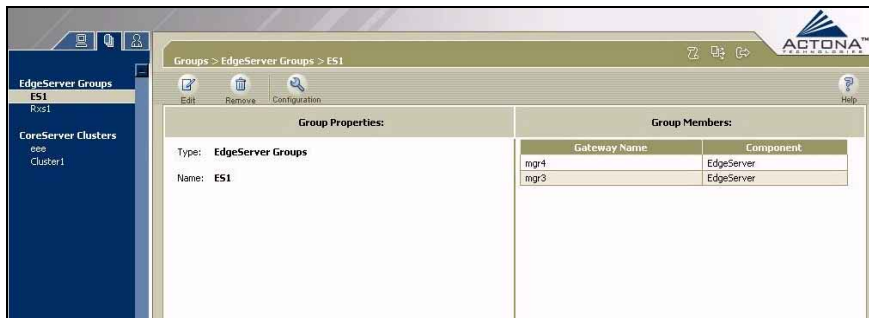
Deleting a pre-position policy terminates the current task generated by that policy.

# Managing Groups

The Groups view enables you to define groups of ActaStor gateways and settings for them. After gateways have been assigned roles in the Setup Wizard (as described in *Chapter 3, Installation and Deployment*), you can define any number of gateways as a group using the Central Manager. This simplifies individual gateway management and streamlines configuration settings, such as connectivity settings, as well as coherency and pre-position policies. You can configure groups according to role, geographical location, and so on.


Group management also enables you to simultaneously apply configuration changes and policy definitions to all the gateways in a group, instead of individually to each gateway.


To access the Groups view, click the **Groups**  tab in the navigation area.



**Figure 5-39: Groups View**

The Groups view includes the following options:


- 
**EdgeServer Groups:** Enables you to group and configure multiple EdgeServers at the same time. For more information, refer to *Defining EdgeServer Groups*, page 5-67.

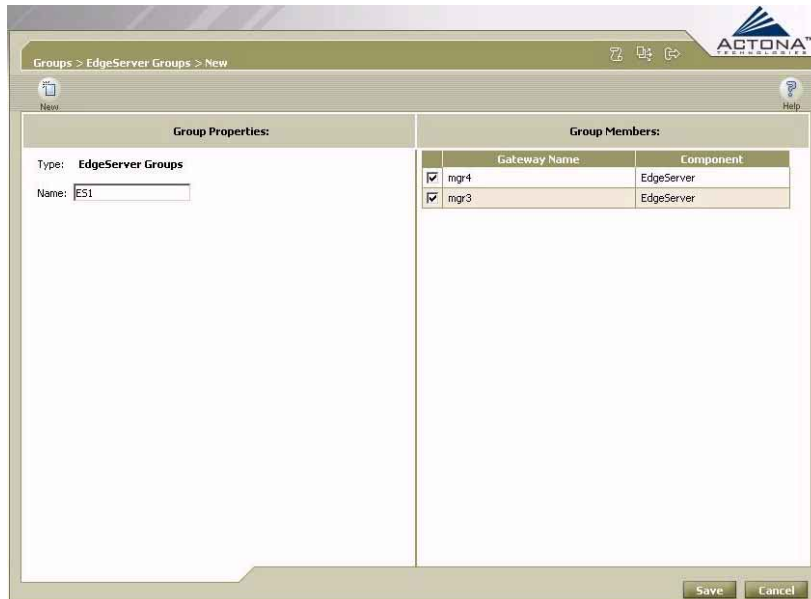
- 
**CoreServer Clusters:** Enables you to define groups of CoreServers as CoreServer clusters. For more information, refer to *Defining CoreServer Clusters*, page 5-74.

## Defining EdgeServer Groups

You can add, edit and delete EdgeServer groups, as required. After a new EdgeServer group has been defined, you can define selected configuration settings for the entire group.

### ➤ To define EdgeServer groups:

- 1 In the navigation area, select **EdgeServer Groups**.
- 2 Click **New**  to display the following:



Group Properties:		Group Members:	
Type:	EdgeServer Groups	Gateway Name	Component
Name:	ES1	<input checked="" type="checkbox"/> mgr4	EdgeServer
		<input checked="" type="checkbox"/> mgr3	EdgeServer

Figure 5-40: EdgeServer Groups Page

The *EdgeServer Groups* page is divided into two areas:

- **Group Properties:** Defines the name of the group.
  - **Group Members:** Lists the available EdgeServers from which you select members to include in the new group.
- 3** In the **Group Properties** area, enter a name for the new EdgeServer group in the **Name** field.
  - 4** In the **Group Members** area, select the checkbox next to each EdgeServer you want to include as a member of the new EdgeServer group. Each EdgeServer can be a member of multiple groups.
  - 5** Click **Save**. The new group is created and added to the list of **EdgeServer Groups** in the navigation area on the *Groups View* page.

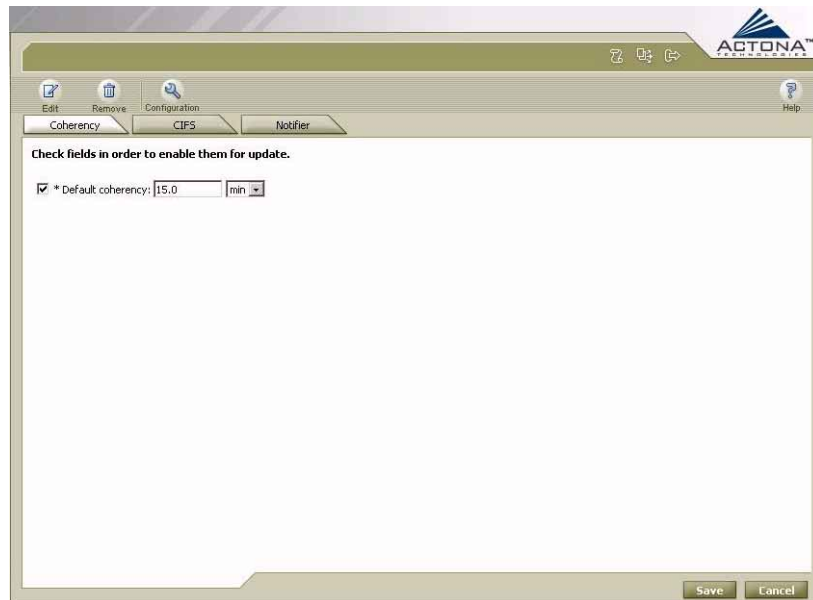
After a new EdgeServer group has been created, you can configure all group members together, as described in the section that follows.

## Defining Configuration Settings for EdgeServer Groups

You can define configuration settings, such as the default coherency, CIFS-related parameters and event notification settings, for the EdgeServers in a group. When configuring EdgeServers as a group, any configuration changes you make override the settings previously defined for the individual EdgeServers. If changes are later made to an individual EdgeServer using the Gateway Manager, these modifications override the group settings defined here.

➤ **To define configuration settings for an EdgeServer group:**

- 1 In the navigation area of the **Groups** tab, select an EdgeServer group and click **Configuration**  to display the following:



**Figure 5-41: EdgeServer Groups Configuration – Coherency Tab**

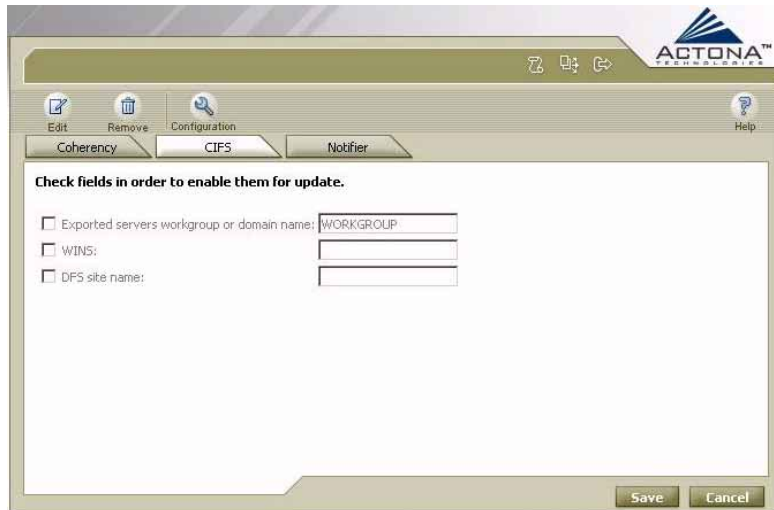
The **EdgeServer Groups Configuration** option includes the following tabs:

- **Coherency:** Enables you to define the default coherency age for the cache contents of all the members of this EdgeServer group. For more information, refer to *Chapter 1, Introduction* and *Chapter 4, Gateway Management*.
- **CIFS:** Enables you to define CIFS-related parameters for each of the members of the group. For more information, refer to *Chapter 3, Installation and Deployment*.

- **Notifier:** Enables you to configure parameters for email notifications that are sent when alerts are generated by member of this EdgeServer group. For more information, refer to *Chapter 3, Installation and Deployment*.

When you display these tabs, the fields contain default values and are disabled. In order to change any of the values, you must first select the checkbox next to the field to enable it. This ensures that only the selected fields are updated in the target gateways.

- 2** In the **Default coherency** field of the **Coherency** tab, enter the time interval for age-based validation and select a time unit from the dropdown list.
- 3** Click the **CIFS** tab to display the following:



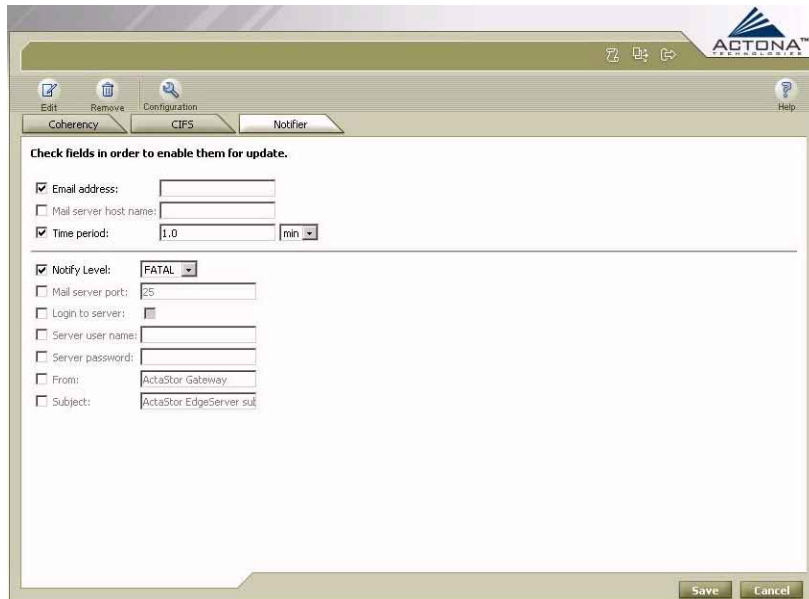
The screenshot shows a web-based configuration interface for Actona Technologies. The interface has a top navigation bar with the Actona logo and icons for Edit, Remove, Configuration, and Help. Below the navigation bar are three tabs: Coherency, CIFS, and Notifier. The CIFS tab is currently selected. The main content area contains a heading "Check fields in order to enable them for update." followed by three checkboxes and text input fields:

- Exported servers workgroup or domain name: WORKGROUP
- WINS:
- DFS site name:

At the bottom right of the form are "Save" and "Cancel" buttons.

