ExtremeZ-IP®

FILE & PRINT SERVER VERSION 7

User Manual

GroupLogic®

GroupLogic, Inc.
1.703.528.1555
Email: ezip@grouplogic.com
Web: www.grouplogic.com

Copyright

Notice

The information and the software discussed in this document are subject to change without notice and should not be considered commitments by GroupLogic, Incorporated. GroupLogic, Incorporated assumes no responsibility for any errors in this document.

The software discussed in this document is furnished under a license and may be used or copied only in accordance with the terms of the license. No responsibility is assumed by GroupLogic, Incorporated for the use or reliability of software on equipment that is not supplied by GroupLogic or its affiliated companies.

All warranties given by GroupLogic, Incorporated about equipment or software are set forth in your purchase contract, and nothing stated in, or implied by, this document or its contents shall be considered or deemed a modification or amendment of such warranties.

Trademarks

GLI 2011.07.06 - 7.2

Table of Contents

ExtremeZ-IP®

GETTING STARTED

With ExtremeZ-IP, Windows® computers can provide AppleShare® IP file sharing and IP-printing, TCP/IP, and AppleTalk® print services to Macintosh® computers. ExtremeZ-IP is optimized to provide the fastest file and print services available. ExtremeZ-IP includes the following services:

- ExtremeZ-IP File Server
- ExtremeZ-IP Print Server

With ExtremeZ-IP, Macintosh users can connect to and mount directories on a Windows file server just as if they also were native AppleShare volumes. With the ExtremeZ-IP Print Server installed, Macintosh users can create desktop printers that deliver print jobs to printers via the server automatically and just as easily as with AppleTalk. ExtremeZ-IP's integration into the existing network is seamless–Macintosh users continue using the same tools and applications for accessing the server and printers that they always have, but the server delivers much higher performance. With ExtremeZ-IP Print Accounting, the Macintosh clients must provide additional information such as a job code or employee ID before the server will accept the job.

System Requirements

Windows

The ExtremeZ-IP File Server operates on Windows 2003®, Windows Server 2008®, Windows XP®, Windows Vista®. For optimal results, your Windows machine should be running the latest service pack from Microsoft®. Adding additional RAM to your Windows machine will greatly enhance ExtremeZ-IP performance. See below for system requirements.

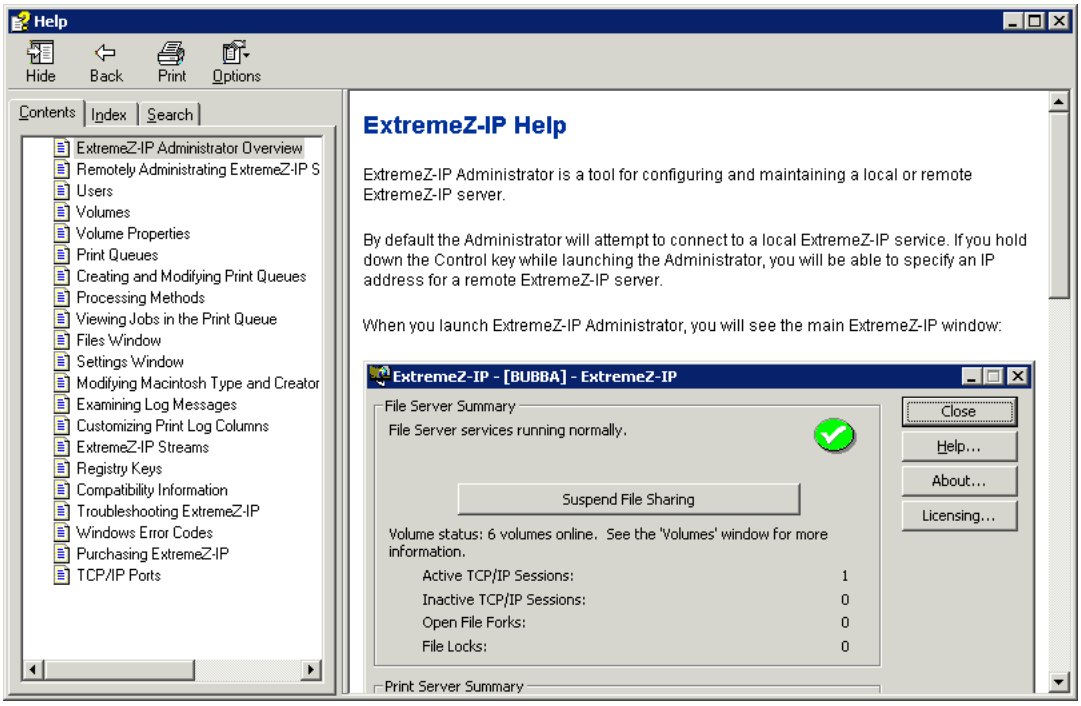
- Windows System Requirements
  - Windows Server Platforms: 2008, 2003, Windows Storage Server, Windows Powered NAS
  - Windows Professional Platforms: Windows 7, Vista, XP Pro, XP Embedded
- Minimum Hardware Recommendation:
  - Processor: Pentium IV
  - Memory: 1 GB

Macintosh Clients

Macintosh clients must have Mac OS 9.0 or later and should run the latest Mac OS release. If Macintosh clients are using Mac OS X, they must have version 10.2.8 or later. ExtremeZ-IP supports the latest Macintosh client technologies, including Bonjour®, the Service Location Protocol (SLP), Kerberos®, and Apple's built-in encrypted logon support for long passwords. Print Accounting requires Mac OS X 10.3. Zidget requires Mac OS X 10.4. DFS and Network Spotlight require Mac OS X 10.5. Print Accounting is not compatible with applications running in 64-bit mode on Mac OS X 10.6 or later.

Getting Help

You can open Help from the Windows menu in the ExtremeZ-IP Administrator.



You can visit Group Logic at: http://www.grouplogic.com

You can find the latest releases of ExtremeZ-IP at http://www.grouplogic.com/files/glidownload/ezipreleases.cfm

The ExtremeZ-IP Manual at http://www.grouplogic.com/files/ez/EZIPManual.pdf

You can search the Knowledgebase at http://www.grouplogic.com/Knowledge/index.cfm

For the first year you own ExtremeZ-IP, technical support and upgrades are included in the price of the product. After your first year of free support, you can purchase extended support. For technical support services, submit a support request at http://www.grouplogic.com/support/requestform/ or call 1.703.528.1555 Monday through Friday, 8:00 am to 6:00 pm ET. Have your ExtremeZ-IP serial number ready for verification. In addition, you can send your questions to support@grouplogic.com

The Maintenance and Support program includes important benefits—e-mail, fax and telephone technical support services for problems that you encounter, upgrades, bug fixes, and other incremental releases of the software.

About This Document

The ExtremeZ-IP User's Guide includes the following sections:

- *Getting Starting with ExtremeZ-IP* describes ExtremeZ-IP, lists system requirements, and explains how you can get help.
- *Installing ExtremeZ-IP* includes instructions for installing and removing the ExtremeZ-IP File Server, the ExtremeZ-IP Print Server and instructions for starting and stopping the ExtremeZ-IP service. In addition, it explains installing AppleTalk, Kerberos, and Clustering.
- *ExtremeZ-IP File Server* provides instructions for administering ExtremeZ-IP File Server on local and remote computers, information about the features of ExtremeZ-IP, and instructions for remapping MS-DOS extensions to make files easy to use for Macintosh users.
- *ExtremeZ-IP Print Server* includes instructions for using the print server and print accounting.
- *ExtremeZ-IP Zidget™* provides instructions for using Zidget with both the file and print server.
- *ExtremeZ-IP DFS - Macintosh Client Configuration* includes instructions for configuring Macintosh clients for DFS support.
- The Appendices cover the following topics.
  - Using the Registry Keys
  - Monitoring ExtremeZ-IP
  - Configuring Guest Access for Windows XP and above
  - Legal Notices

ExtremeZ-IP®

INSTALLING EXTREMEZ-IP

Installing ExtremeZ-IP

The primary component of ExtremeZ-IP is a Windows Service that provides file and print sharing to Macintosh clients. ExtremeZ-IP also includes an administrative tool with which you can configure shared volumes and other settings.

The number of clients who can connect using ExtremeZ-IP depends on your license and its client count. You can upgrade your client count as necessary. ExtremeZ-IP counts multiple connections from one user account on one IP address as one user for licensing purposes.

Before Installing ExtremeZ-IP

The topics covered in this section give you information you need before installing ExtremeZ-IP.

ExtremeZ-IP and SFM

If you are installing a trial version of ExtremeZ-IP on a server and want to continue running Services for Macintosh, the ExtremeZ-IP service will switch to TCP/IP port 549 instead of using the default AFP port 548. Services for Macintosh remains running on port 548, so you can attach using either service. To connect to the ExtremeZ-IP service from a client, add ":549" after the server IP address or DNS name (ex. 192.168.1.1:549)

Required Windows File Permissions for Shared Volumes

ExtremeZ-IP relies on the SYSTEM account on the Windows server to perform many of its core functions. For this reason, any folder hierarchy that is shared as a volume with ExtremeZ-IP requires that the SYSTEM account have ***Full Control*** access to the entire folder hierarchy. These permissions are the default for the Windows OS partition, but any additional disks or partitions containing ExtremeZ-IP volumes must have SYSTEM = "Full Control" set to allow ExtremeZ-IP to function properly. Please verify that all the volumes you share have this permission set.

Sharing the Root of a Drive

Although ExtremeZ-IP supports sharing out the root of the drive, Windows treats permissions at the root of the file system differently from other folders. We recommend that you do not share out drive letters directly. Instead, you should create a sub-folder for your shared volume.

Installing the ExtremeZ-IP Program

To install the ExtremeZ-IP program, do the following:

1. Log into Windows with an administrator account.
2. Run the ExtremeZ-IP installer
3. Follow the steps displayed by the installer.

See the *Installation Quick Start* PDF for step by step installation instructions.

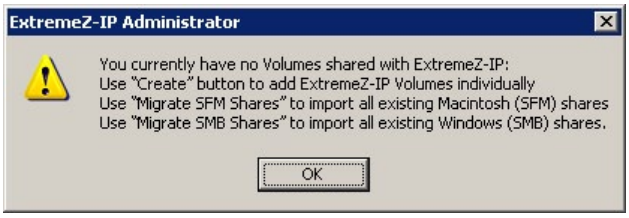
NOTE For reinstallations, the ExtremeZ-IP installer stops the ExtremeZ-IP Service to perform the install. However, in some cases the installation fails because the ExtremeZ-IP Service cannot be stopped; these cases include possible service errors, conflicts with other running processes, or installing while the Services Control Panel is open. If you experience installation failures, you can stop the Service manually from the Services Control Panel and proceed with the install.

Sharing the Print Server Directory

When you install ExtremeZ-IP, the installer creates a directory called ExtremeZ-IP Print Support. You have the option to share that directory for Macintosh clients. If you share the directory with the ExtremeZ-IP File Server, Macintosh clients can mount the volume to download the optional ExtremeZ-IP Macintosh Print Client. Macintosh clients do not need to use this program to print to the ExtremeZ-IP Print Server; however, using it provides easy IP printing and makes it easy for Macintosh clients to use Bonjour (OS X), SLP (OS 9), or an IP address to find the ExtremeZ-IP Print Server.

Launching ExtremeZ-IP the First Time

When you launch the ExtremeZ-IP Administrator for the first time with no configured volumes (shares), ExtremeZ-IP prompts you to create new volumes or import existing volumes. ExtremeZ-IP can import existing volumes on your server that are shared using Services for Macintosh (SFM) and Windows file sharing (SMB). During the import, ExtremeZ-IP migrates SFM/SMB share settings, such as SFM volume passwords and the maximum number of users.

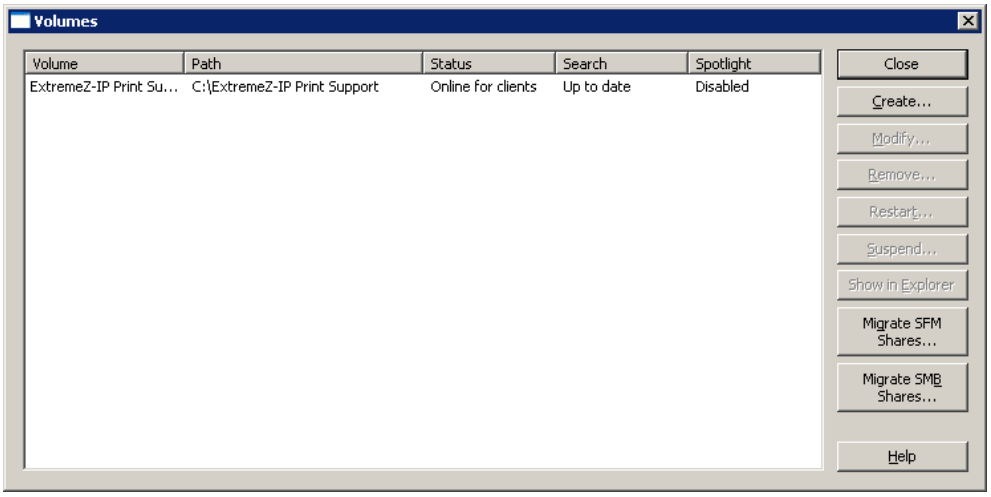


If you are upgrading from a previous version, ExtremeZ-IP checks for volumes shared with previous versions of ExtremeZ-IP and automatically creates these ExtremeZ-IP volumes.

Automatically Importing SFM and SMB Shares

SFM Shares

Each time the ExtremeZ-IP Administrator is launched, ExtremeZ-IP checks for any SFM shares that are not being shared as ExtremeZ-IP volumes. If any such volumes exist, the **Migrate SFM Shares** button within the **Volumes** dialog becomes active.



If you choose **Migrate SFM Shares**, ExtremeZ-IP volumes are created for those SFM shares. In addition, if the SFM service is running, it is stopped and the service disabled. The following bullets describe how ExtremeZ-IP treats shares.

- ExtremeZ-IP does not remove the SFM shares themselves. If you re-enable and run the SFM service, those shares are unchanged.
- In the event that SFM is re-enabled at a later date, ExtremeZ-IP takes the volumes that conflict with SFM shares offline.
- ExtremeZ-IP uses the built-in Apple user authentication modules; therefore, the Microsoft UAM volume from SFM is not migrated.

- ExtremeZ-IP does not reuse SFM's Macintosh file IDs, but any data (including metadata such as Finder info) in the SFM share are accessible through ExtremeZ-IP.

SMB Shares

Each time the ExtremeZ-IP Administrator is launched, ExtremeZ-IP checks for any SMB shares that are not being shared as ExtremeZ-IP volumes. If any such volumes exist, the **Migrate SMB Shares** button within the **Volumes** dialog becomes active. If you choose to do so, ExtremeZ-IP creates new volumes for those SMB shares. ExtremeZ-IP does not replicate hidden shares (for example, C$).

When Mac OS X clients copy files to a server with SMB, they do not have access to alternate streams, where resource fork and Finder information is usually stored. Instead, this resource fork and Finder information is written to a separate file, the "dot underscore" file. To the Macintosh client, this action happens behind the scenes—the dot underscore is hidden, and all they see is a single file that appears to contain resource fork and Finder information. But when you view these files from Windows, the dot underscore file is just another hidden file with no relation to the original data file.

In ExtremeZ-IP, the server can migrate resource and Finder information from the dot underscore file into alternate data streams of the file so that Macintosh clients have access to that information. When a Macintosh client requests information about a file or folder, ExtremeZ-IP first tries to read from the file or folder's Finder info stream (AFP_AfpInfo) and, in the case of a file, from its resource stream (AFP_Resource). If either one of these streams is missing, ExtremeZ-IP tries to find a corresponding dot underscore file. If that file is present and contains the necessary data, the data are migrated into the appropriate stream.

The dot underscore migration feature is enabled by default, but you can disable this feature.

To disable this feature, set the refreshable registry value ServerMigratesDotUnderscoreFiles to 0 and if ExtremeZ-IP is running use the Refresh Registry button in the Administrator to read in the new value.

In addition, ExtremeZ-IP contains an optional feature that allows ExtremeZ-IP to delete a dot underscore file after its contents have been migrated into the data file. This feature is disabled by default, but you can enable this feature.

To enable this feature, set the refreshable registry value ServerDeletesMigratedDotUnderscoreFiles to 1 and refresh the registry.

Since ExtremeZ-IP migrates dot underscore information only when necessary, dot underscore migration may occur over time, as ExtremeZ-IP explores new areas of the volume for the first time. ExtremeZ-IP does not perform this migration all at once when the volume first comes online.

If the dot underscore file is locked, or has different permissions than the corresponding data file, the information may not be copied to the AFP_Resource or AFP_Info streams. This fact is logged.

The dot underscore migration is a transition feature and is not designed for simultaneous use with SMB. ExtremeZ-IP does try to deal with AFP clients accessing a file while it is still being written with SMB, but this is not a supported use of the feature. Any changes that occur to dot underscore files after the initial migration is ignored by ExtremeZ-IP, since the service always "prefers" its alternate streams to dot underscore files. Therefore, if a user alters the resource fork of a file over SMB after the resource fork information has been migrated by ExtremeZ-IP, these changes are not migrated.

While dot underscore files can contain information other than resource fork or Finder information, this other information is not migrated into the data file. The following types of information are not migrated:

- File Comments
- Real Name (File's name as created on home file system)
- Icon, B&W (Standard Macintosh black and white icon)
- Icon, Color (Macintosh color icon)
- File Dates Info (File creation date, modification date, and so on)
- Macintosh File Info (Macintosh file information, attributes and so on)
- Short Name (AFP short name)
- Directory ID (AFP directory ID)

NOTE SMB shares will not be migrated on a Windows Cluster Server installation of ExtremeZ-IP.

Migrating SFM and SMB shares after first launch

The prompting for SFM and SMB migration that is described above is only performed once—the first time you launch the ExtremeZ-IP Administrator. After first launch, use the **Migrate SFM Shares** and **Migrate SMB Shares** buttons in the **Volumes** window of the ExtremeZ-IP Administrator to bring shares over as ExtremeZ-IP volumes. See "Creating volumes for use with ExtremeZ-IP" on page 38 for information about migrating volumes.

Naming Conventions for SFM and SMB volumes

Migrated SFM and replicated SMB volumes must adhere to the standards of ExtremeZ-IP volume names. These names cannot exceed 27 characters (for Mac OS 9 support) or 31 characters when represented in UTF-8 Unicode format (for Mac OS X support). If any migrated or replicated shares have names that are too long, the names are truncated. In the event that a migrated or replicated share has a name matching a current ExtremeZ-IP volume, ExtremeZ-IP appends a number to its volume name, e.g. "Volume (2)". The volume name may be truncated in order to have room to append the number.

Running ExtremeZ-IP and SFM

By default, ExtremeZ-IP and SFM use different default names. SFM's default name is the name of the Windows computer; ExtremeZ-IP uses the name of the Windows computer and adds the suffix IP. If you use the default names for SFM and ExtremeZ-IP, you can run ExtremeZ-IP and SFM on different network ports.

If you change the default names so that ExtremeZ-IP and SFM have identical names, either SFM or ExtremeZ-IP will not function properly. If SFM is started first, ExtremeZ-IP file sharing will work but it does not appear in the Chooser. ExtremeZ-IP logs an error in the Event Viewer when this occurs. If ExtremeZ-IP is started first, SFM cannot start up because it cannot register on the AppleTalk network.

If you are using both ExtremeZ-IP and SFM and one or both fails, check for duplicate folders that have been accidently shared from both. Volume names can be the same, but you cannot share the same folder with both.

Installing AppleTalk

When the AppleTalk protocol is installed on the server, ExtremeZ-IP registers itself with AppleTalk. Mac OS 9 clients see ExtremeZ-IP when they open the **Chooser**.

If AppleTalk is not already installed, you can install the AppleTalk protocol for Windows. To install the AppleTalk protocol, add it as a protocol in the Network Control Panel.

NOTE Windows XP, Windows Vista, and Windows Server 2008 do not include AppleTalk.