**Figure 5-42: EdgeServer Groups Configuration – CIFS Tab**

- 4 Define the following information:
  - In the **Exported servers workgroup or domain name** field, enter the name of the Windows workgroup or domain to which members of this EdgeServer group will belong. When end users connect to these EdgeServers to view information on the file servers, the file servers will appear to the users as members of this workgroup/domain.
  - In the **WINS** field, enter the name or IP address of the WINS server on the LAN, if any.
  - In the **DFS site name** field, enter the name of the site where the EdgeServer is located. This site name, which is typically found in the Active Directory, is used in DFS target selection.
- 5 Click the **Notifier** tab to display the following:



The screenshot shows the 'Notifier' configuration tab in the Actona management interface. The interface includes a top navigation bar with 'Edit', 'Remove', 'Configuration', and 'Help' buttons. Below the navigation bar, there are tabs for 'Coherency', 'CIFS', and 'Notifier'. The 'Notifier' tab is active, displaying a list of configuration options with checkboxes and input fields. The options are:

- Email address: [text input]
- Mail server host name: [text input]
- Time period: [1.0] [min] [dropdown]
- Notify Level: [FATAL] [dropdown]
- Mail server port: [25] [text input]
- Login to server: [checkbox]
- Server user name: [text input]
- Server password: [text input]
- From: [ActaStor Gateway] [text input]
- Subject: [ActaStor EdgeServer.su] [text input]

At the bottom right of the configuration area, there are 'Save' and 'Cancel' buttons.

**Figure 5-43: EdgeServer Groups Configuration – Notifier Tab**



- 6 Define the following information:
  - In the **Email address** field, enter the address to which notifications about members of this EdgeServer group should be sent. This setting overrides the recipient defined when these EdgeServers were deployed, as described in *Chapter 3, Installation and Deployment*.
  - In the **Mail server host name** field, enter the name of the mail server host.
  - In the **Time period** field, enter the time interval for notifications to accumulate until they are sent via email, and select the relevant time unit from the dropdown list, **min** or **sec**.
  - From the **Notify Level** dropdown list, select the minimum event severity level for generating notifications.
  - In the **Mail server port** field, enter the port number for connecting with the mail server.
  - Select the **Login to server** checkbox if the gateway must log in to the mail server in order to send notifications. If this option is selected, additional fields are enabled, as described below.
  - In the **Server user name** field, enter the user name for accessing the mail server.
  - In the **Server password** field, enter the password for accessing the mail server.
  - In the **From** field, enter the text that should appear in the From field of each email notification.
  - In the **Subject** field, enter the text that should appear as the subject of each notification.

- 7 Click **Save**. The configuration settings are saved and distributed to the affected gateways.

**NOTE:**




If a field is enabled, but the default value is not changed, clicking **Save** sends that default value to each EdgeServer in the group. This can be used to restore a default value to an EdgeServer that had one of its properties modified in the Gateway Manager.

## Editing an EdgeServer Group

The properties of an EdgeServer group may be modified at any time.


➤ **To edit an EdgeServer group:**

- 1 Select an EdgeServer group in the navigation area, and then click **Edit** .
- 2 Edit the properties of the group, as required.
- 3 Click **Save**. The modified group is saved and the changes are distributed to the affected gateways.

## Deleting an EdgeServer Group

EdgeServer groups may be deleted at any time. Deleting a group does not delete the individual EdgeServers in the group.

➤ **To delete an EdgeServer group:**

Select an EdgeServer group in the navigation area, and then click **Remove** . The selected group is deleted.

**NOTE:**



Any coherency or pre-position policies defined for the deleted group become invalid and are displayed in red on the *Coherency* and *Pre-position* pages.


## Defining CoreServer Clusters

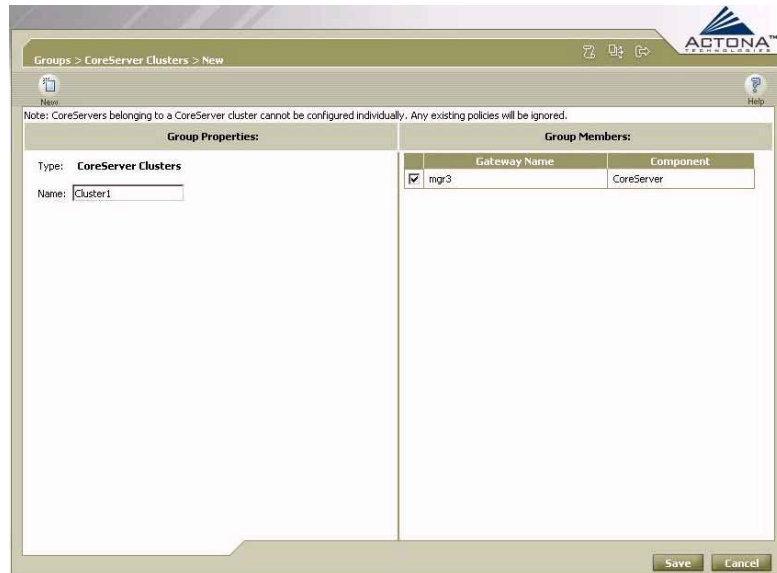
A CoreServer cluster is a group of CoreServers connected to the same file servers that act as a single, logical CoreServer. It provides a high-availability failover capability that minimizes the probability and duration of CoreServer downtime. When a specific CoreServer in the CoreServer cluster fails, all EdgeServers connected to it are redirected to other CoreServers in the cluster, maintaining high availability. Each CoreServer can only be included in one CoreServer cluster.

After a new CoreServer cluster has been defined, you can define which file servers are exported by the cluster, as described in *Defining Configuration Settings for CoreServer Clusters*, page 5-76.

Settings defined for a cluster override any settings made previously to an individual CoreServer in the cluster. You can add, edit and delete CoreServer clusters.

➤ **To define CoreServer clusters:**

- 1 In the navigation area, click **CoreServer Clusters**.
- 2 Click **New**  to display the following:



Groups > CoreServer Clusters > New

Note: CoreServers belonging to a CoreServer cluster cannot be configured individually. Any existing policies will be ignored.

Group Properties:		Group Members:	
Type:	CoreServer Clusters	Gateway Name	Component
Name:	Cluster1	<input checked="" type="checkbox"/> mgr3	CoreServer

Save Cancel

**Figure 5-44: CoreServer Clusters Page**

The *CoreServer Clusters* page is divided into two areas:

- **Group Properties:** Defines the name of the cluster.
  - **Group Members:** Lists the available CoreServers from which you select members to include in the new cluster.
- 3 In the **Group Properties** area, enter a name for the new CoreServer cluster in the **Name** field.
  - 4 In the **Group Members** area, select the checkbox next to each CoreServer you want to include as a member of the new cluster. Only CoreServers that have not yet been defined as members of another CoreServer cluster are displayed.

- 5 Click **Save**. The new cluster is added to the list of CoreServer clusters in the navigation area on the *Groups View* page.

After a new CoreServer cluster has been created, you can define configuration settings for it, as described in the section that follows.

## Defining Configuration Settings for CoreServer Clusters

You can define the file servers to which the CoreServers in a cluster are connected, as well as the email notification settings for the members of this cluster. When configuring CoreServers as a cluster, any configuration changes that you make override the settings previously defined for the individual CoreServers. If changes are later made to an individual CoreServer using the Gateway Manager, these modifications override the cluster settings defined here.

### ➤ To define configuration settings for CoreServer clusters:

- 1 In the navigation area of the **Groups** tab, select a CoreServer cluster and click **Configuration**  to display the following:

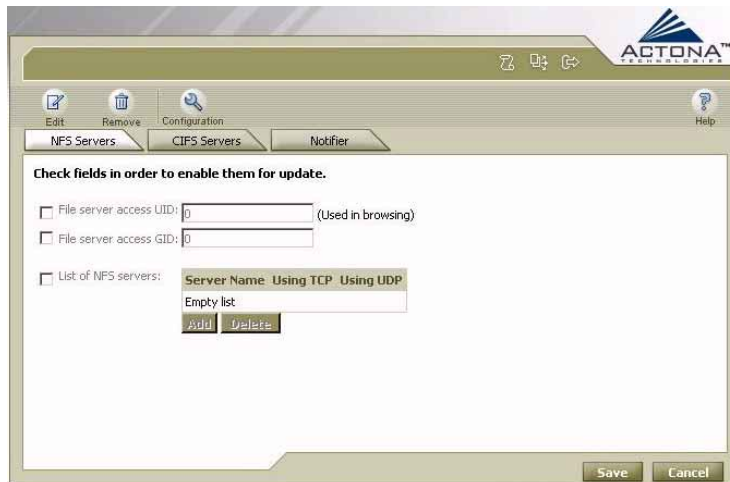


Figure 5-45: CoreServer Cluster Configuration

The **CoreServer Cluster Configuration** option includes the following tabs:

- **NFS Servers:** Enables you to define the NFS file servers to which the cluster connects.
- **CIFS Servers:** Enables you to define the CIFS file servers to which the cluster connects.
- **Notifier:** Enables you to configure parameters for email notifications that are sent when alerts are generated by members of this CoreServer cluster. For more information, refer to *Chapter 3, Installation and Deployment*.

When you display these tabs, the fields contain default values and are disabled. In order to change any of the values, you must first select the checkbox next to the field to enable it. This ensures that only the selected fields are updated in the target gateways.

**2** Define the following information in the **NFS Servers** tab:

- In the **File server access UID** field, enter the user ID the CoreServers will use for browsing NFS file servers. This user ID is used for all NFS file servers connected to this CoreServer cluster.
- In the **File server access GID** field, enter the group ID the CoreServers will use for browsing NFS file servers. This group ID is used for all NFS file servers connected to this CoreServer cluster.

**NOTE:**



The UID and GID are required for browsing during policy definition in the Central Manager.

- In the **List of NFS servers** field, click **Add** to display the following:



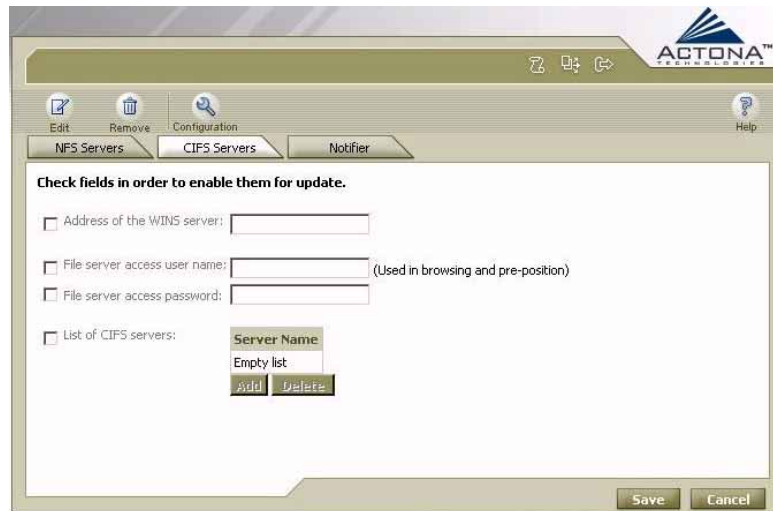
**Figure 5-46: New NFS File Server Window**

- Define the new file server, as follows:
  - In the **Server Name** field, enter the name of the file server.
  - Select the checkboxes for the appropriate connection protocols used by the file server, **Using TCP** or **Using UDP**. At least one option should be selected.
  - Click **Ok**. The file server is added to the list in the **NFS Servers** tab.
- Repeat the steps defined above to add more NFS file servers, if required.