Using Kerberos

The Massachusetts Institute of Technology created Kerberos to address such network security issues as username/password exchange, network security, client computer security, and login persistence. Kerberos is a protocol that provides secure network authentication and support for "single sign-on" to network resources. With single sign-on support, a user logs in one time to a network domain (also called a *realm*) and, after he or she is authenticated, gains access to resources on other computers without resubmitting a user name and password. Kerberos works on the premise that only the client and authenticating server share a piece of secret information and it provides a way to confirm that the shared information is accurate throughout the user's session.

When a user on a client computer types in a username and password and submits that information to a server to log in, Kerberos first authenticates the user and then issues a *ticket* that uniquely identifies the client for that session. The ticket is used for future access to other applications and shared volumes during the user's session. Kerberos provides encrypted key exchange to ensure security on both internal networks (behind firewalls) and insecure networks such as the internet. Once a user is authenticated, all further communication is encrypted for privacy and security. For more information on how Kerberos works on a Windows Server, go to

http://www.microsoft.com/windowsserver2003/technologies/security/kerberos/default.mspx

ExtremeZ-IP supports the Kerberos extensions in the AFP protocol and works directly with Active Directory. It is registered as a Kerberos service provider and can authenticate Macintosh tickets. Since the tickets themselves are a standard format within

Kerberos, ExtremeZ-IP takes tickets from a Macintosh and passes them to Microsoft Windows Active Directory for authentication and then grants access to Windows server resources if Active Directory says the client has a valid ticket.

Troubleshooting Kerberos

If you are having trouble getting Kerberos to work with ExtremeZ-IP, use the following troubleshooting steps:

To verify that a client computer has communicated successfully with the Kerberos ticket authority and received a ticket for ExtremeZ-IP, run the Kerberos application located in **/System/Library/CoreServices.** The active Kerberos tickets are listed in **Kerberos.app.** In addition, the Kerberos application can be used to destroy existing tickets before their normal expiration time.

To verify that a client computer is bound to the Active Directory Domain correctly and is running the right version of Kerberos modules, try connecting to the server from the Macintosh over SMB instead of AFP by typing **smb://SERVER_NAME** into the **Server Address** field in the **Connect To Server** dialog. If you are required to log in then you will know that there is a general problem with Kerberos.

Setting up ExtremeZ-IP Clustering

Clustering provides fast failover and quick restart of the services provided by a failed server node. You set up an ExtremeZ-IP cluster using Microsoft Cluster Servers (MSCS)—specially linked servers running the Microsoft Cluster Service. If one server fails or is taken offline, the other server or servers in the cluster immediately take over the failed server's operations. Applications running on the cluster are always available. Resources running on multiple servers appear to connected clients as a single system, referred to as an *ExtremeZ-IP virtual server*. When a successful failover occurs because of a problem, the connected user sometimes cannot tell that service was interrupted.

ExtremeZ-IP is a cluster-aware application that you can use on active/active clustered configurations. Multiple instances of ExtremeZ-IP can run on a single server node. Each instance has its own IP address and can be assigned its own shared volume. The configuration of multiple virtual servers provides server consolidation and load management benefits. Running multiple instances of ExtremeZ-IP on a server node provides high reliability because each instance runs in isolation from the others.

For help in configuring a cluster, see the following *Cluster Worksheet*. ExtremeZ-IP supports the following services in clustered configurations:

- active-active clustering
- multiple virtual servers per node in a cluster
- improved reliability and availability
- eight node clusters in Windows 2003 & 2008
- possible server consolidation

When you are running ExtremeZ-IP in a clustered environment, the ExtremeZ-IP Administrator window shows the following in the title bar:

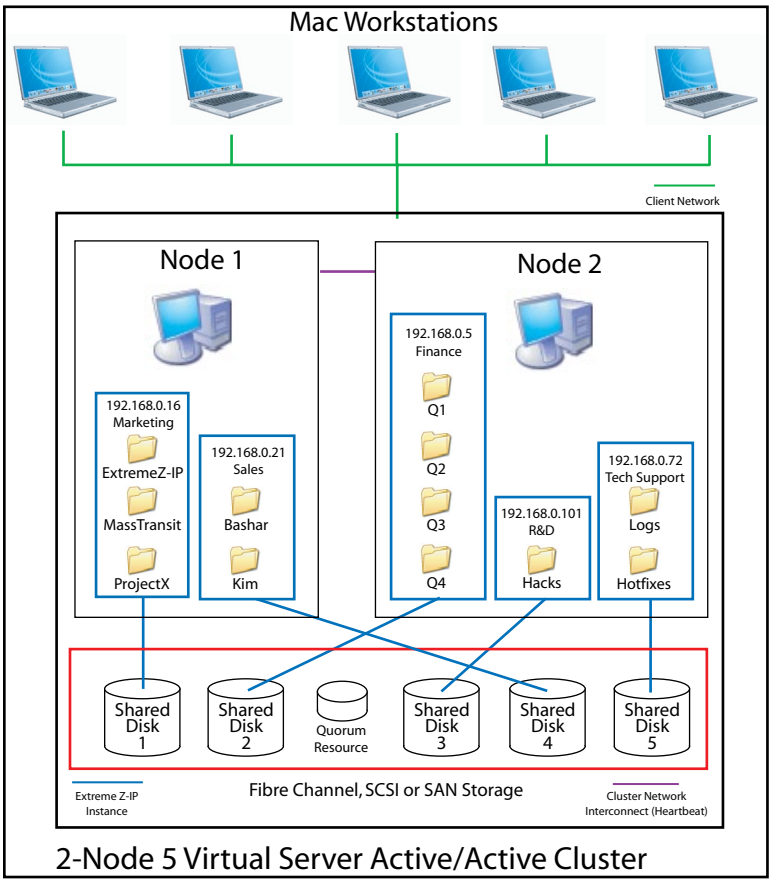
- the name of the server in upper case characters
- the name of the service in upper or lower case as you typed it when you set up the service.

MSCS uses the following terms to describe the component parts of a cluster configuration. Do not confuse these terms as you proceed with installing ExtremeZ-IP.

- **Node**—A single member server in a cluster.
- **Resource**—A hardware or software component that runs in a cluster, such as a disk, an IP address, a network name, or an instance of the ExtremeZ-IP service.
- **Group**—A combination of resources that are managed as a unit of failover. Groups are also known as resource groups or failover groups. A typical ExtremeZ-IP failover group consists of a disk, an IP address, a network name, and an instance of ExtremeZ-IP.
- **Dependency**—A service or other resource that must be available first in order for the dependant service to start.
- **Failover**—The process of moving resources or resource groups from one server to another. Failover can occur when one server experiences a failure of some sort or when you, the administrator, initiate the failover. This term is equivalent to the

Microsoft Cluster Administrator action of moving a Cluster Group to another node.

- **Quorum Resource**—A disk resource containing the failover information that is shared between nodes in a cluster.
- **Heartbeat**—The communication between Cluster nodes tells the other nodes that the service is still running.
- **Virtual Server**—A virtual server is a combination of configuration information and cluster resources, such as an IP address, network name and an application resource. An ExtremeZ-IP Virtual Server (EVS) is defined by its unique IP address.
- **Active/Active**—This term describes a configuration in which multiple nodes are ExtremeZ-IP file servers running in production.
- **Active/Passive**—This term describes a configuration in which one node is active in production and another node sits idle until a failover occurs.
- **Shared Storage**—This term refers to the external SCSI or fibre channel storage system. Shared storage is a requirement for multi-node clusters. Although this storage is shared, only one node can access an external storage resource at any given time.



.

This diagram shows an example of a cluster setup.

NOTE Each server has its own IP address. You can configure multiple shares for each virtual server..

Cluster Worksheet

For each ExtremeZ-IP service running on your cluster you will need the following.

1. A name for the unique ExtremeZ-IP service (the first instance is created by default and is named ExtremeZ-IP)
2. A unique IP address and optionally a network name
3. Shared physical storage
4. A cluster group in which to put the new ExtremeZ-IP service

To simplify this process we have provided a worksheet to prepare for your installation. Duplicate the worksheet for each additional ExtremeZ-IP virtual server you would like to create.

INFORMATION NEEDED TO INSTALL THE SOFTWARE	
ExtremeZ-IP Serial Number:	

For each virtual server you want to set up, you will need to have unique values for all the sections below.

INFORMATION NEEDED TO CREATE A NEW SERVICE	
Unique service name	

INFORMATION NEEDED TO SET UP A NEW CLUSTER GROUP			
Cluster Group name			
IP address			
Network name (DNS/Netbios name)			
Unique service name (created above)			
Volumes to be shared	**Drive Letter**	**Volume Name**	**Is the volume shared with Windows?**

Installing ExtremeZ-IP on a Cluster

Before installing ExtremeZ-IP on a new cluster, you must have installed and configured the clustering service on your servers. On Windows 2003 Server (Enterprise, Storage Node Server, or Datacenter Edition) you will need to install and configure Microsoft Cluster Service. On Windows Server 2008 (Enterprise or Datacenter Edition), you will need to install and configure the Failover Clustering role. In addition, you need the following:

- An ExtremeZ-IP cluster-enabled serial number that is encoded with the number of nodes and virtual servers for which it is licensed. Use a single serial number for all the nodes of the cluster.
- A shared disk or disks where the ExtremeZ-IP shared volumes will reside
- An IP address and network name for each ExtremeZ-IP virtual server you want to create; create a DNS entry for each IP address.

NOTE If folders shared over SMB (for Windows clients) reside on the same physical disk as ExtremeZ-IP shares, Group Logic recommends configuring DFS (Distributed File System) so that your Windows users can use one IP address or host name to access your shared volumes.

Reviewing the Installation Procedure

Installation consists of the following four parts, each with a number of steps that are described in the following sections:

1. Use the installer and serial number provided by Group Logic to install the ExtremeZ-IP on each node of the cluster.
2. Use the ExtremeZ-IP Administrator application to configure the necessary ExtremeZ-IP service(s) on each node of the cluster.
3. Use the Microsoft Cluster Administrator application, provided with Windows 2003, or the Failover Cluster Management application, provided with Windows Server 2008, to configure the Microsoft clustering service.
4. Use the ExtremeZ-IP Administrator application to configure shared folders and other features of the ExtremeZ-IP service.

Configuring ExtremeZ-IP Services

To operate, ExtremeZ-IP requires the following four components:

- IP Address
- Network Name
- Physical Disk
- ExtremeZ-IP Service

Place each set of components in its own cluster group or ExtremeZ-IP Virtual Server (EVS).

The number of EVSs created is based on the number of physical disks that need to be shared out with ExtremeZ-IP. For example, if the volumes are on three physical disks, create three EVSs. This configuration has the most flexibility; however, in some cases you may not want to use up multiple IP addresses. Then you can have multiple physical disks shared out by one EVS. The *Cluster Worksheet* found on page 18 of this chapter can help you set up a plan for your cluster.

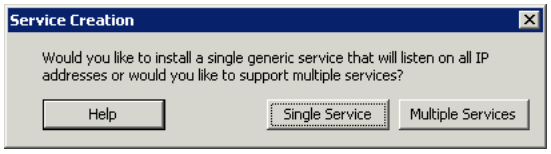
Creating an ExtremeZ-IP Service

Each ExtremeZ-IP virtual server you want to use requires an ExtremeZ-IP service instance. Each of these ExtremeZ-IP services requires a unique **Service Name**. When ExtremeZ-IP is installed on a cluster enabled server, no services are created by default. In this step, you will create a new ExtremeZ-IP service for each virtual server, on each node you want the service to run on.

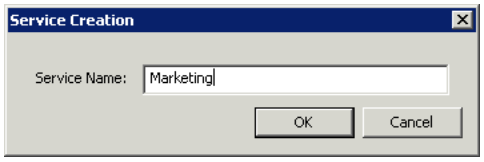
To create an ExtremeZ-IP service, do the following:

1. After completing the ExtremeZ-IP installation process, or on a cluster server with an exiting ExtremeZ-IP installation, run the **ExtremeZ-IP Administrator** application.
2. If ExtremeZ-IP is being installed for the first time and no services exist, you will be prompted to create a service.

3. When setting up a cluster, choose **Multiple Services**.

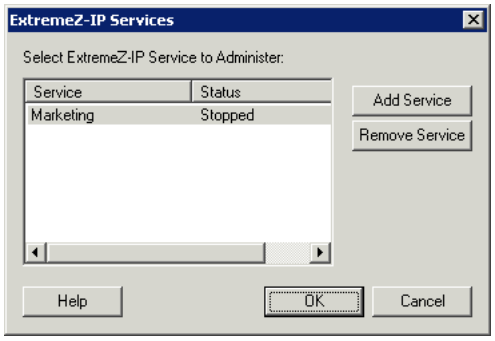


4. You will be prompted to create your first service. Enter the **Service Name** of your choosing. In this example, our service name is "Marketing".

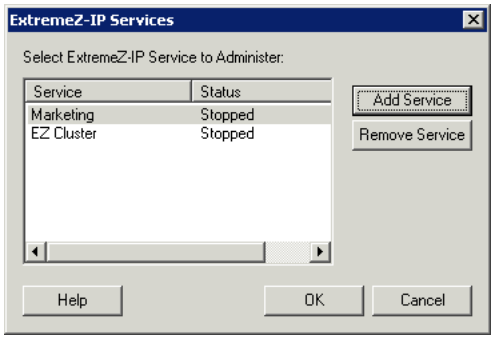


NOTE Write down the exact service name you use in this command. You need the exact name when configuring Microsoft clustering in the next section.

5. After the service is created, it will appear in the **ExtremeZ-IP Services** window. **ExtremeZ-IP Services** will be shown each time the **ExtremeZ-IP Administrator** is launched. It is used to select the service you would like to administer, as well as to add or remove additional services.



6. If you are configuring multiple services, select **Add Service** and to create any additional services necessary.



7. You will need to perform these steps on each cluster node that these ExtremeZ-IP services will run on.

Adding an ExtremeZ-IP Service to a Cluster

You can configure the cluster for ExtremeZ-IP in a number of ways:

- If you already have set up a Cluster Group, simply add ExtremeZ-IP as a generic service to your Cluster Group.
- If you do not have any existing cluster group, follow the steps in the sections below, which take you through the process of using the Cluster Application Wizard® to configure the cluster group.
- Or, you may use another method with which you are familiar.

If folders shared over SMB for Windows clients reside on the same physical disk as your ExtremeZ-IP volumes, you can add the ExtremeZ-IP service to an existing group.

In addition, when using an active/active configuration with Windows SMB shares, you may want to install and configure Windows DFS (Distributed File System). DFS makes it easier for connected users to find shared folders on the network without having to learn multiple IPs or DNS names. For more information, see Microsoft's DFS documentation.

Although the Macintosh client does not support DFS, ExtremeZ-IP has the ability to make DFS volumes available to Macintosh clients. Information on configuring ExtremeZ-IP and Macintosh clients for DFS can be found on pages 36 & 70 of this manual.

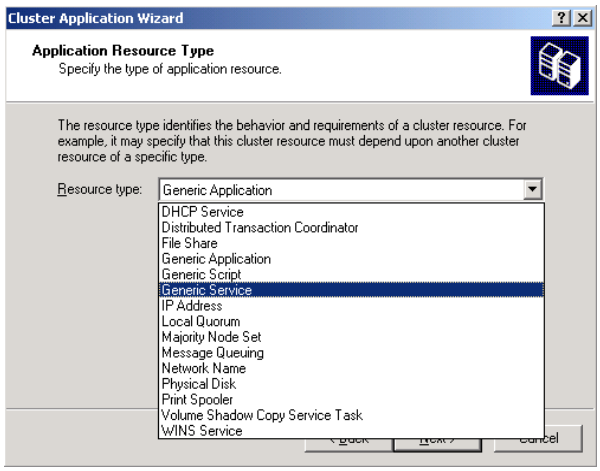
Creating a Windows 2003 Cluster Group

For Windows 2008 instructions, see the next section. The following steps are not the only way to create a new cluster group, but they are generally the fastest and most reliable.

To create a group, do the following:

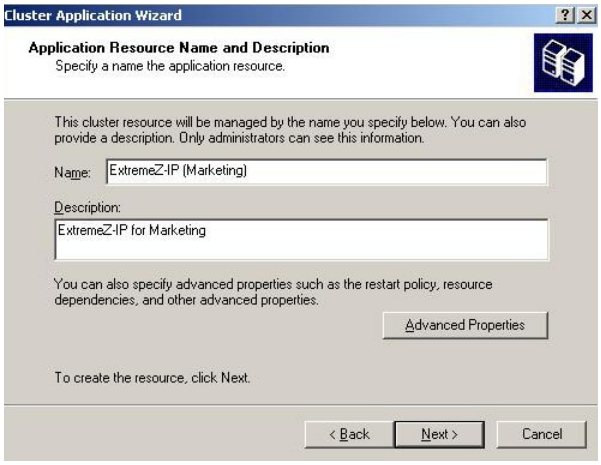
1. Launch **Cluster Administrator**.
2. Right click on **Groups** and select **Configure Application**.
3. Click **Next** to begin the wizard.
4. Select Create a new virtual server and click **Next**.
5. Select **Create a new resource group** and click **Next**.
6. Enter a **Group Name**. Click **Next**.
7. Enter a **Network Name** and an **IP Address**. Click **Next**.
8. Click **Next** on the **Advanced properties for the new virtual server** dialog.
9. Select **Create a cluster resource for my application now** and click **Next**.
10. Select **Generic Service** as the **Resource Type**.

NOTE Make sure you select Generic Service. Selecting Generic Application, which is the default entry, is a common mistake.



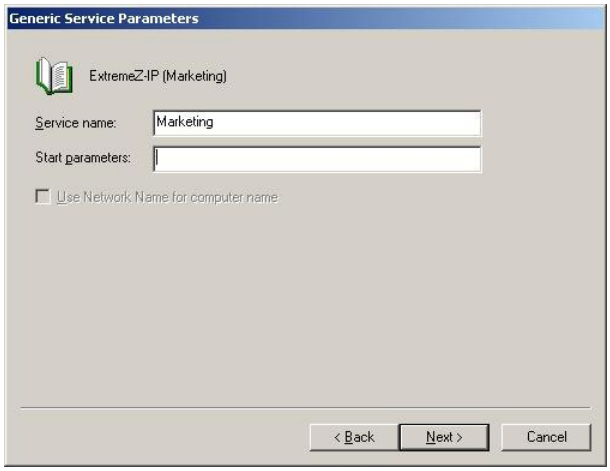
11. Enter the **Resource Name** in the **Name** field.

    Use a meaningful name such as the one used in the examples below—ExtremeZ-IP Service-Marketing.



12. Enter the service name with no **Start** parameters.

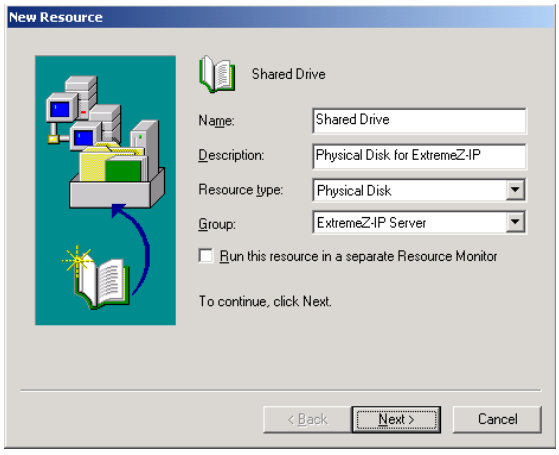
    This name must match the **Service Name** configured in the command line in *Configuring an ExtremeZ-IP Service.*



13. Click **Next** on the **registry replication** dialog. Then, click **Finish.**

To add a disk resource to the newly created group, do the following:

1. Right click on the group and select **New** > **Resource**. Then, select **Physical Disk** in the **Resource Type** drop-down list.
2. Click **Next**.



3. Configure the owners of the **Physical Disk** resource to be all of the nodes ExtremeZ-IP will run under.

   You can add dependencies for the Physical Disk, if needed, but this configuration is not required for ExtremeZ-IP.
4. Select the **Physical Disk** containing the folders you want to share with ExtremeZ-IP, and click **Finish**.

Setting Cluster Service Dependencies

To ensure that cluster services start-up in correct order, you must set resource dependencies for the IP Address, Network Name, and the Physical Disk.