**NOTE:**

The list of file servers entered here overrides the existing list defined for each CoreServer in the cluster.

- 3 Click the **CIFS Servers** tab to display the following:



**Figure 5-47: CoreServer Clusters – CIFS Servers Tab**

- 4 Define the following information:
- In the **Address of the WINS server** field, enter the name or IP address of the WINS server, if any.
  - In the **File server access user name** field, enter the user name the CoreServers will use for browsing CIFS file servers. This user name is used for all CIFS file servers connected to this CoreServer cluster. The format of the user name is: [**<domain>**]\<user name>. (Enter the domain if this is not a local user.)
  - In the **File server access password** field, enter the password the CoreServers will use for browsing CIFS file servers. This password is used for all CIFS file servers connected to this CoreServer cluster.



**NOTE:**

The user name and password are required for browsing during policy definition in the Central Manager and for executing pre-position policies in the EdgeServer.



- In the **List of CIFS servers** field, click **Add** to display the following:



**Figure 5-48: New CIFS File Server Window**

- Define the new file server, as follows:
  - In the **Server Name** field, enter the name of the file server.
  - Click **Ok**. The file server is added to the list in the **CIFS Servers** tab.
- Repeat the steps defined above to add more CIFS file servers, if required.

**NOTE:**

The list of file servers entered here overrides the existing list defined for each CoreServer in the cluster.

- 5** Click the **Notifier** tab and modify the fields displayed, as described on page 5-71.

- 6 Click **Save**. The configuration settings are saved and distributed to the affected gateways.




**NOTE:**

If a field is enabled, but the default value is not changed, clicking **Save** sends that default value to each CoreServer in the cluster. This can be used to restore a default value to a CoreServer that had one of its properties modified in the Gateway Manager.

## Editing a CoreServer Cluster

The properties of a CoreServer cluster may be modified at any time.


➤ **To edit a CoreServer cluster:**

- 1 Select a CoreServer cluster in the navigation area, and then click **Edit** .
- 2 Edit the properties of the cluster, as required.
- 3 Click **Save**. The modified cluster is saved and the changes are distributed to the affected gateways.

## Deleting a CoreServer Cluster

CoreServer clusters may be deleted at any time. Deleting a cluster does not delete the individual CoreServers in the cluster, but it does free them to be selected as members of other CoreServer clusters.

➤ **To delete a CoreServer cluster:**

Select a CoreServer cluster in the navigation area, and then click **Remove** . The selected cluster is deleted.


# Managing Users

The Users view option in the navigation area enables administrators to manage users of the ActaStor managers. ActaStor manager users are primarily IT personnel with rights to access the Gateway and Central managers.

There are three types of ActaStor manager users:

- **Admin:** Users with full rights to perform all operations on all gateways via the Gateway Manager and Central Manager.
- **Central:** Users who can use Gateway Managers and the Central Manager, but cannot define users within the Central Manager.
- **Gateway:** Users who can access the Gateway Manager for selected gateways. These users do not have access to the Central Manager. When you add new Gateway Manager users, you must specify which gateways the user will be authorized to manage.

You can add, edit and delete users, as required.

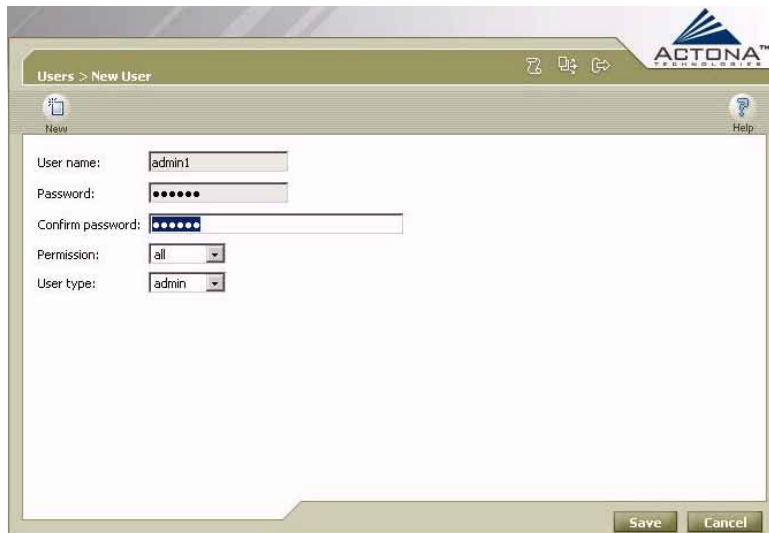
To access the Users view, click the **Users**  tab in the navigation area.

## Adding Users

When adding a new user, you must specify a permissions level and a user type. These two parameters define the actions the new user can take and the gateways on which these actions can be taken.

➤ **To add users:**

- 1 From the Users view, click **New**  to display the following:



**Figure 5-49: New User Page**

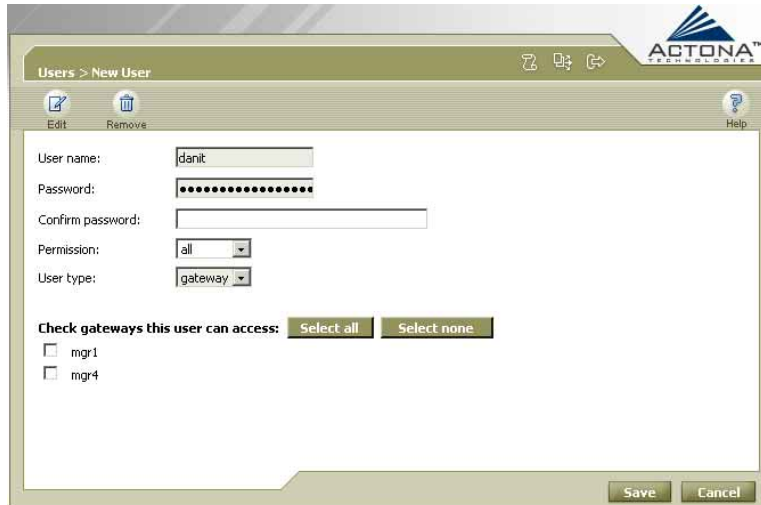
- 2 In the **User name** field, enter a user name for the new user.
- 3 In the **Password** field, enter a password for the new user.

**NOTE:**

The password is case sensitive.

- 4 Confirm the new password by retyping it in the **Confirm password** field.

- 5 From the **Permission** dropdown list, select the level of user permissions for the new user:
  - **All:** Full permissions.
  - **Read Only:** User can view data but cannot change it.
- 6 From the **User type** dropdown list, select the type of user for managing gateways on the ActaStor network:
  - **admin:** Manages all gateways at all levels.
  - **central:** Can access the Central Manager, but cannot define users; can access the Gateway Manager of all gateways.
  - **gateway:** Manages selected Gateway Managers; cannot access the Central Manager.
- 7 If **Gateway** is selected as the user type, a list of all gateways in the ActaStor network is displayed, as shown below.



**Figure 5-50: Defining Gateways to Manage**


- 8 Select the checkbox next to each gateway that can be accessed by the selected Gateway-level user. Click **Select all** if this user will manage all the gateways in the list, or click **Select none** to clear all the checkboxes.

- 9 Click **Save**. The new user is added to the list of users in the navigation area of the Users View.
- 10 Click **Distribute** to distribute the new user information to the appropriate gateways on the ActaStor network.

## Editing Users

User properties may be modified at any time. Modifications must be distributed in order to take effect.


### ➤ To edit a user:

- 1 Select a user in the navigation area, and then click **Edit** .
- 2 Edit the properties of the user, as required.
- 3 Click **Save**. The modified user is saved.
- 4 Click **Distribute** to distribute the modifications to the appropriate gateways.

## Deleting Users

Users may be deleted at any time. Deletions must be distributed in order to take effect.

### ➤ To delete a user:

- 1 Select a user in the navigation area, and then click **Remove** . The selected user is deleted.
- 2 Click **Distribute** to distribute the deletion to the appropriate gateways.



## Chapter 6

# Troubleshooting

### ABOUT THIS CHAPTER

This chapter describes various troubleshooting issues that may arise in your system, the symptoms or problems that may occur and the various checks and actions you can perform to help resolve them. It includes the following sections:

- ▶ **Getting Technical Assistance**, beginning on page 6-2, describes how to contact Actona for troubleshooting help.
- ▶ **Installation and Setup Issues**, beginning on page 6-3, describes common troubleshooting procedures regarding ActaStor installation and setup.
- ▶ **ActaStor Manager Issues**, beginning on page 6-6, describes common troubleshooting procedures for the Gateway Manager and Central Manager.
- ▶ **Client Operation Issues**, beginning on page 6-9, describes common troubleshooting procedures regarding client operation.

The issues that are described in this chapter can occur at any stage of ActaStor operation, such as:

- ▶ Initial appliance setup
- ▶ First-time configuration with the Setup Wizard
- ▶ Client attempts to connect to the EdgeServer
- ▶ Client operation



# Getting Technical Assistance

If you encounter problems that cannot be resolved using this guide, contact Cisco Technical Support:

Email: [tac@cisco.com](mailto:tac@cisco.com)  
Web: [www.cisco.com](http://www.cisco.com)  
Phone: 1 (408) 526-4000

When contacting Cisco Support, it is important to provide as much data as possible, including data from both the EdgeServer and the CoreServer. This data can be obtained using the System Report utility in the relevant Gateway Managers.

## ➤ **To obtain gateway data for Cisco Support:**

- 1** In the *Utilities* page, click the **Support** tab.
- 2** In the **System Report** section, click **Download**. A file is created containing pertinent data about the gateway.
- 3** Send the downloaded file to Cisco Technical Support.

### **NOTE:**

For more information about the *Utilities* page, refer to *Chapter 4, Gateway Management*.

It is recommended to visit the Cisco Web site periodically for the most up-to-date support information.