To set resource dependencies for the IP Address, Network Name, and the Physical Disk, do the following:

1. From the **Cluster Administrator**, right click on the **ExtremeZ-IP service resource**.
2. Click **Properties**.
3. Select the **Dependencies** tab.
4. Click **Modify**.
5. Add the **IP Address**, **Network Name**, and the **Physical Disk** as dependencies.
6. Click **OK**.

Since the ExtremeZ-IP resource is created under the virtual server wizard, all the nodes in the cluster are owners for the resource. If you do not want this configuration, you can change it before you bring the service online.

To change the owners for the resource, click the **General** tab and modify the **Possible Owners** accordingly.

Bringing the New Service Online

When you have configured MSCS on all nodes of the cluster for each **Cluster Group** that contains ExtremeZ-IP, MSCS setup is complete. Once you have configured your setup, you can bring the new service online.

To bring the Cluster Group online, do the following:

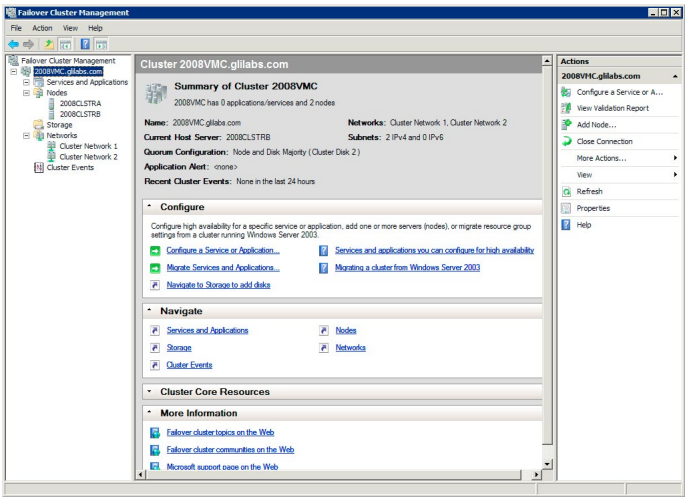
1. Right click the **Group**.
2. Select **Bring Online**.

Creating a Windows 2008 Cluster Group

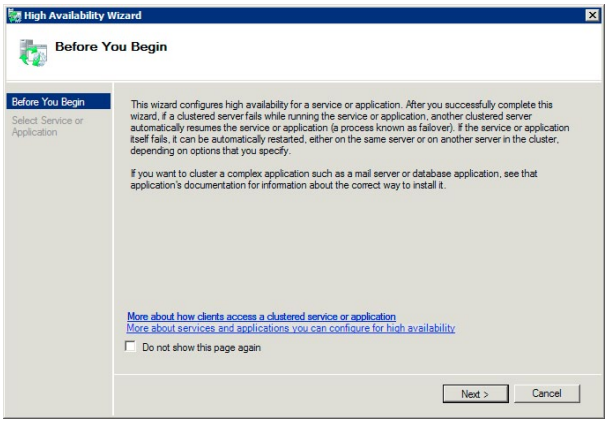
This is the recommended method for creating a new cluster group that includes an ExtremeZ-IP service. If you already have a cluster group configured and would like to add ExtremeZ-IP to that group, right click the cluster group and select **Add Resource - Generic Service**. Then follow the steps below to select the desired ExtremeZ-IP service. This will bypass the cluster group network and storage configuration steps.

To create a cluster group, do the following:

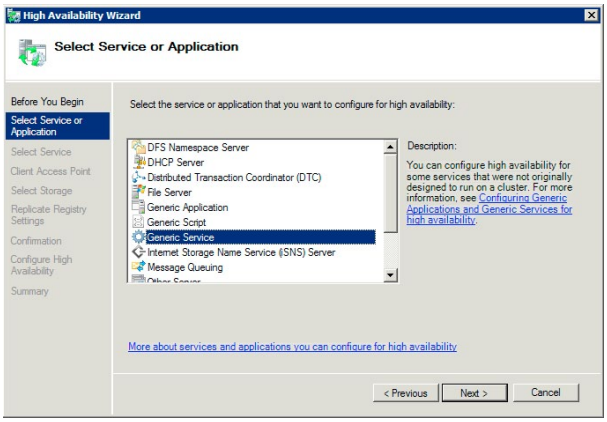
1. Open **Failover Cluster Management** in **Administrative Tools** and select your cluster on the left pane.



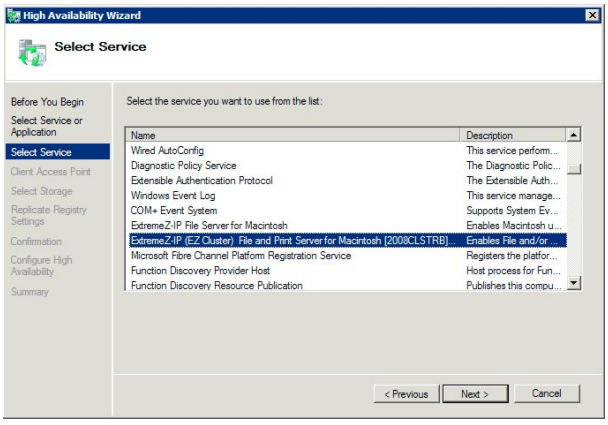
2. Right click on the cluster name and select **Configure a Service or Application**. This will launch the **High Availability Wizard**. Click **Next**.



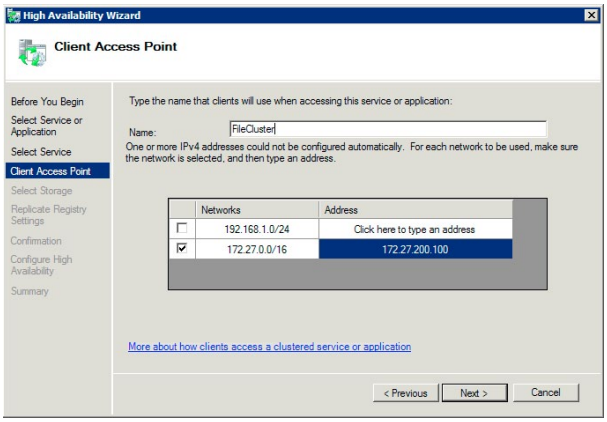
3. Select **Generic Service** and click **Next**.



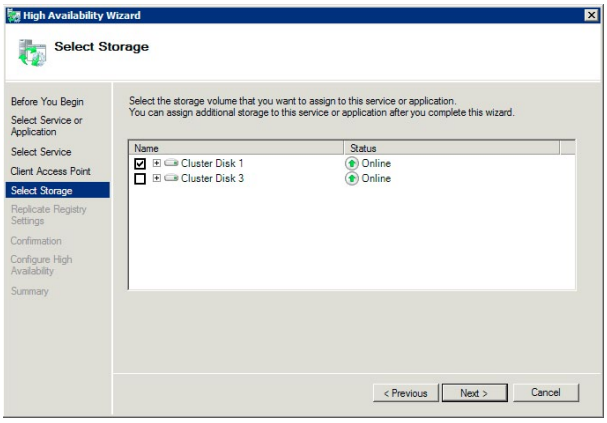
4. You must now select the service to add. You may see multiple entries for ExtremeZ-IP in the list. Each entry will display the ExtremeZ-IP service name as defined when the service was created. See page 19 for further details. Select the entry that includes the specific ExtremeZ-IP service name you would like to configure and click **Next**.



5. Enter the network service name for your cluster group. This will define the DNS name that clients will use to connect to this cluster group. Select the **Networks** that this cluster group will use and define an IP address for the cluster group on each selected network.



6. Select the volume(s) you would like to make available to this cluster group and click **Next**. These should be the volumes that contain the directories to be shared with ExtremeZ-IP.



7. Click **Next** on the **Replicate Registry Settings** step. No changes are necessary.

8. Click **Next** on the **Confirmation** step.

Setting Cluster Resource Dependencies

To ensure that cluster services start-up in correct order, you must set resource dependencies for the IP Address, Network Name, and the Physical Disk.

To set resource dependencies for the IP Address, Network Name, and the Cluster Disk, do the following:

1. From **Failover Cluster Management**, under **Other Resources** for the cluster group, right click on the **ExtremeZ-IP File and Print Server** resource.

2. Click **Properties**.

3. Select the **Dependencies** tab.

4. Add the **IP Address**, **Network Name**, and the **Cluster Disk** as dependencies.

5. Click **OK**.

Since the ExtremeZ-IP resource is created under the High Availability Wizard, all the nodes in the cluster are owners for the resource. If you do not want this configuration, you can change it before you bring the service online.

To change the owners for the resource, click the **Advanced Policies** tab and modify the **Possible Owners** accordingly.

Bringing the New Resource Online

At completion of this configuration, the ExtremeZ-IP resource may be offline. You can now bring the new resource online.

To bring the ExtremeZ-IP resource online, do the following:

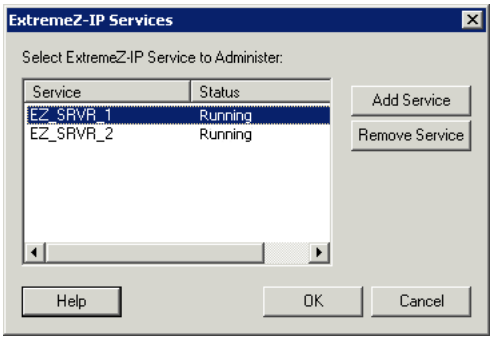
1. Right click the **ExtremeZ-IP File and Print Server** resource.
2. Select **Bring this resource online**.

Administering ExtremeZ-IP on a Cluster

In a clustered environment, the ExtremeZ-IP administrator behaves differently than it does in a non-clustered environment. You should always execute administration tasks on the node currently running the ExtremeZ-IP Virtual Server you want to administer. Starting the service from the ExtremeZ-IP Administrator or the Services control panel is disabled for clustered configurations.

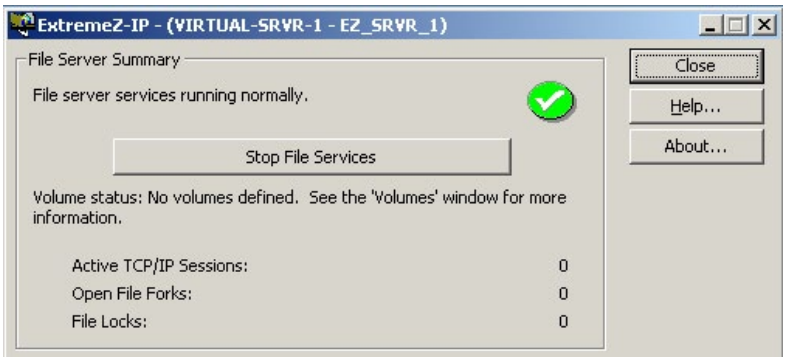
Clustered services should be started ONLY from the Microsoft Cluster Administrator. If the service is started by some other means (an application or the Services control panel) the Cluster Administrator will not know the service is running and, if required, cannot manage a failover.

Administer services only from the node they are running on. Then, you can create volumes that point to a specific folder. On a cluster, a node can only access the disks in its cluster group. In order to select a folder with the **Browse for folder** dialog you must run the ExtremeZ-IP administrator on the node where the Physical Disks are located. Using the ExtremeZ-IP Administrator, you can create a volume on another node; however, you will need to enter the path manually.



When the ExtremeZ-IP Administrator is started, you will be prompted to select the ExtremeZ-IP service that you want to administer. Select an ExtremeZ-IP Service and click **OK**

Once you have chosen a service, the Administrator launches and connects to that service. The Administrator title bar tells you which server it is connected to in the format "(Network Name – Service Name)".



If the connection to the server is broken (that Cluster Group is failed over) the administrator cannot reconnect to that service since it is on another node. However, you can now administer it on the node to which it has been moved. If it fails back to the original node, you can reconnect to it.

ExtremeZ-IP®

EXTREMEZ-IP FILE SERVER

Starting and stopping the ExtremeZ-IP File Server

To start the ExtremeZ-IP File Server, log into Windows with Administrator privileges and launch the ExtremeZ-IP Administrator. If you have not already started the ExtremeZ-IP service, the ExtremeZ-IP Administrator asks if you want to start the service.

In addition, you can start and stop the service from the Service Control Panel on a standalone server or the Cluster Administrator on a cluster server.

Configuring the ExtremeZ-IP Server

This section gives an overview of configuring the ExtremeZ-IP service. Use the ExtremeZ-IP Administrator to view, disconnect, and send messages to connected users, create shared volumes, and adjust specific machine settings. You can configure the local computer or remote computers on which ExtremeZ-IP is installed as long as you have Administrative privileges.

To configure ExtremeZ-IP on the computer you are using, from the Windows **Start** menu, go to **Programs/ExtremeZ-IP** and select **ExtremeZ-IP Administrator**.

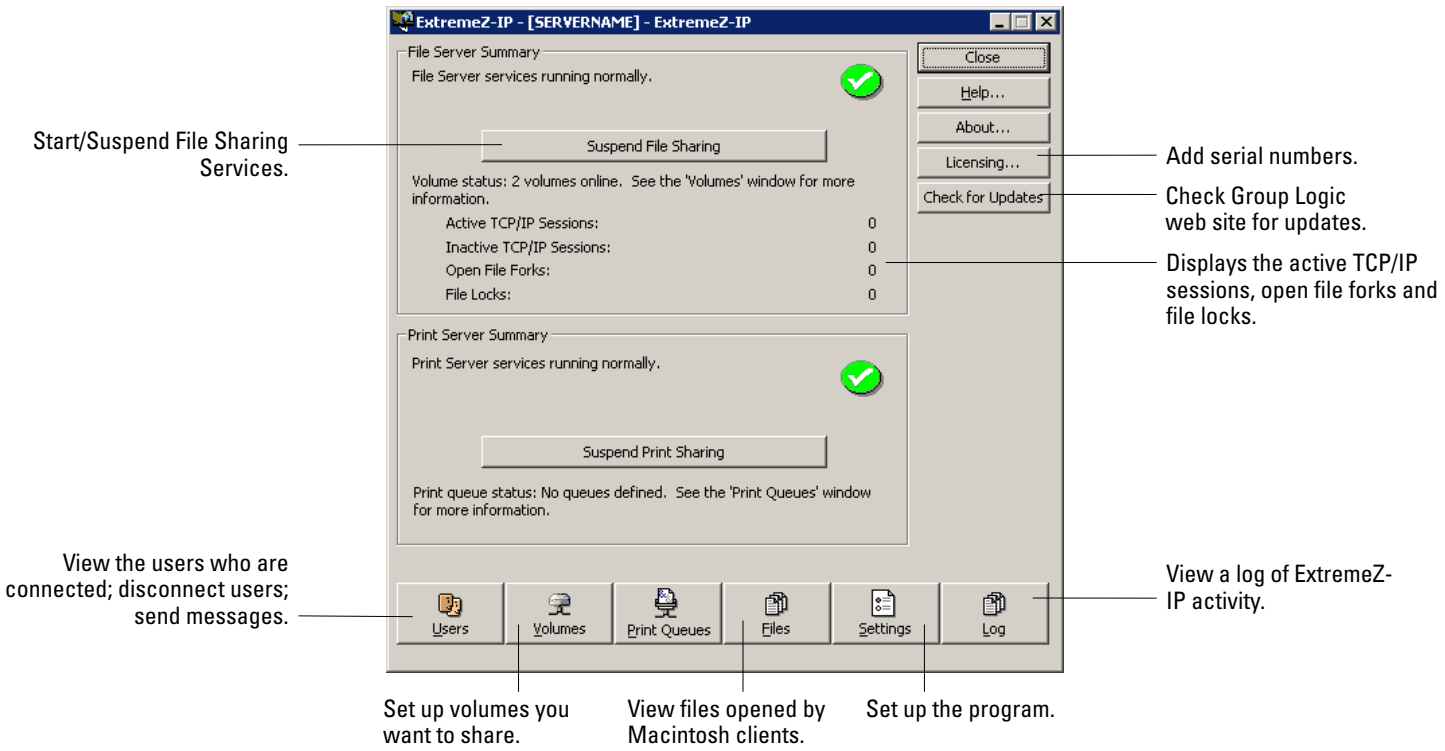
NOTE In addition to the method described above, you can configure ExtremeZ-IP from the command line using the EZIPUTIL.EXE. For more information about EZIPUTIL.EXE see the appendix.

Setting up ExtremeZ-IP

Before using ExtremeZ-IP, review the default settings; you can make changes at this time or later. The **Settings** dialog box has the following tabs: **File Server**, **Print Server**, **Security**, **Search**, **Filename Policy, Service Discovery,** and **DFS**.

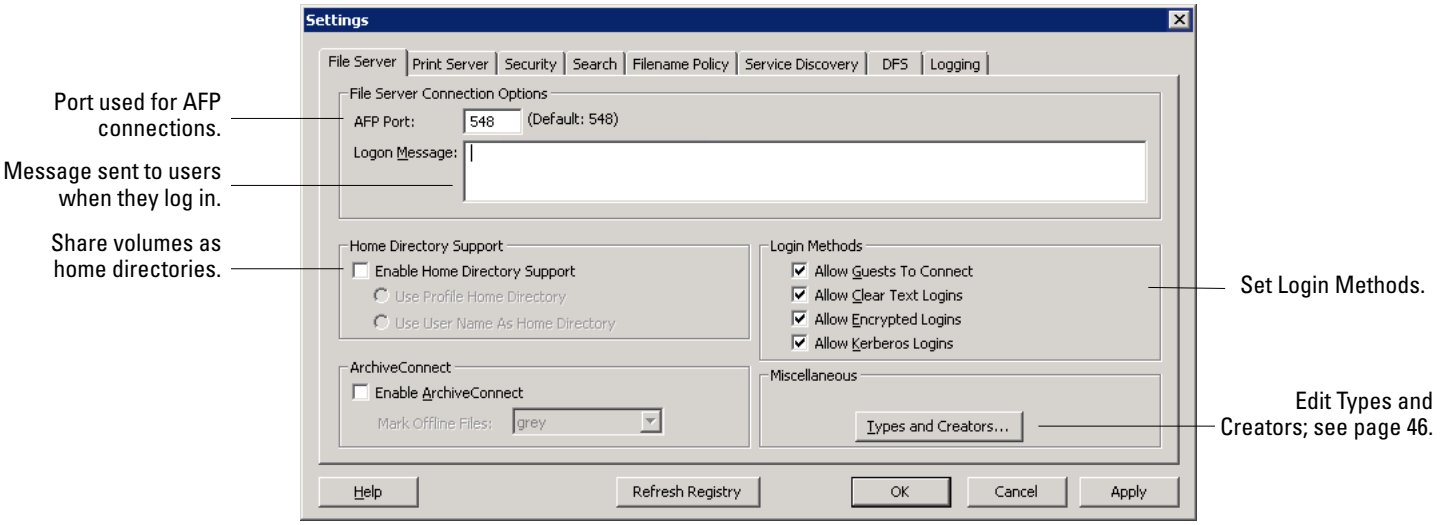
To change settings, do the following:

1. Access the **ExtremeZ-IP Administrator** window.
2. Click **Settings**.
3. Choose the settings appropriate for your use, then click **OK** to return to the ExtremeZ-IP Administrator window.



Setting File Server Options

Use the **File Server Settings** tab to change the way ExtremeZ-IP interacts with Mac clients when it offers file sharing services.



AFP Port

If required for your connection, make changes to the **AFP port.** Although rarely necessary, you can type a new port number for the TCP/IP port the file server uses; the default is 548.

NOTE If Macintosh clients cannot connect to your server, ExtremeZ-IP may be running on a port other than the default. In this case, ExtremeZ-IP displays a message on the ExtremeZ-IP Administrator window warning you that you have picked a non-default port.

Logon Messages

The logon message displays on the Macintosh users' computers after they successfully log in. Leave the message blank if you do not want clients to receive a message when they log in.

To increase the number of characters you can use in the message you send to clients, use the registry key. You can use as many as 500 characters; Macintosh clients using Mac OS 9 see fewer characters.