# Installation and Setup Issues

Problem	Actions
After connecting to the appliance from the MGR port (eth1), you cannot see the ActaStor Manager using Internet Explorer.	<ul style="list-style-type: none"><li>➤ In Internet Explorer, verify that no proxy is defined and that both JavaScript and cookies are enabled.</li><li>➤ Verify that the URL address is correct: <b>http://172.30.30.172/mgr</b>.</li><li>➤ Verify that the IP of the installation console configuring the appliance is within the range <b>172.30.30.173</b> to <b>172.30.30.177</b> and that the subnet mask is <b>255.255.255.0</b>. If the address is not correct, execute the following command from the client to reset the IP: <code>ipconfig /renew</code></li><li>➤ Verify that you are using a crossover Ethernet cable, or use a switch.</li><li>➤ Verify that the Ethernet cable is connected to the correct port on both the installation console and the appliance. On the appliance, it should be connected to the port labeled <b>MGR</b>.</li><li>➤ Use ping to verify the connection between the installation console and the gateway (<b>172.30.30.172</b>).</li></ul>
Failed to change appliance IP address.	<ul style="list-style-type: none"><li>➤ Check for a conflict between the IP address attempted for the appliance and another computer in the domain.</li></ul>

<b>Problem</b>	<b>Actions</b>
After configuring the network connection for the ActaStor appliance, you cannot reach the ActaStor Manager via the NET port (eth0).	<ul style="list-style-type: none"><li data-bbox="639 312 1213 425">▶ In Internet Explorer, verify that no proxy is defined and that both JavaScript and cookies are enabled.</li><li data-bbox="639 442 1213 555">▶ Verify that the URL address is correct: <b>http://&lt;ip-addr&gt;/mgr</b> or <b>http://&lt;name&gt;/mgr.</b></li><li data-bbox="639 572 1213 651">▶ Verify that you are using a regular (non-crossover) Ethernet cable.</li><li data-bbox="639 668 1213 781">▶ Verify that the Ethernet cable is connected to the port labeled <b>NET</b> on the appliance.</li><li data-bbox="639 798 1213 989">▶ Use ping to verify the connection between the installation console and the gateway. If pinging this appliance fails from the same subnet, check the client's DNS and DHCP settings.</li><li data-bbox="639 1006 1213 1197">▶ Reconnect to the ActaStor Manager via the MGR port, and verify that the appliance network settings are correctly configured, including the IP, net mask, DNS and default gateway.</li></ul>

---

**Problem**

From the Setup Wizard, you issued a registration to the Central Manager, and it failed.

**Actions**

- ▶ On the *Connection to Central Manager* page of the Setup Wizard, verify that the name of the Central Manager (or its IP address) is correct.
  - ▶ Verify that the Central Manager is running. If it is not, start it and try to register the appliance via the **Registration** tab of the Gateway Manager **Control** option.
  - ▶ Make sure the appliance port labeled NET is connected.
  - ▶ Check the DNS server settings for these appliances.
  - ▶ Make sure you can ping the Central Manager gateway from the same subnet where this gateway resides. If pinging fails, verify Ethernet connectivity and proper routing.
  - ▶ To overcome temporary external problems, try registering the appliance again via the **Registration** tab of the Gateway Manager **Control** option.
-

# ActaStor Manager Issues

## Gateway Manager

Problem	Actions
Gateway Manager cannot be accessed or navigated properly.	<ul style="list-style-type: none"> <li>Verify that cookies and JavaScript are active in the Web browser. If a popup blocker is in use, disable it.</li> </ul>

### NOTE:



For troubleshooting tips related to pre-position policies, refer to *Central Manager*, below.

## Central Manager

Problem	Actions
Central Manager cannot be accessed or navigated properly.	<ul style="list-style-type: none"> <li>Verify that cookies and JavaScript are active in the Web browser. If a popup blocker is in use, disable it.</li> </ul>
In the <b>Gateways</b> option of the Tasks view, an appliance is missing even though the appliance registration process ended successfully.	<ul style="list-style-type: none"> <li>From the Central Manager, perform a refresh (press the &lt;F5&gt; key), or click the <b>Refresh</b> button.</li> <li>In the Gateway Manager of the missing appliance, verify that the IP address of the Central Manager is correct and then repeat the registration process.</li> </ul>

<b>Problem</b>	<b>Actions</b>
Distribution (of license, policy and so on) to one or more gateways fails.	<ul style="list-style-type: none"><li>➤ Make sure the gateway is registered with the correct IP.</li><li>➤ Make sure you can ping the failing gateways from the same subnet where the Central Manager gateway resides. If pinging fails, verify Ethernet connectivity and proper routing.</li><li>➤ Check the DNS and DHCP (if applicable) settings of all relevant gateways, including the one running the Central Manager.</li></ul>
File-server directory browsing fails during coherency or pre-position policy definition.	<ul style="list-style-type: none"><li>➤ Make sure the relevant CoreServer and file server are running.</li><li>➤ Verify that the file server is defined correctly in the CoreServer configuration with the appropriate browsing credentials (username/password for CIFS, or UID/GID for NFS).</li><li>➤ Make sure you can access the CoreServer gateway from the domain/subnet of the Central Manager via ping.</li><li>➤ Check the DNS and/or WINS settings on the relevant CoreServer.</li><li>➤ Verify that the file server is accessible from other clients, and that you can access it from the CoreServer domain/subnet (via ping, NFS mount or Windows Explorer) and defined browsing credentials.</li></ul>

Problem	Actions
Pre-position of some files fails due to "Access denied".	▶ Check the permissions of the user defined for browsing and pre-position in the CoreServer.
Pre-positioned files cannot be seen after performing the scheduled task.	▶ Check the status of the task in the Central Manager (or Gateway Manager) to see if the task terminated due to a time or space constraint defined in the policy. Modify the policy, if required.
A newly defined policy or user does not appear or operate as intended.	▶ Click <b>Distribute</b> or <b>Distribute All</b> to update the information in the gateways.
A newly defined replication task fails and displays the message, "[Error] the mount <FS_share> is invalid".	▶ Verify that all replication task parameters (such as, login name, password, file server name, target/source of path and share and so on) are entered correctly, then run the task again. ▶ The failure may be due to an IP conflict. Verify the correlation between the file contents of <b>/etc/hosts</b> and the response received to the command, <b>host &lt;host_name&gt;</b> , when issued from one replication gateway to the other.

# Client Operation Issues

Problem	Actions
Windows client cannot reach the EdgeServer shares.	<ul style="list-style-type: none"><li>▶ Verify the following:<ul style="list-style-type: none"><li>▪ Both the EdgeServers and CoreServers are running.</li><li>▪ Connectivity is defined between the EdgeServers and the CoreServers.</li><li>▪ The required file server is defined for this CoreServer.</li></ul></li><li>▶ Verify that the file server is working properly and that you can access it from the CoreServer domain.</li><li>▶ Verify that the domain/Workgroup of the EdgeServer is accessible to this client.</li><li>▶ If the client and the EdgeServer are <b>not</b> in the same subnet, verify that:<ul style="list-style-type: none"><li>▪ A WINS server is configured for the EdgeServer.</li><li>▪ The client and EdgeServer use the same WINS server, or their WINS servers are defined as replication partners.</li></ul></li></ul>



Problem	Actions
	<ul style="list-style-type: none"> <li> <span data-bbox="625 312 656 338">▶</span> Verify that the client can see the cached server in the network (via the <code>net view</code> command). If not, verify the following:               <ul style="list-style-type: none"> <li> <span data-bbox="671 442 692 468">▪</span> The name of the cached server is <b>prefix + file server name</b>. For example, if you selected <b>domain</b> as the domain, <b>GWprefix-</b> as the EdgeServer prefix and <b>FS</b> as the file-server name, the name of the cached server should be <b>\\GWprefix-FS</b> under the <b>domain</b>.                 </li> <li> <span data-bbox="671 772 692 798">▪</span> Verify that the total length of <b>prefix + original file server name</b> does not exceed 15 characters. If this occurs, the cached server name will be <b>prefix + truncated original name</b>.                 </li> <li> <span data-bbox="671 989 692 1015">▪</span> If the EdgeServer prefix has been changed, make sure the EdgeServer was restarted afterwards.                 </li> </ul> </li> <li> <span data-bbox="625 1119 656 1145">▶</span> The required file server is defined for this CoreServer.             </li> </ul>
<p>Windows client receives “Access denied” when trying to access resources on the cached server.</p>	<ul style="list-style-type: none"> <li> <span data-bbox="625 1215 656 1241">▶</span> Check client permissions to these resources on the original file server (try to access the original file server using these user credentials).             </li> <li> <span data-bbox="625 1380 656 1406">▶</span> Verify that the file you are trying to access does not match a file type/pattern defined in a file blocking policy.             </li> </ul>

Problem	Actions
UNIX client cannot access resources on the cached server.	<ul style="list-style-type: none"><li>▶ Check the client permissions to these server resources.</li><li>▶ Verify that the root squash, GID and UID mapping are correctly defined for the relevant EdgeServer connection.</li></ul>
A file or folder was updated in the file server, but it cannot be seen.	<ul style="list-style-type: none"><li>▶ If the coherency policy used by the client is local or global, the client must wait until the coherency age defined in the EdgeServer expires.</li></ul>
Selected offline files or folders on the file server are missing.	<ul style="list-style-type: none"><li>▶ Right-click the entire offline folders tree in Windows Explorer and select <b>Synchronize</b> from the popup menu.</li></ul>
SNMP administrator does not receive SNMP traps from appliances.	<ul style="list-style-type: none"><li>▶ Verify that the SNMP host is properly configured.</li><li>▶ Change the host to generate a message with the new address.</li></ul>
(Windows XP) Files cached on EdgeServer appear as read-only.	<ul style="list-style-type: none"><li>▶ Install the HotFix patch from Microsoft located at: <a href="http://support.microsoft.com/?kbid=826939">http://support.microsoft.com/?kbid=826939</a></li></ul>



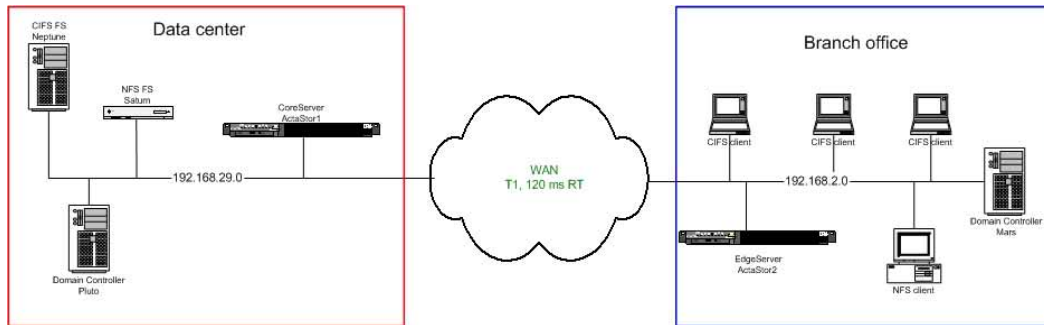
## Appendix A

# Sample Installation

This appendix provides a step-by-step guide for setting up a sample ActaStor network. This sample demonstrates a network comprised of two gateways – a CoreServer residing next to a file server, and an EdgeServer residing in a remote office. A deployment of multiple EdgeServers would be set up in the same manner as described in this example.

The setup example includes a data center and a branch office. The organization has a single DNS domain (us.actona.com) and a single Windows domain (actona-us), where each location is a separate site within the Active Directory. The CoreServer is connected at the data center to two file servers – Neptune, a Windows 2000 server, and Saturn, a Solaris 2.8 server. The clients at the branch office are connected to the EdgeServer.

The following diagram depicts the network setup.



**Figure A-1: Sample Network Setup**

The following table specifies the different parameters and data needed to setup and configure the ActaStor gateways.

Parameter	Data Center		Branch Office	
Network IP	192.168.29.0		192.168.2.0	
Subnet Mask	255.255.255.0		255.255.255.0	
Default Gateway	192.168.29.1		192.168.2.1	
DNS Domain	us.actona.com		us.actona.com	
DNS/WINS Server	Pluto	192.168.29.2	Mars	192.168.2.2
ActaStor Gateway	ActaStor1	192.168.29.50	ActaStor2	192.168.2.11
Windows Domain Controller	Pluto	192.168.29.2	Mars	192.168.2.2
Windows File Server	Neptune	192.168.29.5	N/A	
UNIX File Server	Saturn	192.168.29.6	N/A	

Parameter	Data Center	Branch Office
Windows Clients	N/A	DHCP
UNIX Clients	N/A	DHCP
Windows Domain	actona-us	actona-us

The example installation includes the following steps:

- **Step 1: Unpacking the Hardware**, beginning on page A-4
- **Step 2: Turning on the Appliance**, beginning on page A-4
- **Step 3: Configuring the Client Installation Console**, beginning on page A-5
- **Step 4: Accessing the Setup Wizard**, beginning on page A-6
- **Step 5: Configuring the CoreServer**, beginning on page A-7
- **Step 6: Configuring the EdgeServer**, beginning on page A-13
- **Step 7: Configuring the ActaStor Network with the Central Manager**, beginning on page A-18
- **Step 8: Connecting a Client to the EdgeServer**, beginning on page A-23

# Step 1: Unpacking the Hardware

Prior to installing the ActaStor gateway on your local area network, make sure all the required items are included in the installation package, as described in *Step 1: Unpacking the Hardware* in *Chapter 3, Installation and Deployment*.

➤ **To unpack the hardware:**

- 1 Open the carton and remove the appliance.
- 2 Remove the Ethernet crossover cable.
- 3 If you are mounting the gateway onto a rack, follow the mounting instructions in the attached pamphlet.

# Step 2: Turning on the Appliance

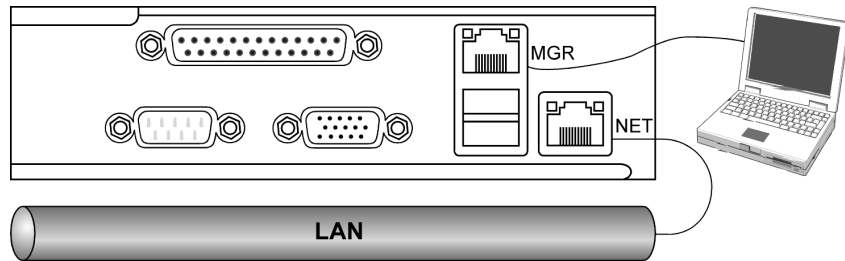
After the gateway is mounted on the rack, you need to connect the power cord and Ethernet crossover cable, and open the front panel to turn on the unit.

For more detailed information, refer to *Step 2: Installing the Appliance* in *Chapter 3, Installation and Deployment*.

➤ **To turn on the appliance:**

- 1 Connect the AC power cable to the power socket on the left side of the rear panel of the appliance.

- 2 Connect one end of the Ethernet crossover cable to the MGR port, and one end of a regular (straight-through) Ethernet cable to the NET port located at the back of the unit, as shown in Figure A-2.



**Figure A-2: System Back-end Connectors**

- 3 Open the front bezel and press the On/Off switch (upper switch).

## Step 3: Configuring the Client Installation Console

After the unit has been turned on, you are ready to configure the client installation console.

➤ **To configure the client installation console:**

On your Windows 2000/XP client, configure the Ethernet port to use DHCP (if not configured already). The ActaStor appliance will provide your client with an IP address, via the DHCP server that is configured on the MGR port.



## Step 4: Accessing the Setup Wizard

This step describes how to access the Setup Wizard using Internet Explorer 5.5 or above.

For more information, refer to *Step 3: Using the Setup Wizard in Chapter 3, Installation and Deployment*.

➤ **To access the Setup Wizard:**

- 1 Open Internet Explorer 5.5 or above and in the address bar, enter the ActaStor Management address **http://172.30.30.172/mgr** to display the *Login* page.
- 2 Enter the default user name (**admin**) and password (**actona**) in the fields provided, and click **Login**.

**NOTE:**

When logging in for the first time to an uninitialized gateway, the first page of the Setup Wizard is displayed automatically.

# Step 5: Configuring the CoreServer

This step describes how to define the CoreServer component of the gateway, and includes the following sections:

- **Defining Local Area Connection Properties**, below
- **Selecting Roles**, page A-8
- **Defining the CoreServer Configuration**, page A-9
- **Defining Notification Settings**, page A-10
- **Registering to the Central Manager**, page A-11

Remember to configure the CoreServer first and designate it as the Central Manager.

For more information, refer to *Step 3: Using the Setup Wizard in Chapter 3, Installation and Deployment*.

## Defining Local Area Connection Properties

This step enables you to configure the appliance for the local area network to which it is being connected.

- **To define the local area connection:**
  - 1 In the *Local Area Connection Properties* page of the Setup Wizard, fill in the fields as follows:
    - Machine name (host name): **ActaStor1**
    - IP address: **192.168.29.50**
    - Net mask: **255.255.255.0**
    - Default GW: **192.168.29.1**
    - Primary DNS: **192.168.29.2**

- Secondary DNS: (not required for this example)
  - DNS domain: **us.actona.com**
- 2** If the system is using DHCP, make sure to create a reservation record for the CoreServer.
  - 3** Click **Next** to proceed to the *System Properties* page of the Setup Wizard.
  - 4** Set the time zone and the date/time of the CoreServer in the fields provided.
  - 5** Click **Next** to proceed to the *Role Selection* page of the Setup Wizard, as described in the section that follows.

## Selecting Roles

This section describes how to select the role of the appliance in the ActaStor network.

➤ **To select roles:**

- 1** In the *Role Selection* page of the Setup Wizard, select the following checkboxes:
  - **CoreServer**
  - **Central Manager**
- 2** Click **Next** to proceed to the next page of the Setup Wizard.

# Defining the CoreServer Configuration

This section enables you to define the file servers (CIFS and NFS) to which this CoreServer will be connected.

## Defining CIFS Servers

This step enables you to define the CIFS file servers that you want the CoreServer to expose, as well as selected parameters required for the connection. Any available share on one of these servers becomes visible to the connected EdgeServers.

For more information, refer to *Defining CIFS Servers* in *Chapter 3, Installation and Deployment*.

### ➤ To define CIFS file servers:

- 1 [Optional] In the *CoreServer Configuration – CIFS* page of the Setup Wizard, enter the WINS server address in the field provided, if WINS is used within the organization.
- 2 In the **Browsing user name** and **password** fields, enter the relevant information. Use any user account with browsing capabilities. This information is required for proper operation of pre-position policies and for browsing the shares when creating coherency policies.
- 3 In the **List of CIFS servers** field, click **Add** and in the popup window displayed, enter **Neptune**. Click **OK**.
- 4 Click **Next** to proceed to the next page of the Setup Wizard.

## Defining NFS Servers

This step enables you to define the NFS file servers that you want the CoreServer to expose, as well as selected parameters required for the connection. For more information, refer to *Defining NFS Servers* in *Chapter 3, Installation and Deployment*.

### ➤ To define NFS servers:

- 1 In the *CoreServer Configuration – NFS* page of the Setup Wizard, enter the required information in the **Browsing UID** and **GID** fields. In most cases, the default values should suffice.
- 2 In the **List of NFS servers** field, click **Add** and in the popup window displayed, enter **Saturn** and select the **Using TCP** and **Using UDP** checkboxes. Click **OK**.
- 3 Click **Next** to proceed to the next page of the Setup Wizard.

## Defining Notification Settings

This step enables you to define the email address to which notifications are sent when alerts are generated by this gateway.

For more information, refer to *Defining Notification Settings* in *Chapter 3, Installation and Deployment*.

### ➤ To define notification settings:

- 1 In the *Notification Setting* page of the Setup Wizard, enter the address to which notifications about this gateway are sent in the **Email address** field.
- 2 In the **Mail server host name** field, enter the name or IP address of the mail server host.
- 3 Click **Next** to proceed to the next page of the Setup Wizard.

## Registering to the Central Manager

This step enables you to define parameters required by the gateway to register to the Central Manager of the ActaStor network.

For more information, refer to *Registering to the Central Manager* in *Chapter 3, Installation and Deployment*.

### ➤ To register the gateway to the Central Manager:

- 1 In the *Connection to Central Manager* page of the Setup Wizard, enter the logical name of the gateway as it will be identified in the ActaStor network in the **Gateway name** field. For this sample installation, enter **ActaStor1**.
- 2 In the **Central host** field, enter the IP address or machine name of the Central Manager. In this example, since the CoreServer is also the Central Manager, enter **192.168.29.50**.
- 3 To ensure the gateway registers with the Central Management Console, select the **Register with central** checkbox.
- 4 Click **Finish** to complete the setup process.

When the process is complete, the **Components** tab of the *Gateway Control* page is displayed, as shown below.



**Figure A-3: Gateway Control Page – Components Tab**

The component that was just configured is marked in red as **not licensed**. After you distribute the license key file from the Central Manager, it will be enabled. For more information, refer to *Distributing Licenses*, page A-19.

## Step 6: Configuring the EdgeServer

Now that the Central Manager is running, you need to set up and configure the remaining gateways as EdgeServers. Unpack another appliance and connect it to an installation console, as described in Steps 1 through 4, above.

If this gateway is to be set up remotely, ensure that the remote location contacts the administrator to verify the setup and configuration after Steps 1 through 4 have been completed.

This step includes the following sections:

- ▲ **Defining Local Area Connection Properties**, page A-14
- ▲ **Selecting Roles**, page A-15
- ▲ **Defining the EdgeServer Configuration**, page A-15
- ▲ **Defining Notification Settings**, page A-16
- ▲ **Registering to the Central Manager**, page A-16

For more information, refer to *Defining the EdgeServer Configuration* in *Chapter 3, Installation and Deployment*.



## Defining Local Area Connection Properties

This step enables you to configure the appliance for the local area network to which it is being connected.

➤ **To define the local area connection:**

- 1** In the *Local Area Connection Properties* page of the Setup Wizard, fill in the fields as follows:
  - Machine name (host name): **ActaStor2**
  - IP address: **192.168.2.11**
  - Net mask: **255.255.255.0**
  - Default GW: **192.168.2.1**
  - Primary DNS: **192.168.2.2**
  - Secondary DNS: (not required for this example)
  - DNS domain: **us.actona.com**
- 2** If the system is using DHCP, make sure to create a reservation record for the EdgeServer.
- 3** Click **Next** to proceed to the *System Properties* page of the Setup Wizard.
- 4** Set the time zone and the date/time of the EdgeServer in the fields provided.
- 5** Click **Next** to proceed to the *Role Selection* page of the Setup Wizard, as described in the section that follows.

## Selecting Roles

This section describes how to select the role of the appliance in the ActaStor network.

➤ **To select roles:**

- 1 In the *Role Selection* page of the Setup Wizard, select the **EdgeServer** checkbox.
- 2 Click **Next** to proceed to the next page of the Setup Wizard.

## Defining the EdgeServer Configuration

This step enables you to define the local configuration for an EdgeServer that will be used to cache content from CIFS file servers. For more information, refer to *Defining the EdgeServer Configuration* in *Chapter 3, Installation and Deployment*.