Enabling Home Directory Support

If you are using some ExtremeZ-IP volumes exclusively for home directories, check **Enable Home Directory Support.** In addition, you must enable home directory support for individual volumes when you set up the volumes; see page 39, the **Volume Properties** dialog box. This setting filters out all directories except the user's home directory when the user asks for the contents of the volume. Users do not see home directory volumes that do not contain their home directories. If your users' home directory locations are specified in their Microsoft Active Directory profile, choose **Use Profile Home Directory**. If your users' home directories are named to match their user names, choose **Use User Name As Home Directory**.

See the Knowledgebase article: http://www.grouplogic.com/knowledge/index.cfm/fuseaction/view/docID/210

Changing Types and Creators

Click the **Types and Creators** button to fill out the Macintosh Type/Creator to **Extension Mappings** dialog box to meet your specifications. See *Remapping Extensions* on page 45 for more information on remapping MS-DOS extensions to Macintosh types.

Allow Guests to Connect

If you choose to allow guests to connect, a Macintosh user can log into the file server without supplying a name and password. Permission to connect does not give Macintosh clients access to your entire computer. You designate which volumes on your computer you want to share with Macintosh clients. See *Volumes*, page 38 in this chapter. The user's privileges during that session are limited to the permissions normally given to the **Everyone** group under Windows.

NOTE You must configure Windows XP and later Windows systems so that guests can access the server. See *Configuring Guest Access for Windows XP and above* in Appendix D on page 79.

Allow Clear Text Logins

Checking this option lets Macintosh users connect by sending their passwords in clear-text form over the network. Clear-text passwords may be a security problem and are limited to 8 characters. Mac OS X versions 10.5 and later do not allow clear-text authentication.

Allow Encrypted Logins

If you select this option, Macintosh users can encrypt their passwords before sending them across the network. With encryption, users have greater security and can use longer passwords.

Allow Kerberos Logons

This option provides support for "single sign-on" to network resources. It applies only to users with Mac OS X 10.3.5 or greater. See the earlier section on page 15 which describes Kerberos in more detail.

Enable ArchiveConnect

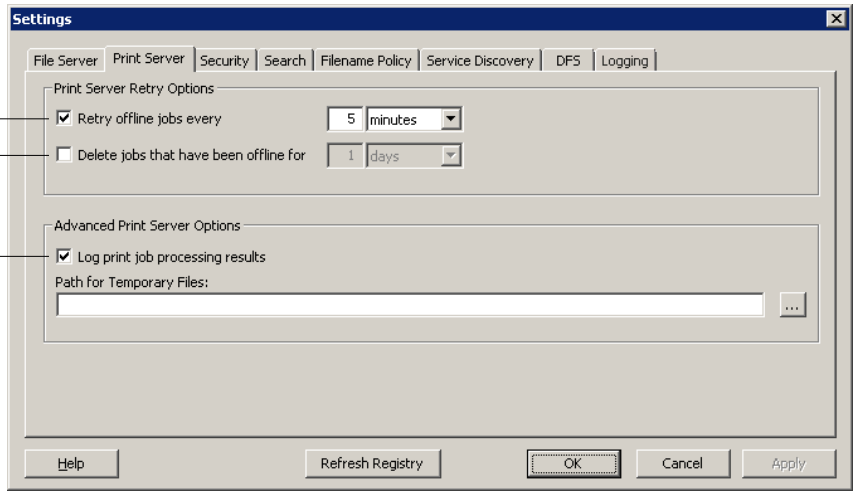
This option turns on enhanced ArchiveConnect support for any file archive volumes shared with ExtremeZ-IP. ArchiveConnect is a separate Mac client-side application that enables Mac OS X clients to access file archives without triggering unintended retrieval of offline files.

Mark Offline Files

Select a custom label color that will be used to highlight offline files within the Mac OS X Finder.

Setting Print Server Options

To make changes to Print Server Settings, click **Settings** on the ExtremeZ-IP **Administrator** window, then click the **Print Server** tab. Changes you make to print server settings take effect immediately after you click the **Apply** or **OK** button.



Automatic Retry of Print Jobs

When a job fails for any reason —LPR error code, TCP connection terminated, error from Windows print queue—the job status is set to *Offline* and it is sent to the end of the queue. Use the **Print Server** tab to configure the interval that will elapse before the server retries printing the job. By default, ExtremeZ-IP automatically retries offline jobs every five minutes until the job prints successfully. To disable this feature, uncheck the **Retry offline jobs every . . .** box. You can enter only one auto-retry interval, which applies to all offline jobs.

Deleting Offline Jobs

ExtremeZ-IP can also automatically delete jobs that have been offline for a specified period of time. This functionality is disabled by default, and, when enabled, the default setting is one day. To enable this feature, check the **Delete jobs that have been offline for . . .** box.

NOTE In order to make sure that jobs aren't automatically deleted because of a queue-wide problem, such as a network problem, or printer turned off, ExtremeZ-IP will not automatically delete a job after the configured period of time unless at least two other jobs have been successfully printed since the job went offline.

For the purposes of our performance counters, any queue that has more than one offline job and has not successfully processed a job since the last job went offline is considered an *offline* queue. So a single offline job does not make a queue offline—it could just be a bad job, but having multiple offline jobs without any recent successful jobs would suggest that a queue-wide problem exists. A queue that is offline does not differ from an online queue in terms of its processing; how it is reported in performance counters is the only difference.

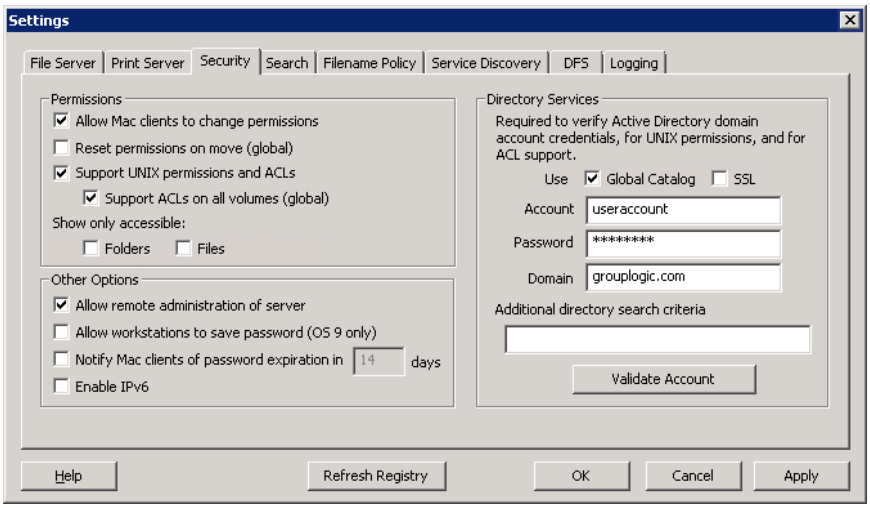
Advanced Print Server Options

If you want each print job to be logged in the Windows Event Log, check the Log print job processing results box. You can enter a location for storing temporary files; as a default, ExtremeZ-IP uses the default temporary directory.

Setting Security Options

On the **Security Settings** tab, place a check in the appropriate checkbox to change permissions and other options.

Enter information for **Directory Services** in the appropriate text boxes.



Allow Mac Clients to Change Folder Permissions

If you select this option, Macintosh clients can change folder permissions. With this option disabled, Mac clients are prevented from changing permissions the Windows Administrator has set on the server. Many Macintosh applications set unexpected permissions without user intervention. For increased reliability, it is recommend that Mac clients not be allowed to modify permissions unless this capability is required for a particular workflow.

Reset Permissions on Move

If you select this option, the behavior of the move operations changes so that, when folders or files are moved, their permissions are changed to those of their new parent folder.

Support UNIX permissions and ACLs

UNIX permissions and Access Control Lists (ACLs) require that the ExtremeZ-IP service have access the list of users in Active Directory in order to resolve SID, UUID, UID, and name mappings. For UNIX permissions, the Macintosh client requests a name mapping for UID. However, for the 'ls' command the Macintosh uses AD and does the name mapping internally. Therefore, the Macintosh does not make a name request to ExtremeZ-IP. If the UID ExtremeZ-IP provides does not match the user's UID obtained from Active Directory, then the Macintosh will not allow the user to change UNIX permissions at all. In addition, the client will not be able to determine the user's group membership or if the user is the owner.

To verify your account, enter the requested information in the **Directory Services** text fields. This account will be used to search Active Directory to resolve account IDs. By default, ExtremeZ-IP will search within your entire Active Directory forest to validate security credentials. If you would like ExtremeZ-IP to only search the **Domain** specified, uncheck the **Use Global Catalog** option. Add additional search criteria, if necessary, and click **Validate Account**.

If the credentials are invalid, the service will not be able to access Active Directory and UNIX permissions will be disabled.

ExtremeZ-IP DFS support requires that this option is enabled and that valid Directory Service credentials are entered.

Support ACLs on all volumes (global)

To support ACLs on all volumes, check this box.

Show Only Accessible: Folders, Files

If you check the **Folders** option, users will see only folders that they can access. If you check the **Files** option, users will only see files that they can access.

Allow Remote Administration of Server

This option lets Windows users, who have Administrative privileges, use the Remote Administration features of ExtremeZ-IP to configure the server remotely; see *Administering ExtremeZ-IP Remotely* on page 37.

Notify Mac Clients of Password Expiration

You can require that Active Directory users change their sign-on password after a specified time. With this textbox, you can notify Macintosh users that their old passwords are about to expire and ask them to create new passwords.

Enable IPv6

If you would like to use IPv6, check the **Enable IPv6** checkbox. On some versions of Windows you will need to install IPv6 manually before services such as ExtremeZ-IP will be able to use it.

Verify Directory Services

UNIX permissions and ACLs require access to Active Directory in order to resolve SID, UUID, UID, and name mappings. For UNIX permissions, Finder requests a name mapping for UID. However, for *ones*, the Macintosh uses AD and does the name mapping internally. Therefore, the Macintosh does not make a name request to ExtremeZ-IP. If the UID ExtremeZ-IP provides does not match the user's UID obtained from Active Directory, then the software will not allow the user to change UNIX permissions at all. In addition, the client will not be able to determine the user's group membership or if the user is the owner.

To verify your account, enter the requested information in the **Directory Services** text fields. Add additional search criteria, if necessary, and click **Validate Account**. The **SSL** option can be selected to enable secure SSL communication with Active Directory.

If the account is not valid, you may not be able to access Active Directory and UNIX permissions support will not be enabled. In addition, DFS support will not function.

Searching with ExtremeZ-IP

The Mac OS performs three types of file searches – enumeration searches, index searches, and Spotlight searches.

Enumeration Search

When the Mac OS performs an enumeration search, it scans each file in the folder and all of its subfolders across the network. An enumeration search is performed if searching a subfolder of a volume or if catalog search is disabled. The process of the client enumerating the entire directory structure below the folder being searched results in drastically reduced search performance.

Index Search

An index search issues a single search request that is processed on the server side. The Mac OS only issues an index search request when the Macintosh user is searching the root of a volume.

ExtremeZ-IP maintains a search index to accelerate these searches. This index contains the name of every file on your ExtremeZ-IP volumes. With indexed searching enabled on the server, a Macintosh client can use the built-in Mac OS search functionality to perform fast searches of ExtremeZ-IP volumes. No client side configuration or applications are necessary. Instead of scanning your server's drive each time a Macintosh client makes a search request and looking through every file in the volume, ExtremeZ-IP checks the file name index to retrieve search results. Index search results can be provided only for searches initiated at the root of a volume. Any search performed below the root of a volume will result in the Mac OS performing an enumeration search.

NOTE Please instruct your users to search the entire ExtremeZ-IP volume for the fastest results.

Spotlight Search

Mac OS X 10.5 or later supports Spotlight searching of AFP file servers. Spotlight search allows files to be found by searching on content, in addition to file names and file attributes. When enabled, Spotlight search replaces both enumeration and catalog search and provides results when searching at both the root of a volume and within subfolders.

Storing Search Index Files

ExtremeZ-IP creates a separate search index file for each ExtremeZ-IP volume; the search index files are stored in a folder called ExtremeZ-IP indexes. Placing index files in one location and excluding this folder from scanning prevents problems with virus scan software and backup applications. You can specify custom index file paths for individual volumes when you set up or modify a volume to be shared; see the section *Creating Volumes for Use with ExtremeZ-IP* starting on page 38.

NOTE To help you locate a search index for a volume, ExtremeZ-IP begins each index file name with the name of the volume to which it belongs.

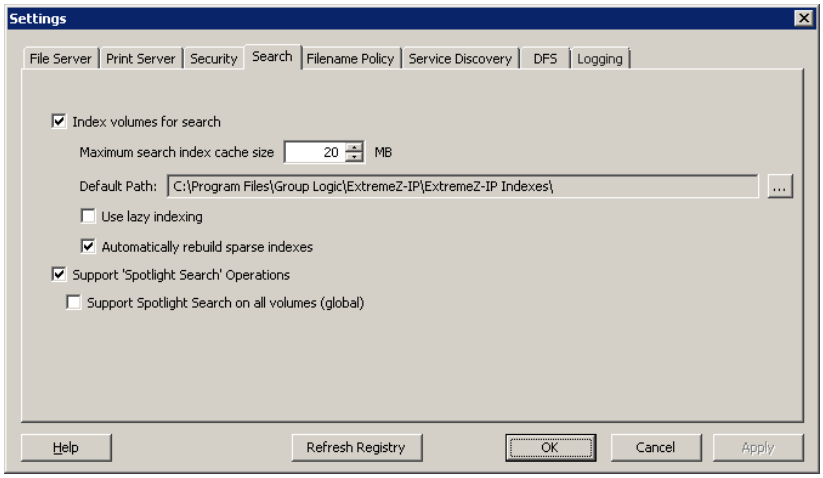
If you do not create a custom path, search index files are stored in a one of two locations.

- ExtremeZ-IP stand-alone server: Search index files are stored in a folder called ExtremeZ-IP Indexes in the ExtremeZ-IP application folder or the custom global location you have set.
- ExtremeZ-IP Cluster: Search index files are stored in a folder called ExtremeZ-IP Indexes at the root of the drive on which the volume resides.

When starting EZIP for the first time, search indexes for a volume is created in the default index path unless you have set individual custom paths for a particular volume or volumes.

Setting Search Options

To set search options, check the appropriate boxes and enter the relevant information.



Index volumes for search

By default, indexed searching is enabled on all existing and newly created volumes. You can disable or enable indexed searching on a per volume basis in the individual volume's **Volume Properties** dialog in **ExtremeZ-IP Administrator**. See page 39. You can set this property at initial volume creation time or after the volume has been created. In order for changes to this setting to take effect, you must stop and restart the ExtremeZ-IP File Services for Macintosh service.

Maximum search index cache size

This cache is set to a maximum size of 20 MB by default. Group Logic does not recommend changing this cache size. An index file containing 250,000 files is only about 8 MB in size. Leaving the cache limit at the default setting gives sufficient performance in almost all cases. If the index files on disk are larger than search index cache size, the file will be read from disk when the client does a search; however in many cases the file will be in the Windows file system cache so performance impact is minimal. When the server is running with limited physical memory, the cache size can be reduced to as little as 8 MB.

Default Path

By default on a standalone server, ExtremeZ-IP stores index files in the ExtremeZ-IP Indexes directory in the ExtremeZ-IP application folder. If you would like to locate the index files in a different location, click **Browse** to select a new folder.

NOTE If you modify the default path while ExtremeZ-IP is running, all index files for volumes without individual custom paths are created in the new location.

Administrators can also specify custom index file paths for individual volumes; this setting overrides the global default path setting.

Use lazy indexing

By default, indexed searching uses any available system resource to keep its indexes current and cooperates with other system processes. It should not affect overall system performance adversely. However, when a server is under high load or is running many different services simultaneously, you can limit the system resources that search indexing consumes by enabling the **Use lazy indexing** checkbox. This setting takes effect immediately.

Automatically rebuild sparse index

In order to optimize runtime performance, the ExtremeZ-IP index file entries for files that have been deleted or moved from a volume are not physically removed from the index file at the time the actual file is deleted. The indexed search service ignores these deleted entries to keep search results accurate. However, the index file grows over time and, as the file gets larger, slows search performance to a small extent. The rate at which the index file grows is dependent on the number of files being added, moved, and deleted on the file server. In order to keep ExtremeZ-IP search performing at optimal levels, volumes' indexes are routinely re-indexed and compacted. The interval at which this occurs is determined by the ratio of deleted (stale) records to valid entries in the index. By default, the ExtremeZ-IP search service re-indexes an individual volume when approximately one-third of that volume's index file records are deleted, stale records.

Maintenance occurs on a per volume basis and only on volumes requiring re-indexing. While re-indexing, the volume's existing search index is kept up to date and used to provide one hundred percent accurate search results. Re-indexing should not have any detrimental effect on other server processes while it is running. While ExtremeZ-IP is re-indexing an individual volume, a status of "Reindexing" shows in the **Volumes** dialog of the ExtremeZ-IP Administrator.

If you prefer, you can schedule re-indexing on a set schedule during off-hours. You can use an EZIPUTIL command, described on page 75 used in a batch file or script and triggered by a scheduling service of your choice. If you choose this method of scheduled re-indexing, disable automatic re-indexing by removing the check in the **Automatic rebuild of sparse indexes** setting checkbox.

Support 'Spotlight Search' Operations

Support for Spotlight Search of shared volumes can be enabled by checking this option. You can enable or disable Spotlight searching on a per volume basis in the individual volume's **Volume Properties** dialog. See page 39. You can set this property at the time of initial volume creation or after the volume has been created. Enabling this setting takes effect for all new sessions using the volume.

In addition to enabling this setting, Spotlight Search requires that the Microsoft Windows Search application be installed on the ExtremeZ-IP server and be configured to index any volume where Spotlight Search is enabled. Windows Search is built into Windows Server 2008 and Windows Vista and no additional installation is required. Windows Search can be installed on Windows 2003 Server and Windows XP by running Windows Update. It is listed as an optional install. Once installed, Windows Search can be configured to index the necessary volumes by right clicking the Windows Search icon in the Start bar and selecting **Windows Search Options**.

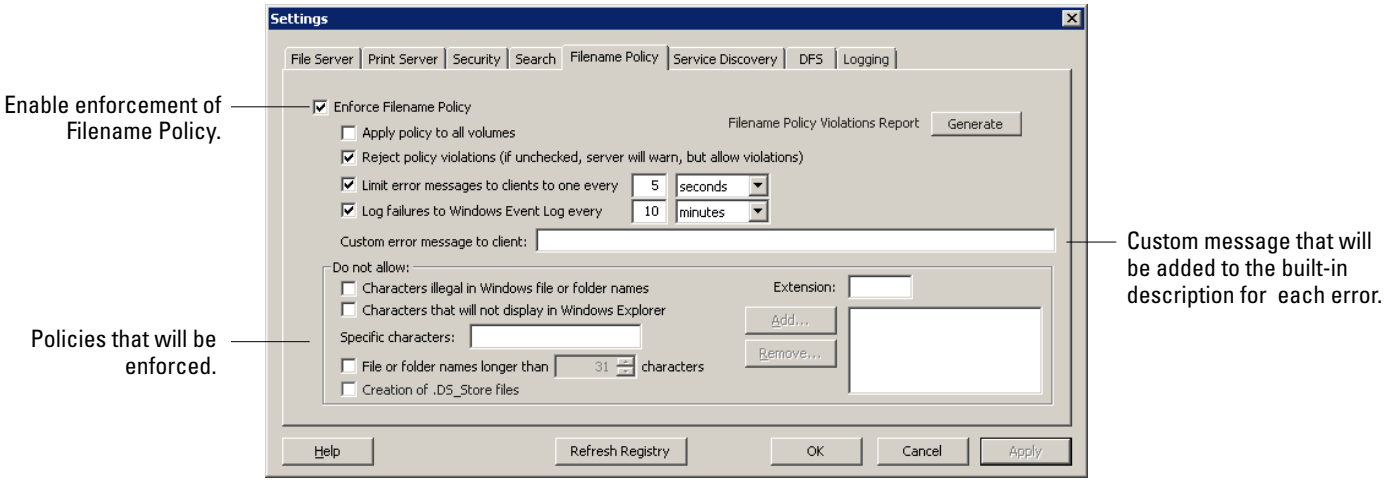
Support Spotlight Search on all volumes

To support Spotlight Search on all volumes, check this box.