➤ **To define the EdgeServer configuration:**

- 1 In the *EdgeServer Configuration* page of the Setup Wizard, enter the name of the domain to which this appliance will belong in the **Exported servers workgroup or domain name** field.

Since all locations in this example belong to the same domain, enter **actona-us**.

- 2 In the **WINS** field, enter the name or IP address of the WINS server on the LAN, if any.
- 3 In the **DFS** field, enter the name of the site where the EdgeServer is located. This site name, which is typically found in the Active Directory database, is used in DFS target selection.
- 4 Click **Next** to proceed to the next page of the Setup Wizard.

## Defining Notification Settings

This step enables you to define the email address to which notifications are sent when alerts are generated by this gateway.

For more information, refer to *Defining Notification Settings* in *Chapter 3, Installation and Deployment*.

### ➤ To define notification settings:

- 1** In the *Notification Setting* page of the Setup Wizard, enter the address to which notifications about this gateway are sent in the **Email address** field.
- 2** In the **Mail server host name** field, enter the name or IP address of the mail server host.
- 3** In the **SNMP notification host** field, enter the name or address of the SNMP manager that will receive traps and notifications from the appliances in the ActaStor network.
- 4** Click **Next** to proceed to the next page of the Setup Wizard.

## Registering to the Central Manager

This step enables you to define parameters required by the gateway to register to the Central Manager of the ActaStor network.

For more information, refer to *Registering to the Central Manager* in *Chapter 3, Installation and Deployment*.

➤ **To register the gateway to the Central Manager:**

- 1** In the *Connection to Central Manager* page of the Setup Wizard, enter the logical name of the gateway as it will be identified in the ActaStor network in the **Gateway name** field. For this sample installation, enter **ActaStor2**.
- 2** In the **Central host** field, enter the IP address or machine name of the Central Manager. In this example, enter **192.168.29.50**.
- 3** To ensure the gateway registers with the Central Management Console, select the **Register with central** checkbox.
- 4** Click **Finish** to complete the setup process. The **Components** tab of the *Gateway Control* page is displayed, as shown in Figure A-3.

The component that was just configured is marked in red as **not licensed**. After you distribute the license key file from the Central Manager, it will be enabled. For more information, refer to *Distributing Licenses*, page A-19.

Congratulations – you have completed setting up two ActaStor gateways. You now need to establish connectivity between the CoreServer and EdgeServer, define coherency policies and test the ActaStor network. These procedures are described in the sections that follow.

# Step 7: Configuring the ActaStor Network with the Central Manager

After the gateway designated as the Central Manager has been deployed, you can launch the Central Manager remotely from any location on the ActaStor network via Internet Explorer. For more information refer to *Chapter 5, Central Management*.

This step includes the following sections:

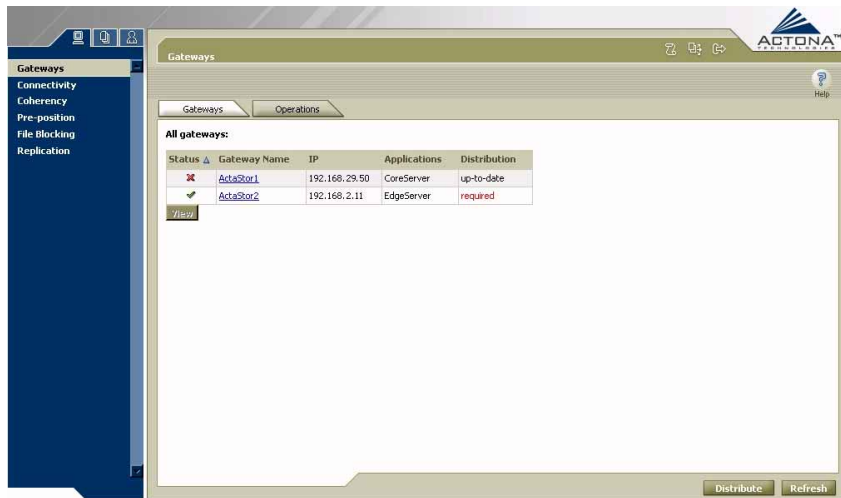
- **Launching the Central Manager**, below
- **Distributing Licenses**, page A-19
- **Starting the Gateway**, page A-21
- **Creating Connectivity Policies**, page A-21

## Launching the Central Manager

You launch the Central Manager from Internet Explorer.

- **To launch the Central Manager:**
  - 1** On a network-connected workstation, open Internet Explorer 5.5 or above and in the address bar, enter the ActaStor Management address **http://192.168.29.50/mgr** or **http://actastor1/mgr** to display the *Login* page.
  - 2** Enter the default user name (**admin**) and password (**actona**) in the fields provided, select the **Central Manager** option and click **Login**.

The Central Manager interface is displayed. The Central Manager includes three main views: Tasks, Groups and Users. By default, the Gateways page is displayed when you first access the Central Manager, as shown in Figure A-4. You can navigate to the different views and management screens using the navigation tabs.




**Figure A-4: Tasks View**

## Distributing Licenses

Activating specific components inside a gateway requires a license file, which is obtained from Actona. The Central Manager must be directed to this file, whose information is then distributed to the relevant gateway.

For more information, refer to *Managing Licenses* in *Chapter 5, Central Management*.

➤ **To distribute licenses:**

- 1 On the upper-right side of the bar above the display area, click the  icon to display the following:



**Figure A-5: License Installation Window**

- 2 In the **Select license file** field, click **Browse** and in the popup window displayed, navigate to the location of the license key file that you received by email, for example, **actona.lic**. (The license file will have an .LIC extension.)
- 3 Click **OK**. The path to the license file appears in the *License Installation* window. The details of the license are displayed in the **Selected license file data** area.
- 4 On the right side of the window, select the checkbox next to the gateway to which the license applies.

- 5 Click **Install License**. The licensing information is processed and distributed to the selected gateway. You can confirm the results in the *Distribution Tasks* window, as described in *Managing Distributions* in *Chapter 5, Central Management*.



**NOTE:**

If the licensing process fails, refer to *Chapter 6, Troubleshooting*.

## Starting the Gateway

Now that the licenses are installed on each gateway, you can start the configured gateway components.

For more information, refer to *Performing Operations on All Gateways* in *Chapter 5, Central Management*.

➤ **To start the gateway:**

- 1 In the left pane of the Tasks view, click **Gateways**. A list of all the registered gateways is displayed in the display area.
- 2 Click the **Operations** tab to display management options.
- 3 Click **Start All** to start all the enabled components in both registered gateways. A distribution window is displayed to indicate the progress of the start command.

## Creating Connectivity Policies

After distributing the license to the two gateways and starting their components, use the **Connectivity** option in the Central Manager to connect the gateways to each other according to their assigned roles.

For more information on connectivity policies, refer to *Defining Connections Between EdgeServers and CoreServers* in *Chapter 5, Central Management*.



➤ **To define a new connection:**

- 1 In the navigation area, click **Connectivity** to display the *Connectivity* page.
- 2 Click **Add** to display the following:



**Figure A-6: Selecting CoreServers for Connection**

- 3 In the **CoreServer** tab, select **ActaStor1**.
- 4 In the **EdgeServers** tab, select **ActaStor2**.
- 5 In the **NFS** tab, do the following:
  - Select the **Is root squash enabled on file servers** checkbox.
  - In both the **UID** and **GID** fields, change the default values (-2) to **60001**.

- 6 Click **Save** to save the new connection. Connection details are displayed on the *Connectivity* page.
- 7 Click **Distribute** to distribute the new connections to the gateways.

## Step 8: Connecting a Client to the EdgeServer

The EdgeServer behaves as just another node on your network. Clients can access it using the same methods used to access NFS or Windows file servers, such as UNC, drive mapping, share mounting and so on.

**NOTE:**



It is recommended that clients map a network drive to the EdgeServer.

- **To access the EdgeServer via a mapped drive:**
  - 1 Open Windows Explorer.
  - 2 From the *Tools* menu, select **Map Network Drive**.
  - 3 In the **Drive** field, browse to the drive to be mapped, `\\as-neptune\actona-us`, and click **OK**. After a few moments, the selected drive map is displayed in a new window.
- **To access the EdgeServer via UNC:**
  - 1 From the Windows *Start* menu, select **Run**.
  - 2 In the **Open** field, enter `\\as-neptune` and click **OK**. After a few moments, a new window should open. This window shows the available network shares on **Neptune** as they are exported via the local EdgeServer.

➤ **To mount a UNIX share:**

- 1** From the UNIX client, issue the following command:  
`showmount -e ActaStor1`. This displays the available exported shares on the EdgeServer. The naming convention is as follows:  
**`/<CoreServer-name>/<FileServer-name>/<Share-name>`**.
- 2** Issue the following mount command and press **<Enter>**:  
`mount actastor2:/actastor1/Saturn/public  
/mnt/public`
- 3** Issue the following command to change the directory to the mounted share and press **<Enter>**:  
`cd /mnt/public`

## Appendix B

# Third-party Licenses

The table below lists the third-party software components, libraries and modules referred to in the Software Licensing Agreement.

Name	Software License
Tomcat	The Apache Software License, Version 1.1
Struts	The Apache Software License, Version 1.1
Log4J	The Apache Software License, Version 1.1
Regexp	The Apache Software License, Version 1.1
Commons	The Apache Software License, Version 1.1
MX4J	The MX4J License, Version 1.0
Xerces	The Apache Software License, version 1.1
Seda	
Jdom	\$Id: LICENSE.txt,v 1.8 2002/01/19 10:15:17 jhunter Exp \$
Westhawk's SNMP Stack	
Rsync	GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Name	Software License
Red Hat Linux	GNU GENERAL PUBLIC LICENSE Version 2, June 1991
Ethereal	GNU GENERAL PUBLIC LICENSE Version 2, June 1991
SAMBA	GNU GENERAL PUBLIC LICENSE Version 2, June 1991
PathRate	GNU GENERAL PUBLIC LICENSE Version 2, June 1991
MRTG	GNU GENERAL PUBLIC LICENSE Version 2, June 1991
CUPS	GNU GENERAL PUBLIC LICENSE Version 2, June 1991

**NOTE:**

The source code for this package can be made available by contacting Cisco at [tac@cisco.com](mailto:tac@cisco.com).

## The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org).

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.



## The Apache Software License, Version 1.1

Copyright (c) 2001-2003 The Apache Software Foundation. All rights reserved.  
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgement: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."

Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear.

4. The names "Apache", "The Jakarta Project", "Commons", and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org).
5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their name without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====  
This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

## The MX4J License, Version 1.0

Copyright (c) 2001 MX4J. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the MX4J project (<http://sourceforge.net/projects/mx4j>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "MX4J" and "mx4j" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [biorn\\_steedom@users.sourceforge.net](mailto:biorn_steedom@users.sourceforge.net)
5. Products derived from this software may not be called "MX4J", nor may "MX4J" appear in their name, without prior written permission of Simone Bordet.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CHRIS SEGUIN OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====  
This software consists of voluntary contributions made by many individuals on behalf of MX4J. For more information on MX4J, please see <http://sourceforge.net/projects/mx4j>.





## The Apache Software License, Version 1.1

Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Xerces" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org).
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright (c) 1999, International Business Machines, Inc., <http://www.ibm.com>. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

The SEDA release is covered under the following Open Source license:

Copyright (c) 2002 by Matt Welsh and The Regents of the University of California. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without written agreement is hereby granted, provided that the above copyright notice and the following two paragraphs appear in all copies of this software.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.