Setting Filename Policy

Because ExtremeZ-IP sits in a key position between the file server and the Macintosh client, we can enforce policies on valid file names as well as file types to prevent the Macintosh users from breaking workflows. You can configure ExtremeZ-IP to detect and reject the Macintosh client attempting to save (create, rename, move) files with characters that are "illegal" in Microsoft Explorer or other applications that don't support the Unicode file system APIs. The administrator can configure what is allowed or deemed illegal. This list can include characters that cannot be displayed on Windows, "trailing spaces" Unicode characters not available in the default Windows font, any specified character, file names longer than "x" characters, or specific file extensions.

NOTE Filename Policies do not affect existing files on the server or files that are copied using Windows file sharing.



Enforce Filename Policy

Checking this setting will allow you to enforce filename policies set in ExtremeZ-IP.

Filename Policy Violations Report

A report listing all existing files and folders that violate the presently configured filename policy can be created by clicking the **Generate** button. A confirmation dialog box will appear and allow you to access the folder containing the report's output. This folder will contain a Report Summary text file and individual, comma-seperated summary files for each ExtremeZ-IP volume on the server. These CSV files can be viewed in a spreadsheet application or text editor.

Apply policy to all volumes

You can enforce filename policies globally or on a per volume basis. A globally enabled feature takes precedence over a per-volume setting. Checking this setting applies filename policies across all ExtremeZ-IP volumes and overrides individual volume policy settings.

Limit error messages to clients to one every

Checking this setting limits the number of error messages to one for each client at the specified time interval. You can set the time interval.

Log failures to Windows Event Log every

If you check this setting, the server will log errors to the Windows Event Log at the specified time interval.

Custom message on error

You can specify a custom message that will be appended to the standard filename policy error messages. For example: "This action violates company policy regarding filenames." would lead to the following message being sent to the user: "File 'foo.mp3' cannot be created because the 'mp3' extension is not allowed. This action violates company policy regarding filenames."

Do Not Allow

In this section, set characters, filenames, and extensions that your Macintosh users will not be able to save to your file server .

Characters Illegal in Windows Filenames—If you check this setting, users cannot save files with names that include characters illegal in Windows. The characters are / ? < > \ : * | and trailing spaces and trailing periods.

Characters Not Displayable in Windows Explorer—If you check this setting, users cannot save files with names that include

characters that cannot be displayed in the font used by Windows Explorer (the default is Tahoma).

Specific Characters—You can specify additional characters that you do not want users to include in filenames. Type the characters in this field without separators.

File or Folder names over—You can limit file or folder names to a specified number of characters.

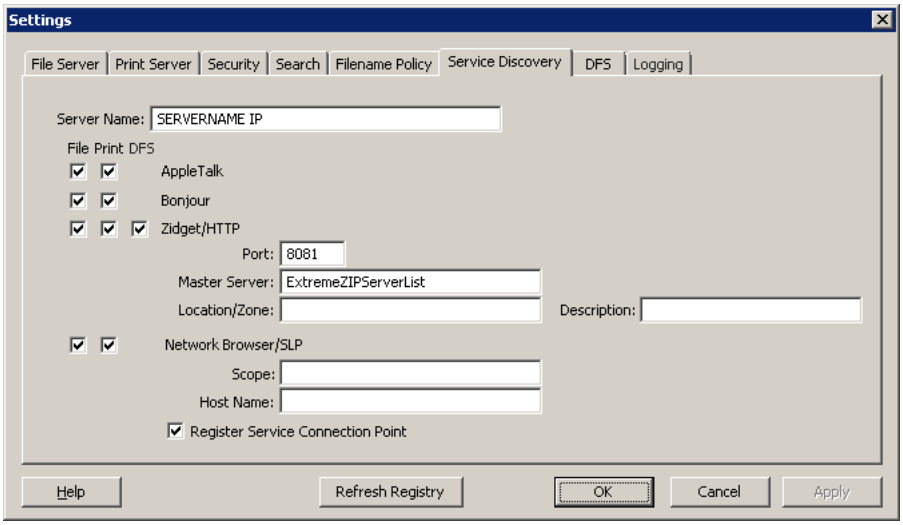
Creation of .DS_Store files—You can prevent Macintosh clients from saving .DS_Store files.

Extension—You can restrict users from saving specific file extensions, such as mp3, mov and wav, by typing in the extension without the (.) dot precursor and clicking **Add**. To remove extensions from the list, highlight the extension and click **Remove**.

Service Discovery

Macintosh clients can use a number of different protocols to discover an ExtremeZ-IP server, depending on what operating system is being used and how the administrator configures the server.

Select the network protocols you want the server to use to register with—AppleTalk, Bonjour, Zidget/HTTP, or SLP— by placing a check in the appropriate checkboxes. The protocols available for discovering file, print, and DFS resources can be configured independently.



Server Name

The Server name appears in the login window whenever a Macintosh user connects to the server. This name also appears in the Mac OS X **Connect to Server dialog** and on earlier Mac OS systems in the **Chooser** and the **Network Browser** when Macintosh users browse the network. You may change the name; use uppercase and lowercase text.

AppleTalk

The AppleTalk protocol is primarily used by the Mac OS 9 **Chooser**. When AppleTalk is selected, Mac OS 9 users can see volumes and print queues in the **Chooser** without specifying the IP address, and Mac OS X users can see them in **Connect to Server** and **Add Printer dialogs**. To register the server on AppleTalk, the protocol must be installed on the Windows server. Windows XP, Vista, and Windows 2008 Servers do not include AppleTalk support.

Bonjour

Bonjour allows Mac OS X users to see volumes in the **Connect to Server** dialog and print queues in the **Print Center**.

Zidget/HTTP

The ExtremeZ-IP Zidget is a replacement for AppleTalk and Bonjour service discovery that works across subnets without your having to configure your router. The Zidget uses XML over HTTP to retrieve a list of ExtremeZ-IP servers and their Print Queues from a Master ExtremeZ-IP server. By default this master server is named ExtremeZIPServerList. If there is a DNS entry in the default domain for ExtremeZIPServerList, then Macintosh clients ask that server for a list of all the ExtremeZ-IP servers on the network. They then query each server individually for its default zone or location and any print queues that it hosts. Because the ExtremeZ-IP Zidget uses standard HTML and XML, the administrators can use this protocol to create their own web interfaces as well. More details about how to do this can be found in the Zidget section of the manual.

Port

Enter the port used for client server communication between the server and Zidget and Print Accounting.

> **NOTE** Even if you turn off Zidget/HTTP ExtremeZ-IP still uses this port to support the legacy ExtremeZ-IP Print Components and Print Accounting. Only the new features are disabled.

Master Server

Zidget supports connecting to a single master server to discover the other ExtremeZ-IP servers on the network. By default this is set to ExtremeZIPServerList. It is recommended that you keep this setting and create a CNAME record in DNS pointing to the host name of your master server. You can change it to any server name listed in the DNS.

Location

This field specifies the location of the server. It is similar to an AppleTalk zone, but allows for multi-level hierarchies. The location is also the default location of print queues on the server, but you can assign a different location on a queue by queue basis. Zidget groups the AFP Server and print queue display based on location. If you want to have a hierarchy of locations, such as 1100 N. Glebe RD, Arlington, Virginia, enter the locations separated by colons ("Virginia:Arlington:1100 N. Glebe RD").

Description

The optional description for the server. Zidget displays this description when the user selects a file server.

SLP

With SLP, Mac OS 9 users can see volumes and print queues in the Network Browser. Type the name of the SLP scope (or Neighborhood) in which you want the file server to appear when Mac OS 9 clients use the Network Browser. Type a host name, which is the name of the server provided to Macintosh clients when they use the Network Browser.

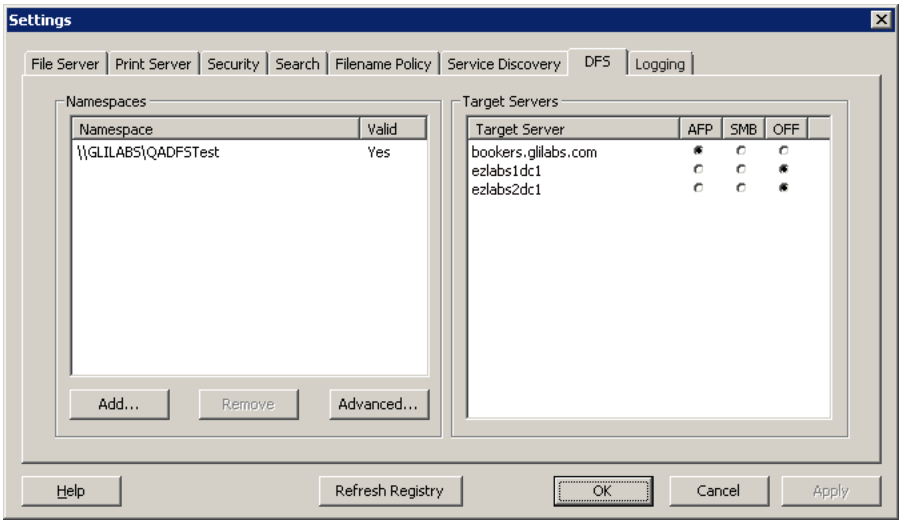
Register Service Connection Point

This option allows ExtremeZ-IP to publish its existence using a Microsoft Service Connection Point (SCP). This technology is used to locate and contact other ExtremeZ-IP servers in your Active Directory.

DFS

ExtremeZ-IP can be configured to make a Microsoft Distributed File System (DFS) available to Macintosh clients. In addition to the server side configuration, installation of the ExtremeZ-IP Zidget dashboard widget (for Mac OS X 10.4 or later), or either a client application or an update to a configuration file (for Mac OS X 10.5 or later) is required for each Macintosh client that requires access to DFS. Details on the required client side configuration can be found on page 70.

DFS support also requires two settings on the **Security** tab of the **Settings** dialog. Valid **Directory Services** credentials must be entered and **Support UNIX Permissions and ACLs** must be enabled for DFS to function.



Namespaces

To add a namespace, click the **Add** button. You will be prompted to enter the path of your DFS namespace.

ExtremeZ-IP will attempt to verify that the DFS namespace entered is valid. If it is not valid, you will be prompted to correct the DFS namespace path.

ExtremeZ-IP will automatically create a DFS virtual root volume in the 'ExtremeZ-IP DFS Volumes' folder, located in the ExtremeZ-IP program directory. This volume will contain links to target servers in the DFS namespace and will be added as a shared volume with a volume name matching your DFS domain or host server name. The location where DFS virtual root volumes are created can be modified by selecting **Advanced** on the **DFS** settings tab.

You are returned to the **DFS** tab, which is updated with the newly added namespace's information. You will find your namespace listed on the left and the target servers in that namespace listed on the right. The **Valid** column in the **Namespaces** list will indicate if the namespace was successfully validated.

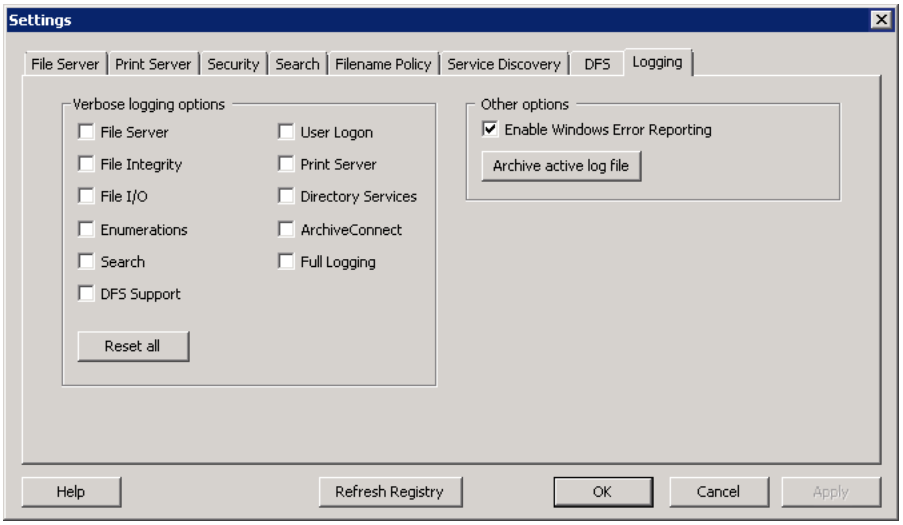
DFS namespaces can later be removed by selecting the namespace and clicking the **Remove** button.

Target Servers

The protocol used by Macintosh clients to connect to each target server can be configured on a per target server basis. When a namespace is first added, ExtremeZ-IP will attempt to detect, for each target server in the namespace, whether it supports the AFP protocol. If AFP is supported, the target server will be set to **AFP** by default. If AFP support cannot be confirmed, the target server will be set to **OFF**. Links to target servers set to OFF will not be visible to Macintosh clients in the DFS volume(s). If you would like Macintosh clients to connect to a target server using SMB, you can select the **SMB** option for each individual server. If you later install ExtremeZ-IP on a target server, you can return to the DFS settings tab and select **AFP** for that server.

Logging

ExtremeZ-IP allows the customization and configuration of it's logging functionality and it's ability to generate Windows Error Reports.



Verbose logging options

When enabled, these logging options increase the level of detail recorded in the ExtremeZ-IP log file. Options are available for various aspects of ExtremeZ-IP operations. These are typically only needed when working with Group Logic technical support. Enabling verbose logging could potentially have an impact on performance and should be used for troubleshooting. The **Reset all** button will return all ExtremeZ-IP logging to default settings.

Enable Windows Error Reporting

When enabled, Windows will give you the option of sending error reports in the event of an issue. These error reports can be used by Group Logic to identify and address potential problems.

Archive Active Log File

Click this button to ZIP archive the current ExtremeZ-IP log file and start a new log file. This can be used to reduce the size of your existing log file for archiving or to package your log file for delivery to Group Logic technical support. Log files are located in the \Program Files\Group Logic\ExtremeZ-IP\Logs\ExtremeZ-IP\ folder on your system drive by default.

Adding License Numbers

Using the Licensing button on the ExtremeZ-IP Administrator window, you can enter a serial number for any upgrade licenses without stopping the ExtremeZ-IP service. When you enter license numbers while the ExtremeZ-IP service is running; Macintosh clients stay connected and continue to use ExtremeZ-IP volumes.

You need to enter license numbers when:

- you have a trial version of ExtremeZ-IP installed and you purchase a license for the product.
- you are upgrading your client count.
- you are adding an additional ExtremeZ-IP companion product, such as ShadowConnect, to your server.

To add a serial number, do the following:

1. Open the **ExtremeZ-IP Administrator** application.
2. Click **Licensing** on the main **ExtremeZ-IP Administrator** window.
3. Click **Add License**, enter the serial number, and click **OK**.
4. The serial number will be displayed in the **Active Licenses** list and will take effect immediately.
5. Click **Close** to return to the **ExtremeZ-IP Administrator**.

The **Licensing** window can also be used to remove serial numbers or replace serial numbers to upgrade client count.

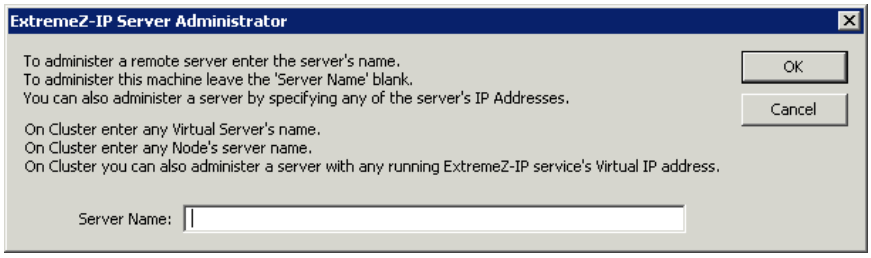
NOTE When adding companion product serial numbers to ExtremeZ-IP, you may be required to enter a serial number that matches the ExtremeZ-IP Server's client count and server type (retail, cluster, enterprise licences, etc).

Administering ExtremeZ-IP remotely

You can configure ExtremeZ-IP on a remote computer if ExtremeZ-IP is already installed on that computer. You must have Windows Administrative privileges on the remote computer. The experience of administering a remote server is very similar to that of the local server Administrator, except that the title of the Administrator dialog box shows the name or IP Address of the remote computer whose ExtremeZ-IP service you are configuring and you cannot browse for folders to share. Otherwise, you can configure the remote server just as you would a local server.

To administer a remote ExtremeZ-IP server, do the following:

1. Hold down the **Control** key while you launch the ExtremeZ-IP Administrator. Alternatively, if there is no local installation of ExtremeZ-IP, ExtremeZ-IP Administrator will start immediately in remote mode.



2. Type the name or IP Address of the remote computer and click **OK**.
3. The Administrator will attempt to use your Windows credentials to log onto the server. If necessary, you will be prompted for an alternate username and password.

Using the ExtremeZ-IP File Server

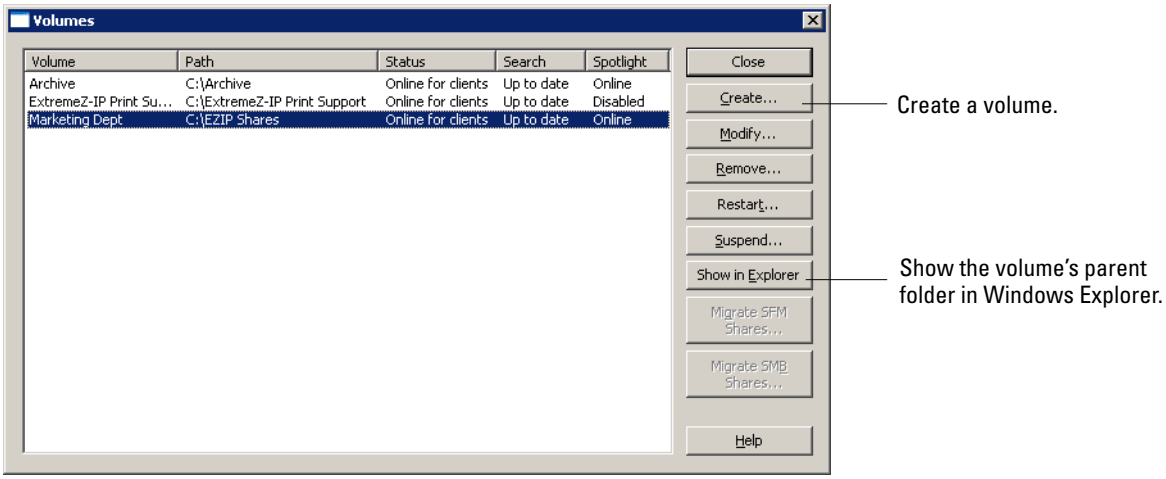
After using the **ExtremeZ-IP Settings** dialog box to set up your server name, security and other settings, you can create the volumes you want to share and the printers you want your Macintosh clients to use. After completing these tasks, Macintosh clients can connect to your server and use the volumes and printers you set up. You can check the **Users** and **File** dialog boxes to see who is connected and which files they are accessing, In addition, you can send messages, disconnect users, and delete items from the files being viewed.

Creating Volumes for Use with ExtremeZ-IP

You can share NTFS directories located on your Windows system for Macintosh users. When Macintosh users connect, they see these directories as remote AppleShare "volumes." Use the **Volumes** dialog box to create, modify, or delete individual volumes to share with Macintosh users.

Viewing the Volume Window

Click **Volume** on the **Administrator** dialog box to display the **Volumes** dialog.