\$Id: LICENSE.txt,v 1.8 2002/01/19 10:15:17 jhunter Exp \$

Copyright (C) 2000-2002 Brett McLaughlin & Jason Hunter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [license@jdom.org](mailto:license@jdom.org).
4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management ([pm@jdom.org](mailto:pm@jdom.org)).

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (<http://www.jdom.org/>)."

Alternatively, the acknowledgment may be graphical using the logos available at <http://www.jdom.org/images/logos>.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====  
This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Brett McLaughlin <[brett@jdom.org](mailto:brett@jdom.org)> and Jason Hunter <[jhunter@jdom.org](mailto:jhunter@jdom.org)>. For more information on the JDOM Project, please see <<http://www.jdom.org/>>.

## Westhawk

Copyright (C) 2002 by Westhawk Ltd ([www.westhawk.co.uk](http://www.westhawk.co.uk))

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation.

This software is provided "as is" without express or implied warranty.

author <[a href="mailto:snmp@westhawk.co.uk">href="mailto:snmp@westhawk.co.uk"](mailto:snmp@westhawk.co.uk)>Tim Panton</a> \*/



## GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)



These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.





9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also, add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w' This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker. <signature of Ty Coon>, 1 April 1989  
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.



# Index

## A

### Accessing

Setup Wizard, 3-6

### ActaStor

Benefits, 1-8

Capacity Limitations, 2-23

Deployment, 1-5, 3-2

Deployment Scenarios, 2-21

Features, 1-6

Getting Technical Assistance, 6-2

Integration, 2-17, 2-26

Introduction, 1-2

Launching Central Manager, 5-2

Launching Gateway Manager, 4-3

License, 3-24

Modules, 1-3

Network Planning, 2-21

Sample Installation, A-1

Scenarios and Applications, 1-10

SNMP Support, 1-7

Target Audience, 1-9

Technical Overview, 2-6

Terms and Concepts, 2-2

Transparency, 1-7, 2-8

Troubleshooting, 6-2

Active Directory, 2-29, 4-39, 5-71, A-15

Actona Support, 6-2

### Adding

Users, 5-83

### Advanced Options

CIFS and NFS, 5-62

Unregistering Gateways, 5-14

### Authentication, 2-4

## B

### Backing Up/Restoring

Configuration Files, 4-13

## C

### Cache Removal, 4-26, 4-63

Running, 4-26

### Caching, 1-6, 2-2

Negative, 2-9

Partial, 2-9

Technical Overview, 2-9

### Central Manager

Registering Gateway, 3-21

### Central Manager, 2-21, 4-16

Adding Users, 5-83

Defining Coherency Policies, 5-29

Defining Connections, 5-17

Defining CoreServer Clusters, 5-74



- Defining EdgeServer Groups, 5-67
- Defining File Blocking Policies, 5-49
- Defining Notification Settings, 5-71
- Defining Pre-position Policies, 5-37
- Defining Replication Policies, 5-54
- Deleting Coherency Policies, 5-36
- Deleting CoreServer Clusters, 5-81
- Deleting EdgeServer Connections, 5-28
- Deleting EdgeServer Groups, 5-73
- Deleting File Blocking Policies, 5-54
- Deleting Pre-position Policies, 5-49
- Deleting Replication Policies, 5-65
- Deleting Users, 5-85
- Duplicating Coherency Policies, 5-36
- Duplicating File Blocking Policies, 5-53
- Duplicating Pre-position Policies, 5-48
- Duplicating Replication Policies, 5-65
- Editing Coherency Policies, 5-35
- Editing CoreServer Clusters, 5-81
- Editing EdgeServer Connections, 5-28
- Editing EdgeServer Groups, 5-73
- Editing File Blocking Policies, 5-53
- Editing Pre-position Policies, 5-48
- Editing Replication Policies, 5-64
- Editing Users, 5-85
- Gateways Option, 5-11
- Groups View, 5-66
- Introduction, 1-4
- Launching, 5-2
- Logging Out, 5-4
- Managing Distributions, 5-7
- Managing Groups, 5-66
- Managing Licenses, 5-6
- Managing Tasks, 5-10
- Managing Users, 5-82
- Modifying Group CIFS Settings, 5-70
- Network Planning, 2-25
- Quick Tour, 5-3
- Setting Default Coherency Age, 5-70
- Tasks View, 5-10
- Troubleshooting, 6-6
- Users View, 5-82
- Workflow, 5-5
- Central Office, 2-22, 2-26, 2-31
- CIFS, 2-2, 2-7, 2-18, 3-15, 4-30, 5-58, A-9
  - Advanced Options, 5-62
  - Defining Servers, 3-15
  - Defining Servers for Cluster, 5-79
  - Deleting Servers, 4-33
  - Modifying Settings in EdgeServer, 4-38
  - Modifying Settings in EdgeServer Groups, 5-70
  - Selecting Servers, 4-30
- Clustering, 2-18
- Clusters
  - Defining Configuration Settings, 5-76
  - Defining for CoreServer, 5-74
- Coherency, 1-6, 2-3
  - Age-based Validation, 2-13
  - Common Semantics, 2-12
  - Defining Policies, 5-29
  - Deleting Rules, 5-36
  - Duplicating Policies, 5-36
  - Editing Policies, 5-35
  - Setting Default Age, 4-35, 5-70
- Technical Overview, 2-11

Component

- Central Manager, 1-4
- CoreServer, 1-3, 4-27
- EdgeServer, 1-3, 4-34
- Replication, 4-44

Components

- Starting, 3-24
- Starting/Stopping, 4-8

Concurrency, 1-6, 2-3

- Technical Overview, 2-13

Configuration Files

- Backing Up/Restoring, 4-13

Configuration Option

- Configuring Print Services, 4-18
- CoreServer, 4-27
- Defining Manager Configuration, 4-15
- Defining Notification Settings, 4-23
- Defining SNMP Manager, 4-16
- EdgeServer, 4-34
- Gateway, 4-14
- Viewing Connection Settings, 4-17

Configuring

- Print Services, 4-18

Connection Settings

- Viewing, 4-17

Contacting

- Actona Support, 6-2

Control Option, 4-8

- Backing Up/Restoring Configuration Files, 4-13
- Rebooting Gateway, 4-11
- Registering Gateways, 4-12
- Shutting Down Gateway, 4-11
- Starting/Stopping Components, 4-8

CoreServer

- Configuration Option, 4-27
- CoreServer Clusters, 5-74
- Defining Clusters, 5-74
- Defining Clusters Settings, 5-76
- Defining Connections, 5-17
- Deleting Clusters, 5-81
- Editing Clusters, 5-81
- Failover, 5-74
- High Availability, 5-74
- Initial Configuration, 3-14
- Integration, 2-28
- Introduction, 1-3
- Managing Component, 4-27
- Network Planning, 2-25
- Viewing Connections to, 4-37
- CoreServer Clusters, 1-7, 2-18
- Defining, 5-74
- Defining Configuration Settings, 5-76
- Deleting, 5-81
- Editing, 5-81
- Planning, 2-25
- CoreServer Component
- Configuration Option, 4-27
- Managing, 4-27
- Monitoring, 4-53
- CoreServer Configuration, 3-14
- Defining CIFS Servers, 3-15
- Defining NFS Servers, 3-17
- CoreServer Integration
- Registering in DNS Server, 2-28
- CoreServer Option
- Selecting CIFS Servers, 4-30
- Selecting NFS Servers, 4-28

**D**

## Defining

- CIFS Servers, 3-15
- Coherency Policies, 5-29
- Connections, 5-17
- CoreServer Clusters, 5-74
- CoreServer Configuration, 3-14
- EdgeServer Configuration, 3-12
- EdgeServer Groups, 5-67
- File Blocking Policies, 5-49
- Gateway Connectivity, 3-24
- Local Area Connection Properties, 3-8
- Manager Configuration, 4-15
- NFS Servers, 3-17
- Notification Settings, 4-23, 5-71
- Pre-position Policies, 5-37
- Replication Policies, 5-54
- SNMP Manager, 4-16
- System Properties, 3-9

## Deleting

- CIFS Servers, 4-33
- Coherency Policies, 5-36
- CoreServer Clusters, 5-81
- EdgeServer Connections, 5-28
- EdgeServer Groups, 5-73
- File Blocking Policies, 5-54
- NFS Servers, 4-30
- Pre-position Policies, 5-49
- Replication Policies, 5-65
- Users, 5-85

## Deployment

- Defining Connectivity, 3-24
- Installing Appliance, 3-3

- Installing License, 3-24
- Starting Components, 3-24
- Unpacking Hardware, 3-2
- Using Setup Wizard, 3-5
- Deployment Scenarios, 2-21
  - Centralization, 2-21
  - Collaboration, 2-22, 2-27
- DFS, 2-29, 4-39, 5-71, A-15
  - Namespace, 2-19
- DFS Site Name, 2-29
- DHCP, 2-28, 2-29, 3-2, 3-3, 3-9, 3-23, 4-18, 6-4, 6-7
- Distributions
  - Managing, 5-7
  - Viewing Details, 5-9
  - Viewing Tasks, 5-8
- DNS, 6-4, 6-7
- DNS Server, 2-29
- DNS Server and Domain, 2-28, 2-29, 2-30
- Domain Controller, 2-27
- Duplicating
  - Coherency Policies, 5-36
  - File Blocking Policies, 5-53
  - Pre-position Policies, 5-48
  - Replication Policies, 5-65

**E**

## EdgeServer

- Configuration Option, 4-34
- Defining Connections, 5-17
- Defining Group Settings, 5-68
- Defining Groups, 5-67
- Deleting Connections, 5-28

- Deleting Groups, 5-73
- Editing Connections, 5-28
- Editing Groups, 5-73
- Integration, 2-29
- Introduction, 1-3
- Managing Component, 4-34
- Modifying CIFS Settings, 4-38
- Modifying Group CIFS Settings, 5-70
- Network Planning, 2-25
- Policies Option, 4-39
- Setting Group Default Coherency Age, 5-70
- Viewing CoreServer Connections, 4-37
- Viewing Logs, 4-63
- EdgeServer Component
  - Configuration Option, 4-34
  - Managing, 4-34
  - Monitoring, 4-56
  - Policies Option, 4-39
- EdgeServer Integration
  - Adding Server Names to Active Directory, 2-29
  - Registering in DNS Server, 2-29
  - Registering on Domain Master Browser, 2-29
- EdgeServer Option
  - Modifying CIFS Settings, 4-38
  - Setting Default Coherency Age, 4-35
  - Viewing CoreServer Connection, 4-37
- Editing
  - Coherency Policies, 5-35
  - CoreServer Clusters, 5-81
  - EdgeServer Connections, 5-28
  - EdgeServer Groups, 5-73

- File Blocking Policies, 5-53
- Pre-position Policies, 5-48
- Replication Policies, 5-64
- Users, 5-85

## F

- Failover, 1-7, 2-18, 5-74
- File Blocking
  - Defining Policies, 5-49
  - Deleting Policies, 5-54
  - Duplicating Policies, 5-53
  - Editing Policies, 5-53
- File System Protocol
  - CIFS, 2-2
  - NFS, 2-2
- Firewall, 2-27

## G

- Gateway Component
  - Configuration Option, 4-14
  - Control Option, 4-8
  - Managing, 4-7
  - Monitoring, 4-52
  - Utilities Option, 4-24
- Gateway Manager
  - Accessing from Central Manager, 5-13, 5-14
  - Backing Up/Restoring Configuration Files, 4-13
  - Configuring Print Services, 4-18
  - Control Option, 4-8
  - CoreServer Component, 4-27
  - CoreServer Configuration Option, 4-27
  - Defining Manager Configuration, 4-15



- Defining Notification Settings, 4-23
- Defining SNMP Manager, 4-16
- EdgeServer Component, 4-34
- EdgeServer Configuration Option, 4-34
- EdgeServer Policies Option, 4-39
- Gateway Component, 4-7
- Gateway Configuration Option, 4-14
- Introduction, 1-4
- Launching, 4-3
- Logging Out, 4-5
- Modifying CIFS Settings, 4-38
- Monitoring Gateway, 4-49
- Quick Tour, 4-4
- Rebooting Gateway, 4-11
- Registering Gateways, 4-12
- Replication Component, 4-44
- Running Cache Removal Utility, 4-26
- Running Support Utilities, 4-25
- Selecting CIFS Servers, 4-30
- Selecting NFS Servers, 4-28
- Setting Default Coherency Age, 4-35
- Setup Wizard, 3-5
- Shutting Down Gateway, 4-11
- Starting/Stopping Components, 4-8
- Troubleshooting, 6-6
- Utilities Option, 4-24
- Viewing Connection Settings, 4-17
- Viewing CoreServer Connections, 4-37
- Viewing Logs, 4-63
- Viewing Monitoring Graphs, 4-50
- Workflow, 4-6
- Gateways
  - Backing Up/Restoring Configuration Files, 4-13
  - Configuring Print Services, 4-18
  - Defining Coherency Policies, 5-29
  - Defining Connections, 5-17
  - Defining CoreServer Clusters, 5-74
  - Defining EdgeServer Groups, 5-67
  - Defining File Blocking Policies, 5-49
  - Defining Manager Configuration, 4-15
  - Defining Notification Settings, 4-23
  - Defining Pre-position Policies, 5-37
  - Defining Replication Policies, 5-54
  - Defining SNMP Manager, 4-16
  - Deleting Coherency Policies, 5-36
  - Deleting CoreServer Clusters, 5-81
  - Deleting EdgeServer Connections, 5-28
  - Deleting EdgeServer Groups, 5-73
  - Deleting File Blocking Policies, 5-54
  - Deleting Pre-position Policies, 5-49
  - Deleting Replication Policies, 5-65
  - Deleting Users, 5-85
  - Duplicating Coherency Policies, 5-36
  - Duplicating File Blocking Policies, 5-53
  - Duplicating Pre-position Policies, 5-48
  - Duplicating Replication Policies, 5-65
  - Editing Coherency Policies, 5-35
  - Editing CoreServer Clusters, 5-81
  - Editing EdgeServer Connections, 5-28
  - Editing EdgeServer Groups, 5-73
  - Editing File Blocking Policies, 5-53
  - Editing Pre-position Policies, 5-48
  - Editing Replication Policies, 5-64
  - Editing Users, 5-85
  - Managing, 5-12
  - Managing Tasks, 5-10

- Modifying CIFS Settings, 4-38, 5-70
- Monitoring, 4-49
- Performing Operations on All, 5-15
- Rebooting, 4-11
- Registering, 4-12
- Running Cache Removal Utility, 4-26
- Running Support Utilities, 4-25
- Selecting CIFS Servers, 4-30
- Selecting NFS Servers, 4-28
- Setting Default Coherency Age, 4-35, 5-70
- Shutting Down, 4-11
- Starting/Stopping, 5-15
- Starting/Stopping Components, 4-8
- Updating, 5-15
- Viewing Connection Settings, 4-17
- Viewing CoreServer Connections, 4-37
- Viewing Details, 5-12
- Viewing Logs, 4-63
- Viewing Monitoring Graphs, 4-50

Gateways Option, 5-11

Groups

- Defining CoreServer Clusters, 5-74
- Defining CoreServer Clusters Settings, 5-76
- Defining EdgeServer Group Settings, 5-68
- Defining EdgeServer Groups, 5-67
- Managing, 5-66

## H

- High Availability, 1-7, 5-74

## I

- Installation Console, 3-2, 3-23
- Integration, 2-17, 2-26
  - Clustering and Failover, 2-18
  - CoreServer, 2-28
  - EdgeServer, 2-29
  - End Users, 2-18
  - File Servers, 2-17
  - Firewall, 2-27
  - Mapping UNIX Users, 2-31
  - Namespace, 2-19
  - Pre-installation, 2-27
  - SNMP Support, 2-19
  - UNIX Network, 2-30
  - Windows Network, 2-27

## L

Launching

- Central Manager, 5-2
- Gateway Manager, 4-3

Licenses

- Installing, 3-24
- Managing, 5-6

Load Balancing, 2-18

Login

- Central Manager, 5-2
- Gateway Manager, 4-3
- Setup Wizard, 3-6

## Logs

Severity Levels, 4-63

Viewing, 4-63

**M**

## Managing

CoreServer Component, 4-27

Distributions, 5-7

EdgeServer Component, 4-34

Gateway Component, 4-7

Gateways, 5-12

Groups, 5-66

Licenses, 5-6

Tasks, 5-10

Users, 5-82

Master Browser, 2-27

MGR Port, 3-3, 6-3

## Modifying

EdgeServer CIFS Settings, 4-38

EdgeServer Group CIFS Settings, 5-70

## Monitoring

CoreServer Component, 4-53

EdgeServer Component, 4-56

Gateway Component, 4-52

Gateways, 4-49

## Monitoring Graphs

Viewing, 4-50

**N**

## Namespace

DFS, 2-19

NAS Appliances, 1-11

NAS Devices, 2-2

NET Port, 3-4, 6-4

## Network Planning, 2-21

Calculating Components, 2-25

Capacity Limitations, 2-23

NFS, 2-2, 2-7, 2-18, 3-17, 4-28, 5-58,

A-10

Advanced Options, 5-62

Connection Parameters, 5-19

Defining Servers, 3-17

Defining Servers for Cluster, 5-77

Deleting Servers, 4-30

Selecting Servers, 4-28

NIS, 2-30, 2-31

## Notification Settings

Defining, 4-23

Defining for Group, 5-71

**P**

## Policies Option

EdgeServer, 4-39

## Pre-position

Terminating Task, 4-43

## Pre-position Task

Terminating, 4-43

## Pre-positioning, 1-6

Defining Policies, 5-37

Deleting Policies, 5-49

Duplicating Policies, 5-48

Editing Policies, 5-48

## Print Services, 4-18

Configuring Printer Drivers, 4-22

## Q

### Quick Tour

- Central Manager, 5-3
- Gateway Manager, 4-4

## R

### Rebooting

- Gateways, 4-11

### Registering

- Gateways, 4-12

### Replication, 1-6, 2-4

- Defining Policies, 5-54
- Deleting Policies, 5-65
- Destination Gateway, 5-55
- Duplicating Policies, 5-65
- Editing Policies, 5-64
- Replication Client, 2-17
- Replication Server, 2-17
- Replication Task, 2-17
- Source Gateway, 5-55
- Technical Overview, 2-16
- Terminating Task, 4-48

### Replication Component, 4-44

### Replication Task

- Terminating, 4-48

### Root Squash, 5-25

### Running

- Cache Removal Utility, 4-26
- Support Utilities, 4-25

## S

### Sample Installation

- Accessing the Central Manager, A-18

### Accessing the Setup Wizard, A-6

- Configuring the Client Installation  
Console, A-5

### Configuring the CoreServer, A-7

### Configuring the EdgeServer, A-13

- Connecting a Client to the EdgeServer,  
A-23

### Turning on Appliance, A-4

### Unpacking the Hardware, A-4

### Scenarios and Applications, 1-10

- Branch Office Data Protection, 1-10
- Centralized Backup, 1-11
- Corporate Information Sharing, 1-12
- File Server Consolidation, 1-10
- Global Data Access, 1-11

### Selecting

- CIFS Servers, 4-30
- NFS Servers, 4-28
- Roles, 3-11

### Setting

- Default Coherency Age, 4-35, 5-70

### Setup Wizard, 3-5, 4-17, 4-27, 4-38, 6-1

#### Accessing, 3-6

- Defining CoreServer Configuration,  
3-14

- Defining EdgeServer Configuration,  
3-12

#### Defining LAN Properties, 3-8

#### Defining Notification Settings, 3-20

#### Defining System Properties, 3-9

#### Login, 3-6

#### Registering to Central Manager, 3-21

#### Selecting Roles, 3-11



Shutting Down  
Gateways, 4-11

SNMP, 2-19  
Support, 1-7

Starting/Stopping  
Components, 4-8  
Gateways, 5-15

Support Utilities  
Running, 4-25

## T

Technical Assistance, 6-2  
Technical Overview, 2-6  
Coherency, 2-11  
Concurrency, 2-13  
Data Management Goals, 2-6  
File System Caching, 2-9  
Pre-positioning, 2-10  
Print Services, 2-10  
Challenge, 2-7  
Replication, 2-16  
Security, 2-11  
Solution, 2-8  
WAN Adaptation, 2-14

Terminating  
Pre-position Task, 4-43  
Replication Task, 4-48

Terms and Concepts, 2-2  
Authentication, 2-4  
Authorization/Access Control, 2-4  
Concurrency, 2-3  
Data Coherency, 2-3  
File Servers, 2-2  
File System Caching, 2-2

Replication, 2-4  
WAN, 2-5  
Troubleshooting, 6-2  
ActaStor Managers, 6-6  
Central Manager, 6-6  
Client Operation, 6-9  
Gateway Manager, 6-6

## U

UNIX Integration  
Registering Gateways in DNS Server,  
2-30  
Updating  
Gateways, 5-15  
Users  
Adding, 5-83  
Deleting, 5-85  
Editing, 5-85  
Managing, 5-82  
Types, 5-82  
Utilities  
Cache, 4-26  
Support, 4-25  
System Report, 6-2  
Utilities Option, 4-24  
Running Cache Removal Utility, 4-26  
Running Support Utilities, 4-25

## V

Viewing  
Connection Settings, 4-17  
CoreServer Connections, 4-37  
Gateway Details, 5-12

Gateway Logs, 4-63  
Monitoring Graphs, 4-50  
Views  
Groups, 5-66  
Tasks, 5-10  
Users, 5-82

## **W**

WAN Adaptation, 2-14  
Disconnected Mode, 2-16  
Optimization, 2-14

Watchdog  
Viewing Logs, 4-63  
Windows Domain Name, 2-29  
WINS Server, 2-28, 2-29, 3-13, 4-38,  
4-39, 5-71  
Workflow  
Central Manager, 5-5  
Gateway Manager, 4-6









## **Cisco Systems, Inc.**

170 West Tasman Drive  
San Jose, CA 95134  
408.526.4000

Web: [www.cisco.com](http://www.cisco.com)

Email: [tac@cisco.com](mailto:tac@cisco.com)