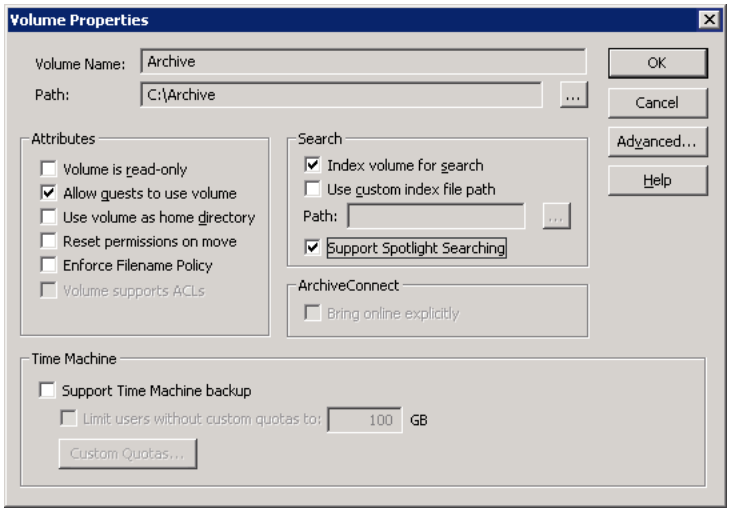


Creating a Volume

Folders can only be shared as ExtremeZ-IP volumes if they reside on an NTFS formatted disk. If you try to create a volume that is not on an NTFS formatted disk, ExtremeZ-IP gives an error message.

1. Create a new directory on an NTFS formatted volume on the server machine or find an existing directory that you want to use.
2. From the ExtremeZ-IP Administrator window, click **Volumes**.
3. On the **Volumes** dialog, click **Create**.
4. Using the **Browse for Folder**, locate and select the folder (directory) you want to share from an NTFS formatted disk.

5. Click **OK** and the **Volume Properties** window will appear.



6. Edit the **Volume Name** if you want to change the name.

NOTE A name can have no more than 27 characters. If you type more, ExtremeZ-IP truncates the name to 27 characters.

7. Choose any additional settings required.

8. Click **OK** to create the volume.

As soon as a volume's status becomes *Online for Clients*, Macintosh clients can see and connect to it.

Volume Properties

Attributes

Volume is read-only Setting the Volume to read-only prohibits Macintosh users from changing any documents on the volume or adding any new files or folders.

Allow guests to use volume If you want a Macintosh user who logs into ExtremeZ-IP as a guest to access the volume, check this checkbox.

Use Volume as home directory To filter the contents of this volume so that it only shows a user their own home directory, check this checkbox. In order for this feature to function, the server-wide **Enable Home Directory Support** option in the **File Server Settings** dialog box must also be enabled; see page 28.

Reset permissions on move If you would like files and folders to always inherit permissions from their parent folder after they have been moved, check this checkbox .

NOTE If the directory that is moved contains a large number of sub-folders, resetting the permissions can take awhile.

Enforce Filename Policy Enforcing Filename Policy will prevent Macintosh clients from saving files to the server that do not comply with the filename policies that the administrator has set in the global **Filename Policy** settings.

Volume supports ACLs Click this check box if you want the volume to support Access Control Lists.

Search Settings

Index volume for search Indexed searching is enabled on newly created volumes. To disable this feature, remove the check from this checkbox; in addition, you must stop and restart service the ExtremeZ-IP Files service for this change to take effect.

Use custom index file path To specify an alternate index file location for a volume, place a check this checkbox and select a path for the new index file location.

Support Spotlight Searching Enables Spotlight searching on the individual volume by Mac OS X 10.5 or later clients. This feature requires that Microsoft Windows Search is installed on the server and must be enabled on the **Search** tab of the **Settings** dialog before it can be enabled for the specific volume.

ArchiveConnect

Bring online explicitly ArchiveConnect is a separate Mac client-side application that enables Mac OS X clients to access file archives without triggering unintended retrieval of offline files. Normally, ArchiveConnect retrieves offline files automatically when a user double clicks to open them. This option requires the user to right click on an offline file and explicitly use a contextual menu option to bring the file online.

Time Machine

Support Time Machine backup When you check the Allow Time Machine Backup box, Macintosh clients can use the selected ExtremeZ-IP volume as a Time Machine backup destination. On the local network, Time Machine uses Bonjour to discover Time Machine supported volumes. Time Machine stores backup data as sparse disk image format or as HFS+. When you select a destination volume, Time Machine creates a disk image for the backup. By default, the Support Time Machine backup setting is disabled for a volume.

> **NOTE** You cannot enable Support Time Machine backup for volumes that are read-only or used as home directories. When you enable *Support Time Machine backup*, ExtremeZ-IP disables *Volume is read only* and *Use volume as home directory*. The opposite is also true.

Limit users without custom quotas to X GB Check this box and enter a value to limit the size of Time Machine backups per user. When the Macintosh client connects to the server for the first time it sees the available space on the drive as whatever the quota was set to. On subsequent logins it will see the available space as the quota size minus however much space has been used by that user's other backups. This quota applies to all users who do not have a custom quota assigned.

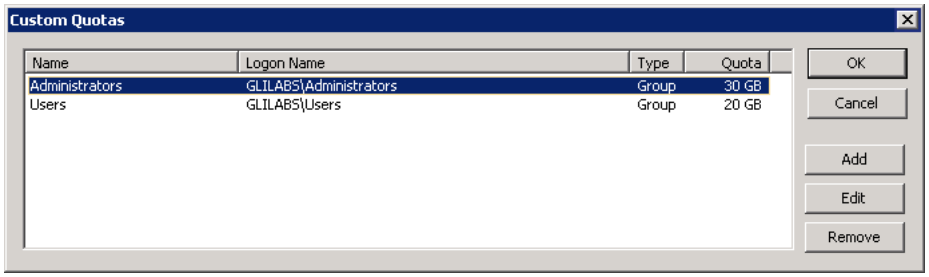
> **NOTE** Because ExtremeZ-IP has to tell the Macintosh how much space is available immediately when the user logs in, prior to Time Machine opening a specific backup file, the quota is applied on a per user basis not a per machine basis. If a user backs up both a desktop machine and a laptop, the quota will apply to the combined size of the backups.

Custom quotas This button opens the Custom Quotas window.

Using Custom Quotas

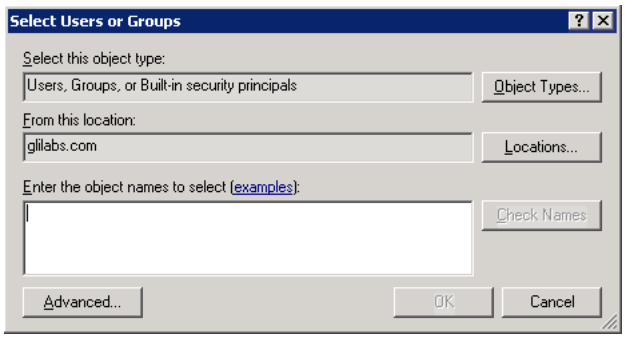
You can use **Custom Quotas** to define user-based or group-based Time Machine backup quotas. Quotas can be assigned to users and groups that exist locally on the server or within Active Directory. Custom quota settings always override the **Limit users without custom quotas** setting. Custom user quotas always override custom group quotas.

1. Click the **Custom Quotas** button on the **Volume Properties** dialog box to open the **Custom Quotas** window.

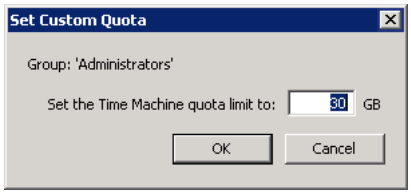


2. Click **Add** to add a new user-based or group-based quota.

3. Use the **Select Users or Groups** dialog to choose the users or groups you would like to apply a quota to. You can pick more than one user or group at a time if you would like to set them all to the same quota value.

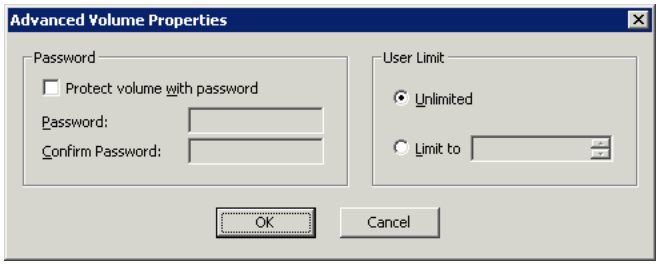


4. Enter the desired quota limit value in GB and click **OK**.



Using Advanced Volume Properties

You rarely need to use the **Advanced Volume Properties** dialog box. But, if you want to require that users enter an additional password, beyond their normal login password, when they mount volumes, you can use this dialog to establish that password. On this dialog, you can also limit the number of users that can use a specific volume.



NOTE Volume specific passwords were eliminated in Mac OS X 10.5, but have been re-enabled in Mac OS X 10.6.

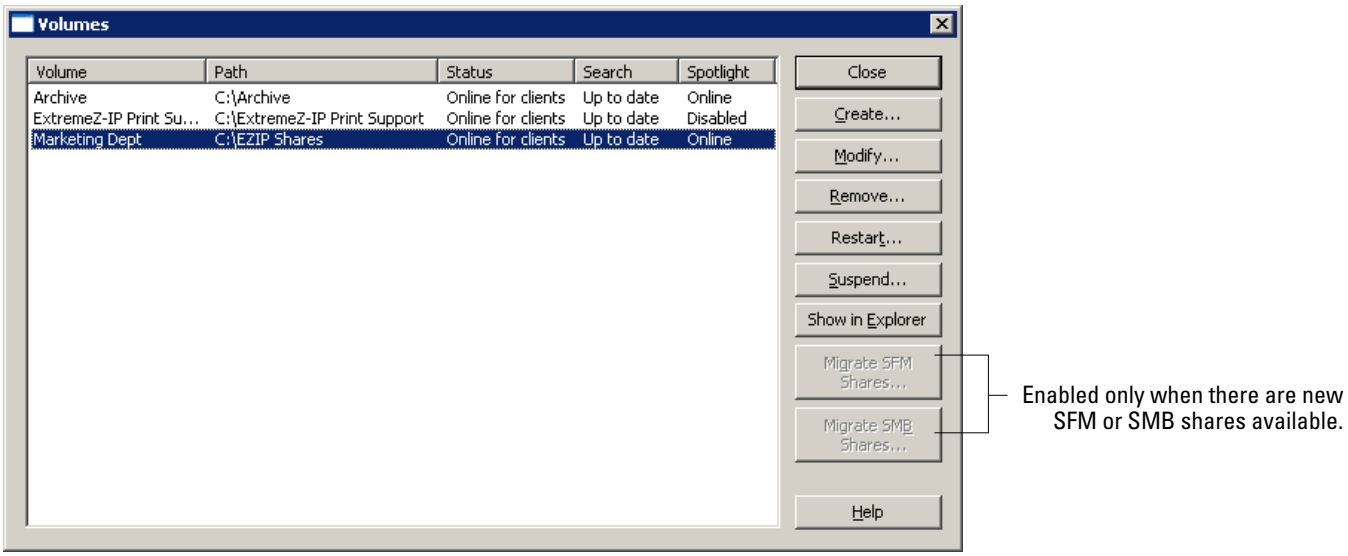
Changing Permissions for Shared Files and Folders

ExtremeZ-IP uses the existing Windows user logon and passwords, so file and folder security is identical to that provided by Windows Services for Macintosh (SFM). Unless you enable ACL support, Windows and Macintosh computers handle folder and file properties differently and not all Windows access information is displayed on the Macintosh.

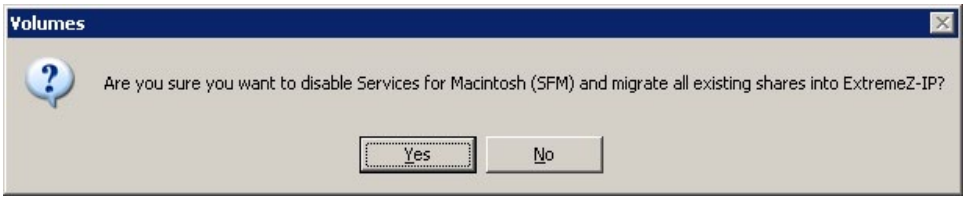
Because ExtremeZ-IP enforces Windows security settings, you should normally use Windows's built-in tools for adjusting directory and file permissions. The standard Windows tools provide the most flexibility for setting up your security policy.

Migrating or Replicating Volumes

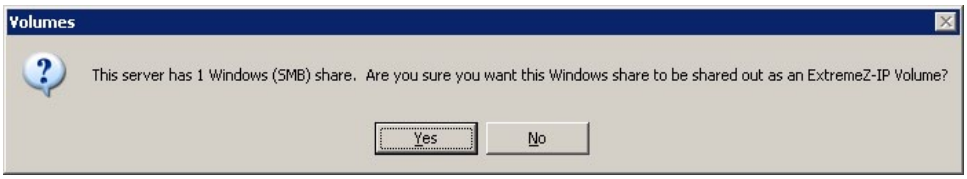
Each time you reopen the **Volumes** window, ExtremeZ-IP checks for any SFM or SMB volumes that are not currently shared as ExtremeZ-IP volumes. If such volumes are found, the appropriate **Migrate** button is enabled.



When you click **Migrate SFM Shares**, you are asked to verify that you want to migrate the shares and disable SFM.



When you click **Migrate SMB Shares**, you are asked to verify that you want to migrate the shares.



If you follow this procedure, preexisting SFM and SMB shares will become available as ExtremeZ-IP volumes. This procedure is the same as that used the first time you launch ExtremeZ-IP (see page 13).

Because someone could add or remove volumes to either the SFM or SMB service at any time, when you reopen the **Volumes** window, note the state of the **Migrate** buttons. If they are dimmed (disabled), no new SFM/SMB volumes have been added. If one of the corresponding ExtremeZ-IP volumes is removed, the button is enabled.

NOTE This button updates only when the **Volumes** window is opened. Changes occurring to SMB/SFM shares have no effect on the button state while the **Volumes** window remains opened.

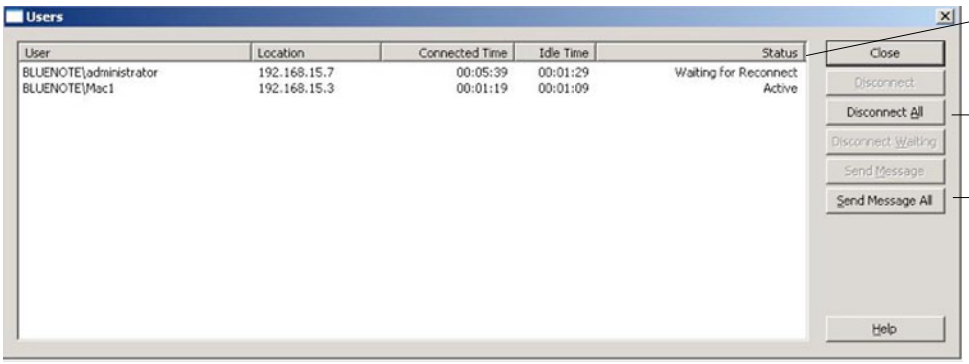
ExtremeZ-IP Users

The **Users** dialog box lets you view the users connected to the server, disconnect those users, or send messages to them. See the section on the next page "Connecting Macintosh Users" for information on user name and password entry.

To view the **Users** dialog box, click **Users** on the **ExtremeZ-IP Administrator** window.

Names and IP addresses identify users who are currently connected. Their connection and idle times are given. The dialog refreshes automatically.

Click on a column title to sort the list by a column.



The status tells you if the Macintosh client is idle, sleeping, or being reconnected; see "Reconnecting a Dropped User Session" on page 43.

NOTE User accounts are defined in Windows. ExtremeZ-IP uses this information to determine the user access privileges.

Connecting Macintosh Users

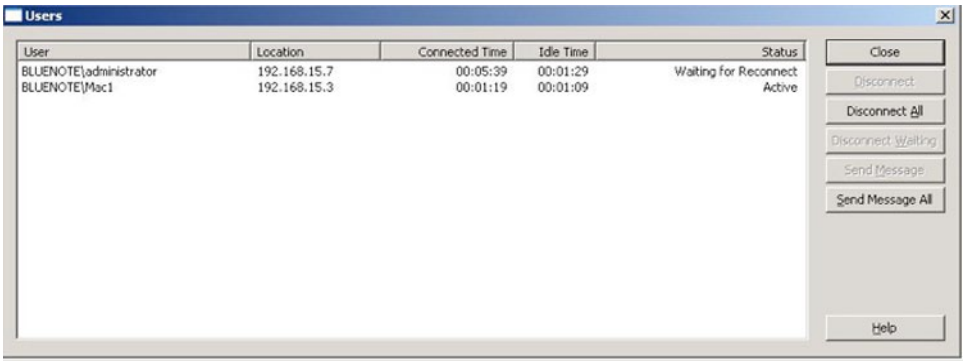
ExtremeZ-IP supports Active Directory. When Macintosh users connect to the ExtremeZ-IP server, they enter their user names and passwords. ExtremeZ-IP authenticates this account against the primary domain of the Windows machine that it is running on. If this machine is not a member of a domain, the account must be a member of the local accounts that appear in Windows **User Manager**. If the machine is a member of a domain, then the user name you give the Macintosh user must be either a member of the primary domain, the local accounts, or a trusted domain. You may specify to be authenticated against a specific domain by prefixing the user name with the domain name and a backslash (\). For example, to authenticate the user name Joe from the Marketing domain, in the user name portion of your AFP client logon enter MARKETING\joe.

ExtremeZ-IP clients on Mac OS 9 see a server name in their **Chooser** only if the AppleTalk protocol is installed on the Windows server and the client's connection to the server supports AppleTalk.

NOTE Macintosh OS 9 users can connect to a server, even if they cannot see the server name in the **Chooser,** by clicking **AppleShare** and then **Server IP Address i**n the **Chooser** and entering the server IP address or DNS name.

Reconnecting a Dropped User Session

ExtremeZ-IP supports reconnecting user sessions in the event of a temporary network outage. In addition, it supports automatic closing of locked files after a Macintosh client crash or reboot.



Reconnecting If a Session is Dropped

When Mac OS X clients connect to ExtremeZ-IP, they receive an encrypted reconnect credential. In the event that the connection to the server is broken, ExtremeZ-IP keeps the session alive by putting it into *Waiting For Reconnect* mode. While in this mode, all files and volumes opened by the session remain open. When the client machine reestablishes contact with the server, the client (silently) supplies the server with the reconnect credential. ExtremeZ-IP decrypts the credential and uses it to authenticate the user. If the authentication is successful, the client is logged into the server. The computer follows up this login with a request to disconnect its old session. ExtremeZ-IP finds the old session, transfers its open files and volumes to the new session, and deletes the old session. The new session has access to the old session's assets.

If the old session is no longer available because it timed out or was manually disconnected or because the ExtremeZ-IP service restarted or failed over, ExtremeZ-IP returns an error to the client when the client tries to disconnect the old session. In this case, the client machine tries to reopen any files and volumes that were open in the old session. Any data written to those files are lost if those data have not yet been flushed to disk. However, the new session has access to those files automatically.

In the event that the Macintosh client crashes and reboots while connected to the ExtremeZ-IP server, the old session is placed in *Waiting For Reconnect* mode as described above. The next time the Macintosh client logs into the server, ExtremeZ-IP detects that a client reboot has taken place and automatically disconnects the old session and closes any files that the session had opened. Since the client has rebooted, ExtremeZ-IP does not transfer files to the new session; the reboot has wiped away knowledge of the old session from the client. This feature helps alleviate the problem of a client-side crash leaving files open on the server.

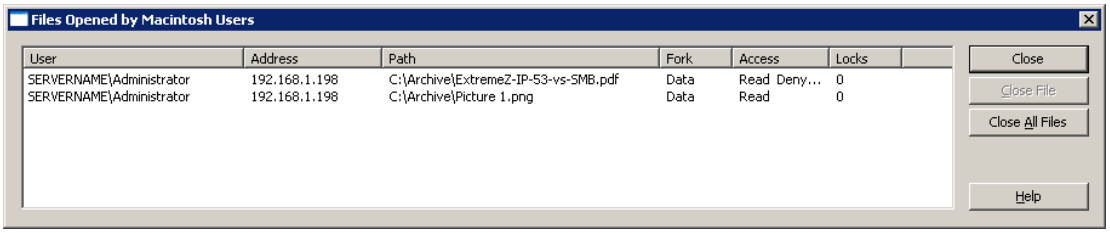
Sessions remain in a *Waiting For Reconnect* state for five minutes; then they are automatically disconnected and their open files closed. This reconnect timeout is configurable through a registry setting. You can use the registry keys to affect the way ExtremeZ-IP reconnects a session; see *Appendix A: Using the Registry Keys* on page 74.

Reconnecting with Kerberos Authentication Kerberos is a protocol that provides secure network authentication and support for single sign-on to network resources: see *Using Kerberos* on page 15. Because of limitations in the Windows OS, users that originally logged in using Kerberos authentication cannot reconnect automatically if their old session is no longer available. Therefore, while users logging in with cleartext or DHX-encrypted passwords silently reconnect after a cluster failover, clients logging in with Kerberos may be disconnected.

Viewing Files Opened with ExtremeZ-IP

The **Files Opened by Macintosh Users** dialog box displays files currently in use. Macintosh users may open the data or resource fork of a file.

To view the **Files Opened by Macintosh Users** dialog box, click the **Files** button on the **ExtremeZ-IP Administrator** dialog box.



The dialog refreshes itself as new files are used by the Macintosh Users.

The dialog box lists the following information about each file being used:

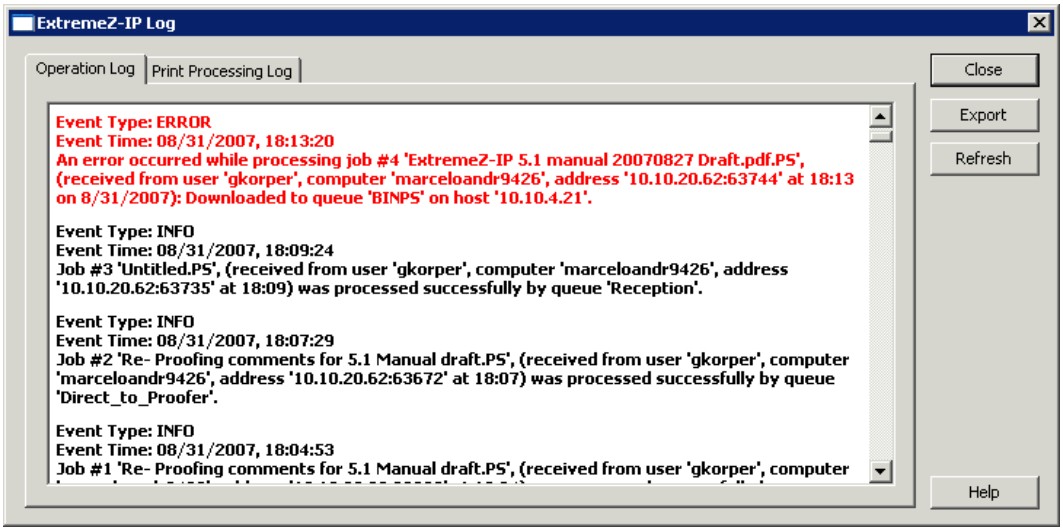
- the name of the Macintosh user using the file.
- the IP Address from which the user is connected.
- the name of the file being used.
- the fork being accessed by the user—either the Resource or Data fork.
- access information (for example, read access or write access).
- a count for the number of locked sections on a file if a user has locked portions of that file for exclusive access, which happens often for database programs.

NOTE You should use caution when closing a file this way because a user may experience data loss and possibly a crash. Instead, disconnect a user using the Users dialog box; this automatically closes all files opened by that user.

Keeping Track of Activities with the Log

The **ExtremeZ-IP Administrator** provides a log of the ExtremeZ-IP server's activities. The log contains details regarding the connections that have been made along with other operational information. You can export the log to a tab-delimited text file for use in other programs. Once the log is exported to a text file, you can import it into a spreadsheet or system designed to make use of the information.

To view the log, click the **Log** button on the **ExtremeZ-IP Administrator** dialog box.



You can view the type of entry, the time the entry was made, and the message about the entry.

Exporting the Log

You can export the Log to save it in a text format.

Exporting the Log within ExtremeZ-IP

To export the log within ExtremeZ-IP, do the following:

1. From the ExtremeZ-IP **Log** window, click **Export** to save the log as text.
2. Type a name and format.
3. Click **Save** to return to the log.

Exporting the Log from the Command Line

To export the log from the command line, do the following:

1. Navigate in a DOS prompt to the folder where ExtremeZ-IP is installed.
2. Type EZIPUTIL PRINT /EXPORT_LOG /PATH:fullpathoflog where fullpathoflog specifies the location and name of the log file that should be exported, such as C:\Logs\file.txt.

See the included sample batch file Export_Print_Log.bat that came with ExtremeZ-IP.

Remapping Extensions

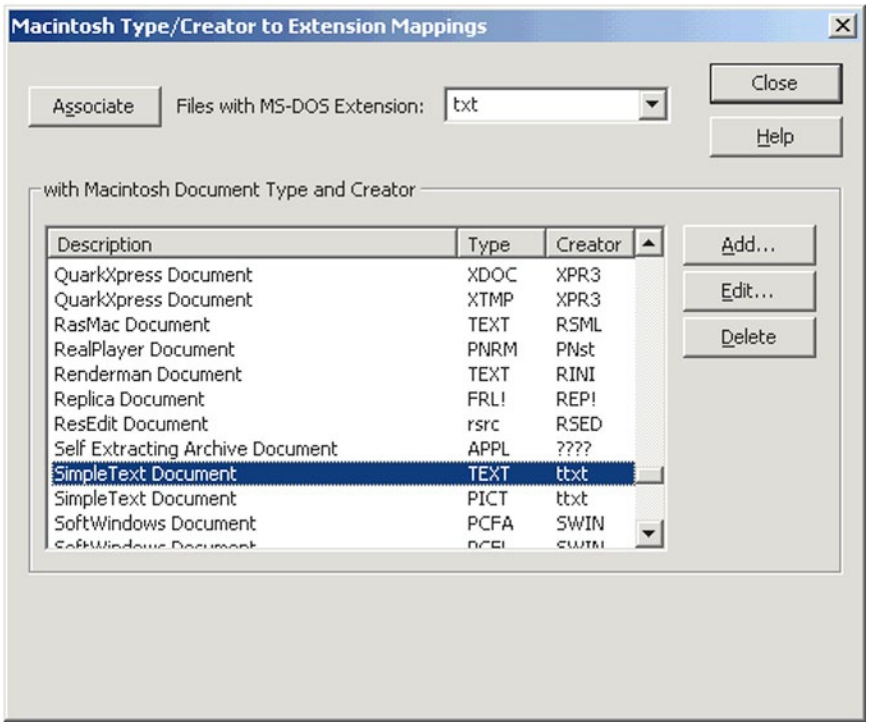
Macintosh programs use a document's type and creator to launch particular applications from the Finder® automatically. Windows users normally do not have access to the Macintosh-specific type and creator information. With ExtremeZ-IP, you can automatically map MS-DOS extensions to particular type/creator combinations. For example, you can map Adobe® Acrobat documents that have a PDF extension, to the Macintosh type "PDF" and creator "CARO." ExtremeZ-IP installs a number of default mappings for certain document types; you can change these at any time. You can create a new type and creator to assign to a document. You can also edit and delete types and creators.

Associating a Type and Creator

You can associate MS-DOS file extensions with Macintosh types and creators, create new types and creators, and edit or delete types and creators. For example, you may want to associate PDF files with Illustrator rather than Acrobat.

To associate files with a type and creator or to create new types and creators, do the following.

1. From the **ExtremeZ-IP Administrator**, click **Settings**.
2. Click **Types and Creators...**

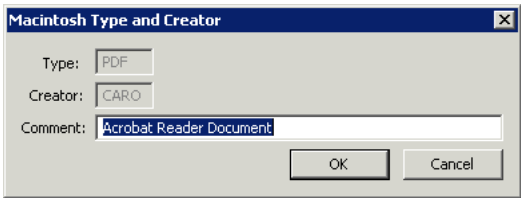


3. From the **Files with MS-DOS Extension** drop list at the top of the **Macintosh Type/Creator to Extension Mappings** dialog box, select a new extension.
4. From the list of types and creators, select the entry you want to remap.
5. Click **Associate.**

The extension is associated with the selected type and creator.

Creating a New Type and Creator

1. Click **Add** on the **Macintosh Type/Creator to Extension Mappings** dialog box.



2. Fill out the dialog box to meet your specifications.
3. Click **OK** to return to the **Macintosh Type/Creator to Extension Mappings** dialog box.

The new type and creator is now listed in the database.

EXTREMEZ-IP PRINT SERVER

The ExtremeZ-IP Print Server supports IP-based printing from Macintosh computers. Macintosh clients can print without using AppleTalk. Mac OS X clients set up printers using Zidget, Bonjour, or the Print Center. Mac OS 9 clients set up printers using the Chooser or Choose IP Printer, an Apple menu item. In addition to these printing capabilities, your Mac OS X clients can access shared volumes as described in the ExtremeZ-IP File Server chapter. Print Accounting, installed with the ExtremeZ-IP Print Server, provides additional print support; you can capture, validate and track cost-accounting information with each print job as the user prints it.

How the Print Server Works

After receiving a print job from a Macintosh, ExtremeZ-IP uses one of several processing methods to process it. These methods include Windows print queues, AppleTalk printers, LPR printers, and "hot folders"—special output directories where additional software, such as a RIP or OPI server, can process the job. In addition, you can view the print jobs in progress, speed or delay processing of jobs, and delete jobs from the list. Macintosh clients can use IP or Appletalk to print to the ExtremeZ-IP Print Server.

The ExtremeZ-IP Print Server logs many aspects of the print jobs that your users send to the server—job name, name of the user that sent the job, time and date of printing, page size, number of pages, size of job in bytes, address of the computer that printed the job, and the name of the print queue used. You can export this log automatically to a text file that can be imported into an accounting or other cost-tracking system.

Print Accounting captures and tracks additional information of your choosing and requires that the Macintosh client enter one or more billing codes that you set up before printing to a queue. The accounting information is added to the log of the print job and can be imported into standard accounting and cost-tracking systems. See page 54 for additional information on using Print Accounting. See page 52 for information on viewing or retrieving the log.

Setting up Print Queues

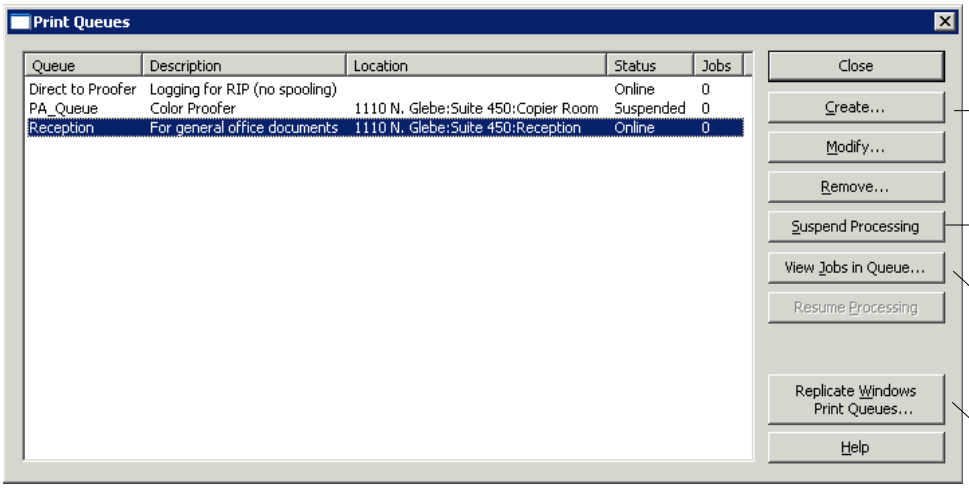
A print queue is a virtual printer that Macintosh users can access. When Macintosh users print files to one of your printers, the resulting print job is delivered to your server and can be tracked and processed there. Read the section on creating print queues, then read the specific section on the following pages to configure specific settings for the four types of print queues: Windows, LPR, Directory (Hot Folder), and AppleTalk.

Creating A Print Queue

To create a print queue, do the following:

1. On the **ExtremeZ-IP Administrator** dialog box, click **Print Queues**.

NOTE Click on a column title to sort the list of print queues.



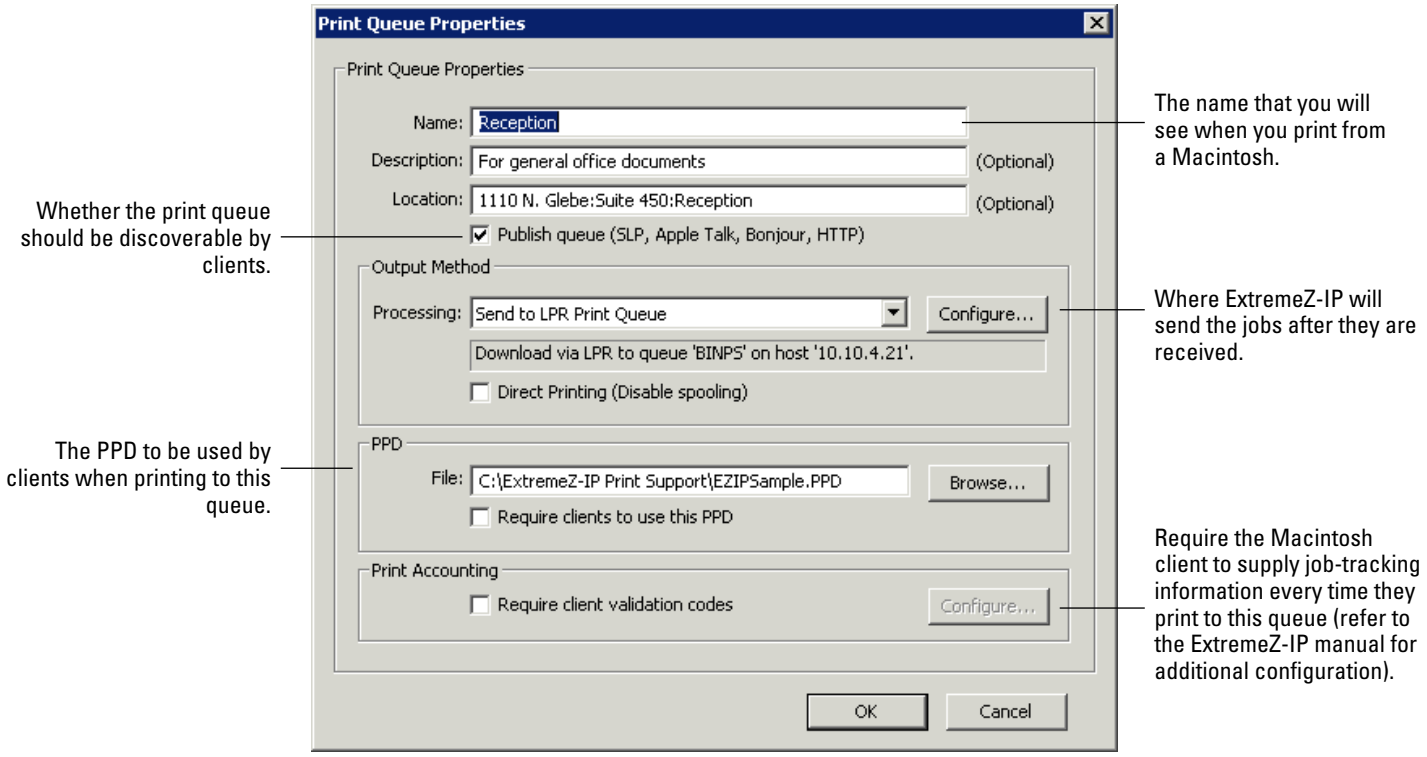
Create print queues.

When a queue is suspended, jobs are accepted by the server. However, they are not sent to the printer until processing is resumed.

Open a window with a list of the pending jobs. From there you can start, stop, or reorder the print jobs.

Takes the existing Windows print queues and republishes them as ExtremeZ-IP queues as well.

2. Click **Create** to define a print queue.



NOTE If you plan to use Print Accounting, enable the checkbox allowing to you to Require Client Validation Codes. See page 54 for information about setting up print accounting for a print queue.

3. Type a name for the print queue you are setting up.

4. Associate a PPD file with the queue and choose a processing method. See the sections below for instructions for each kind.

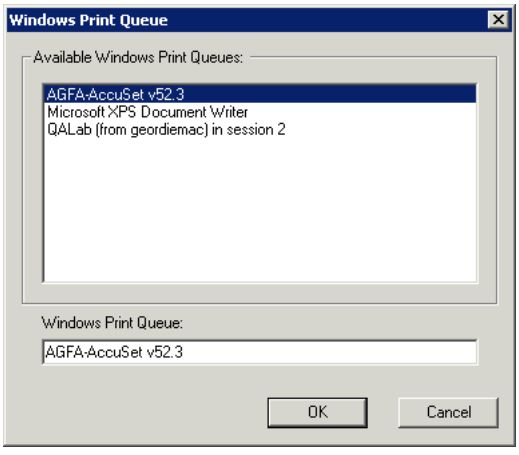
Setting Up Processing Methods

When ExtremeZ-IP receives a job from a client, it can output the job to a Windows print queue, an LPR printer, a directory, or an AppleTalk printer. The following section describes how to configure each of these methods.

Sending to a Windows Print Queue

To select a Windows print queue for your processing method, do the following:

1. Select **Send to Windows Print Queue** on the **Processing** pull down menu of the **Print Queue Properties** dialog box.



You see a list of Windows printers that you have already shared for Windows clients on the server.

2. Select a printer.

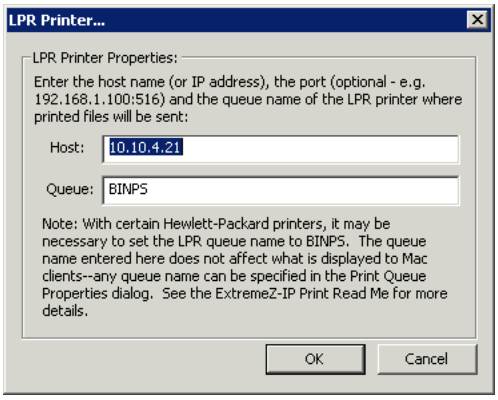
If this list is empty, you must create a Windows printer from the Windows Print Wizard and set it to be shared.

Sending to an LPR printer queue

To select an LPR printer for your processing method, do the following

1. In the **Processing** pull down menu of the **Print Queue Properties** dialog box, select **Send to LPR Print Queue.**

2. Type a name for the print queue you are setting up.



Queue names must be unique; you cannot have two queues with the same name. See the section *Controlling printing with an LPR printer* for information about controlling the LPR print queue.

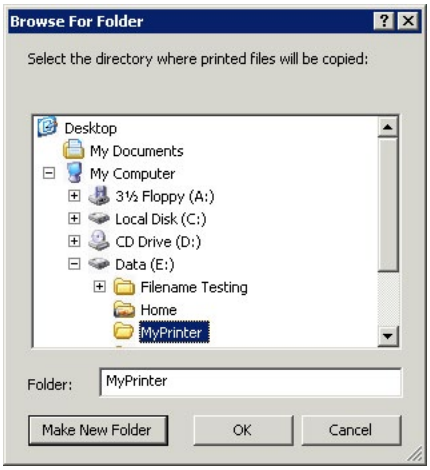
Sending to a Specified Directory (Hot Folder)

You can create a print queue that sends files to a specified directory or hot folder. You can choose a local folder or one from the network. For network locations you use a UNC path.

> **NOTE** If you select a network location, the Computer account for the server in Active Directory must be given access to the network location on the remote server. Giving a computer account access to a folder is performed the same way as giving a User account access to a folder.

To use a specified directory as your processing method, perform the following:

1. Select **Send to Specified Directory** in the **Processing** pull down menu of the **Print Queue Properties** dialog box.



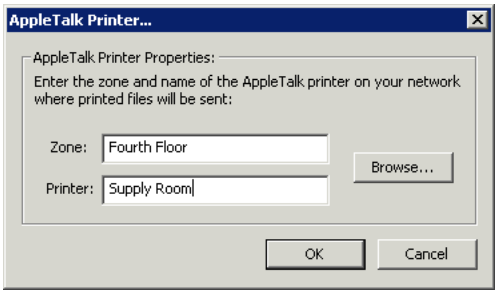
2. Use the **Browse for Folder** dialog to locate and select the directory.

3. Click **OK**.

Sending to an AppleTalk Printer

To use an AppleTalk Printer as your processing method, do the following:

1. In the **Processing** pull down menu of the **Print Queue Properties** dialog box, select **Send to AppleTalk Printer**.



2. Type the **Zone** in which the printer is located or an asterisk (*) if you do not have zones on your AppleTalk network.
3. Enter the name of the **Printer**.

You can click **Browse** to search for the printer on your network.

Associating a PPD File with a Print Queue

You may associate a PostScript Printer Description (PPD) with each queue. PPDs are used on the Macintosh when creating printers. If you provide a PPD file for the print queue, Macintosh clients can download and configure the printer for use on their desktops without having a PPD already installed on their machines. The ExtremeZ-IP server includes an option that automatically downloads the specified PPD to Macintosh users when they create printers. You should obtain and use PPD files that were created on a Macintosh, since they include additional information such as special icons to deliver the user experience that Macintosh users expect. Specifying a PPD when you set up a queue makes it available for download, but its presence on the server does not affect printing.

To associate a PPD file with a print queue, enter the path to the PPD file in the PPD section of the **Print Queue Properties** dialog box or use the **Browse** button to locate the correct PPD.

NOTE These files must be on a disk accessible by the server.

Controlling the Processing of Jobs

You can control the processing of jobs that Macintosh users send to the ExtremeZ-IP server. On the **Print Queues** dialog, you can do the following:

- view the status of each job in the queue in the **Status** column.
- suspend processing of all jobs in a print queue and a particular job in a print queue.
- resume processing when you want.
- control which jobs are processed first.
- delete jobs.

To access the Print Queues dialog, click **Print Queues** on the **ExtremeZ-IP Administrator** window.

This dialog lists the print queues available to Macintosh clients.

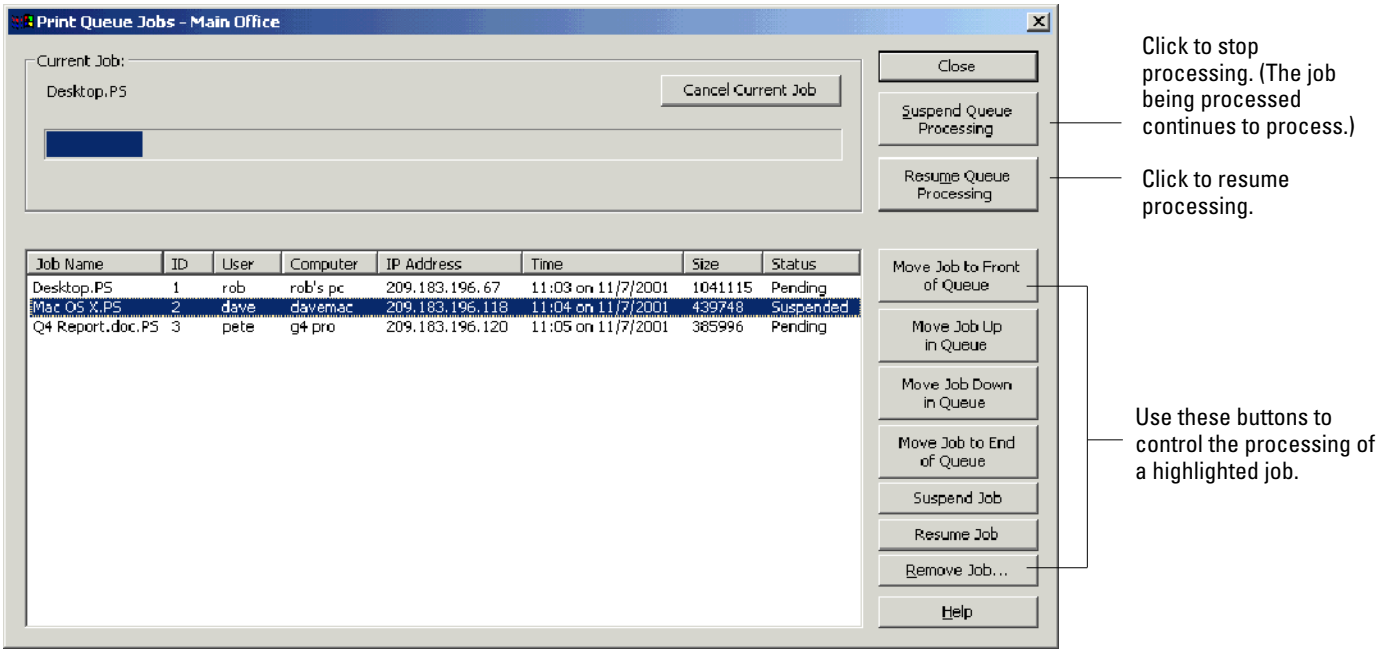
Viewing and Managing Print Jobs

You can view and manage jobs being processed in the **Print Queue Jobs** dialog box for one or more print queues at the same time.

To view a list of the jobs being processed in a print queue, do the following:

1. Highlight a print queue in the **Print Queue** dialog box.
2. Click **View Jobs in Queue**.

The **Print Queue Jobs** dialog box lists the jobs being processed. When a job is being processed, you see the progress indicator and the name of the job being processed.



Publishing A Print Queue

ExtremeZ-IP Print Server advertises all print queues automatically over Bonjour, Zidget/HTTP, AFP, and SLP. Mac OS X and Windows clients can set up and print to Bonjour printers in a single step. Similarly, Mac OS 9 clients can use AppleTalk. If your clients are using Mac OS X 10.4.3 or later, they can take advantage of the new ExtremeZ-IP Zidget. Once you select a printer using any of these methods, it is available as an installed printer in the print dialog. You do not have to set up your printer each time you want to print to it. See the *Client* section starting on page 57 for information for clients.

You can disable the automatic advertisement of printers over Bonjour, Zidget/HTTP, AFP, and SLP globally for the entire server or on a queue-by-queue basis.

To disable any advertisement protocol, do the following:

1. From the **ExtremeZ-IP Administrator**, click **Settings**.
2. On the **Settings** dialog box, click the **Service Discovery** tab
3. Disable the services you do not want to use; see page 35.

You can also disable publishing a specific queue so that only people who know the queue exists can use it.

Using the Print Log

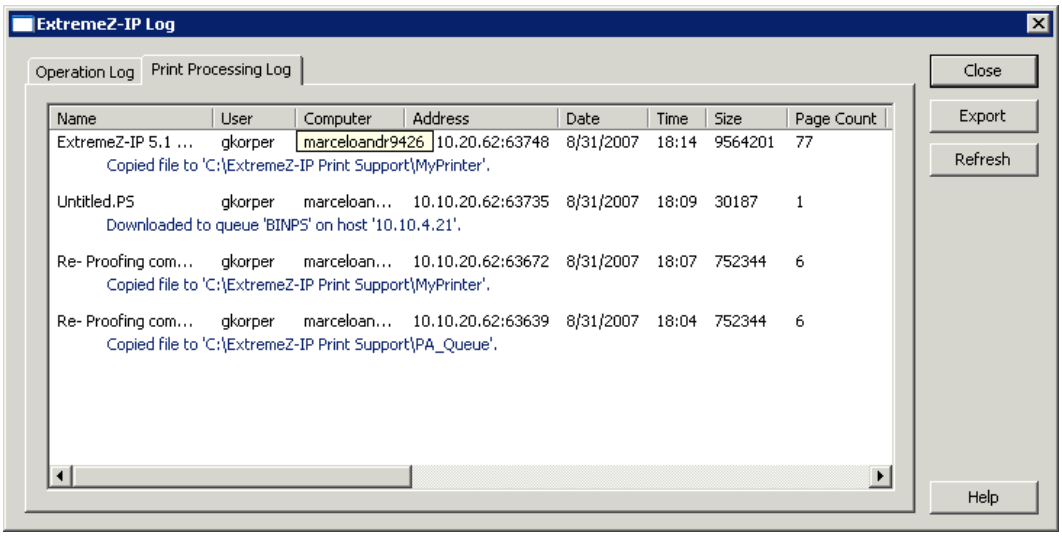
You can view a log of ExtremeZ-IP activities. The log tells you what jobs have been printed and other information.

To view the log, do the following:

1. Click **Log** on the **ExtremeZ-IP Administrator**s dialog box.
2. Click the **Print Processing Log** tab to display it.

The **Print Processing Log** contains standard printing information. You can sort the log by any column by clicking on the column title.

To toggle the sort between ascending and descending, click the column title a second time.



Using the registry keys, you can add each new print log entry to a specified text file automatically. See *Appendix A: Using the Registry Keys*" on page 74.

Customizing ExtremeZ-IP Print Processing Log Columns

You can override the default configuration and customize your view of the **Print Processing Log** by using registry keys to display columns in any order. When you print the log, only those columns displayed in the log are printed. Change the registry keys to display and print different columns. See *Appendix A: Using the Registry Keys* on page 74 for instructions.

NOTE Data for all columns are always stored; when you display different columns, the saved data are filtered.

If you use Print Accounting you can require Macintosh users to fill out code fields before printing. These are displayed in the **Print Processing Log**. See the following section for information about Print Accounting.

Exporting the Print Log from ExtremeZ-IP

You can export either log in a tab-delimited text file for use in other programs. Once the log is exported to a text file, you can import it to a spreadsheet or system designed to make use of the information.

To export the log using the **Export** button, do the following:

1. Access the **ExtremeZ-IP Log** dialog in the **ExtremeZ-IP Administrator**.
2. To export a log, display its tab—**Print Processing** or **Operation**—and click **Export**.
3. Click **Save** to save the log. If you export the printing jobs, the file is named ExtremeZ-IP Print Jobs.txt.
4. Click **Close** to return to the **ExtremeZ-IP Administrator**.

Exporting the Print log with the Command Line

To export either log using the command line, do the following:

1. Navigate in a command prompt to the folder where ExtremeZ-IP is installed.
2. Type EZIPUTIL PRINT /EXPORT_LOG /PATH:fullpathoflog where "fullpathoflog" specifies the location and name of the log file that should be exported, such as C:\Logs\PrintAccounting.txt.

See the included sample batch file Export_Print_Log.bat that came with ExtremeZ-IP.

Using Print Accounting

Print Accounting allows you to validate, capture, and track cost-accounting information with each print job as the user prints it. Information obtained through Print Accounting is logged with other information in the **Print Processing Log**. You can use the print accounting information for these and other tasks:

- allocating proofing costs between clients and jobs.
- tracking use of shared printing resources and assigning costs correctly to departments and jobs.
- tracking the use of printers between employees, students, or projects.
- ensuring that only authorized users can print to certain printers.

You can configure print queues to require that Macintosh users enter accounting codes before printers will accept jobs from them. You decide how many accounting codes are required for each print queue, the names of the codes, and whether the codes are optional or required. When codes are required, Macintosh users cannot print a job until codes are entered. You may allow clients to browse a list of valid accounting codes or pick from the most recently used codes on their computer.

Each print accounting code is associated with a text file that contains valid codes and descriptions—for example, an employee number/name (2312, Jane Smith), or project number/name (Q98331A, Mockup for Acme Corp Annual Report). When clients print to a queue, they are prompted to enter the print accounting codes based on the configuration on the server. Validation is performed against this text file when the client prints, so you can update these codes and descriptions on the server without having to reconfigure the client.

Setting up Print Accounting

Print Accounting supports Macintosh clients using OS X 10.2.8 or later. You must modify a PPD for use with Mac OS X before using print accounting. See page 56 for directions for modifying a PPD. Print Accounting is supported through TCP/IP or AppleTalk on Mac OS X. It is not available when printing from applications running in Classic mode under Mac OS X.

ExtremeZ-IP also supports an option called Direct Printing with which you can route Print Accounting through the ExtremeZ-IP server, while Macintoshes send jobs directly to a printer that supports the LPR/CUPS™ (Common UNIX Printing System) printing architecture.

Creating a List of Codes for Customers

To use Print Accounting, you must first create text files containing the codes and descriptions for each code. If the codes already exist in another system, such as an accounting system, you can export them as tab delimited files and make any adjustments necessary to conform to the ExtremeZ-IP format.

For each print queue for which you want to use print accounting, create a separate file for each code field that includes the code and its description, separated by a tab, in a word processor or text editor. If you use a word processing program, you must save the file as a text file. For example, enter the information in the following way for employee identification:

123 <tab> Sue <return>

124<tab> Jim

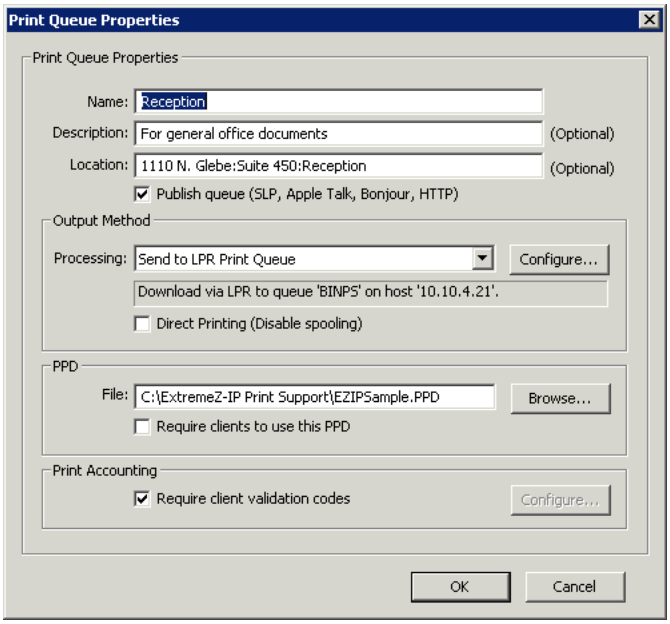
NOTE If you change the code text files, ExtremeZ-IP does not reload them automatically. To reload the codes after making changes, restart the ExtremeZ-IP service or use the command line argument EZIPUTIL.EXE PRINT /REFRESH_CODES

Setting up a Print Queue to Provide Print Accounting Information

Once you define your codes and code descriptions, assign them to print queues as you set up print queues or modify them. You set up validation codes for each print queue; every Macintosh client using that print queue will have the same fields.

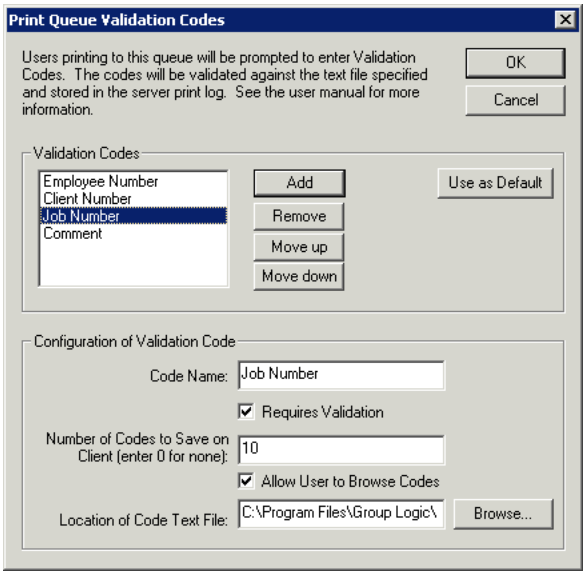
To set up a print queue to provide Print Accounting information, do the following:

1. In the **ExtremeZ-IP Administrator,** click **Print Queues**.
2. Select an existing print queue and click **Modify** or click **Create** to create a new print queue.
3. Check the **Require client validation codes** checkbox.



4. To add the first code, click **Configure**. You can change the name of the code to anything you would like.

   This name appears next to the field on the Macintosh print dialog box.



5. If you want to require the Macintosh user to fill in the code before printing instead of it being optional, check the checkbox **Requires Validation**. Use fields that do not require validation for information such as comments.
6. If you want the Macintosh user to be able to browse the code list, place a check in the **Allow User to Browse Codes** checkbox.
7. Click **Browse** to locate the text file that contains the codes you set up earlier.
8. Click **OK** to save the entered code or click **Add** to add additional code fields.
9. Provide the PPD for each Macintosh by placing it on the ExtremeZ-IP server and configuring the print queue to require it.

Modifying a PPD for use with Print Accounting

On Mac OS X, the PPD selected for each print queue must be modified to include additional information, including the IP address of the server. Macintosh PPDs are normally in the folder /Library/Printers/PPDs/Contents/Resources. A sample PPD called ExtremeZ-IPSample.PPD is included with the software. To modify a PPD for use with Print Accounting, follow these steps:

1. Find the PPD you want to modify.
2. Default PPDs are compressed in the gzip format. Expand one by double-clicking it.
3. Open the uncompressed PPD in a text editor.
4. Copy the following lines to the PPD from the ExtremeZ-IP sample PPD.

```
*%**************************************************************************
*%          ExtremeZ-IP Print Accounting CUPS Filter
*%**************************************************************************
*cupsFilter: “application/vnd.cups-postscript 0 ExtremeZ-IP_filter”
*ExtremeZ-IP_Print_Accounting_IP:                “192.168.1.5”
*ExtremeZ-IP_Print_Accounting_Queue_Name:        “My Queue Name”

*%**************************************************************************
*%          ExtremeZ-IP Print registering UI element for plugin invocation
*%**************************************************************************
*OpenUI *ExtremeZ-IPValidationRequired/ValidationRequired: Boolean
*DefaultExtremeZ-IPValidationRequired: False
*ExtremeZ-IPValidationRequired True/Required: “”
*ExtremeZ-IPValidationRequired False/Not Required: “”
*?ExtremeZ-IP_Validation_Required: “query code”
*CloseUI: *ExtremeZ-IPValidationRequired
```

NOTE If the PPD you are modifying already has a CUPS filter it may conflict with the ExtremeZ-IP filter.

5. Modify the line ExtremeZ-IP_Print_Accounting_IP to be the TCP/IP address of the ExtremeZ-IP server.
6. Modify the line ExtremeZ-IP_Print_Accounting_Queue_Name to be the name of the queue as it is specified in the ExtremeZ-IP Administrator.
7. Modify the NickName of the PPD. There should be a line that starts *NickName:
8. This name will appear when selected during creation of a desktop printer. If you don’t modify the NickName and, instead, leave the original compressed PPD installed, you will not be able to select the modified one.
9. Save the PPD from the text editor with a .ppd extension. The standard TextEdit application asks you if you want to append a .txt extension. Click **Don’t Append a .txt** and do not re-compress the PPD.

Configuring Client Computers to Print to ExtremeZ-IP

To make use of ExtremeZ-IP printing, clients follow specific steps depending on their operating system. Once you add print queues through the **ExtremeZ-IP Administrator Print Queues** dialog box, they are immediately available for clients to print to them. Printer Browser installers for Macintosh clients are copied onto your server's drive when you install ExtremeZ-IP. Macintosh clients can copy to their computer, and install, an operating system specific Printer Browser installer from the ExtremeZ-IP server. It is also possible to use Apple Remote Desktop to deploy the installer packages to multiple Macintosh computers. A Macintosh user can select an ExtremeZ-IP queue to print to in a number of ways, depending on the operating system they are using and the functionality they need.

When using Mac OS X, the following are the primary ways to set up a printer:

- **ExtremeZ-IP Zidget** supports discovering printers across subnets, automatic PPD download, and adding queues that have been set up to require Print Accounting codes if the Macintosh also has the optional ExtremeZ-IP print components on it. It is also available from inside any application, therefore; you can set up a printer when you need to print without leaving your current application. The slight downside is that you must install it on each Macintosh. Although simple to install, it does require additional work.
- **Bonjour** discovery from within the print window of an application has the advantage of being built-in to Mac OS X. The native Mac OS X Bonjour discovery is also very simple to use. The disadvantage of Bonjour is that it does not support automatic PPD download or Print Accounting queues.
- **ExtremeZ-IP Printer Browser** works from within the Apple Printer Setup Utility. It supports automatic PPD download from the server and can be used to add queues that have been set up to require Print Accounting codes. The disadvantage to the custom ExtremeZ-IP print components is that they have to be installed by someone with administrator rights on the client computer either manually or with Apple Remote Desktop. It also requires more training than the Zidget does.

When using Mac OS 9, there are two options for setting up a printer:

- The built in **Chooser** desk accessory can use AppleTalk to locate and set up the printer. Note: AppleTalk is not installed by default on Windows servers.
- **ExtremeZ-IP Choose IP Printer** is an optional install that supports faster printing. It uses the SLP and TCP/IP protocols.

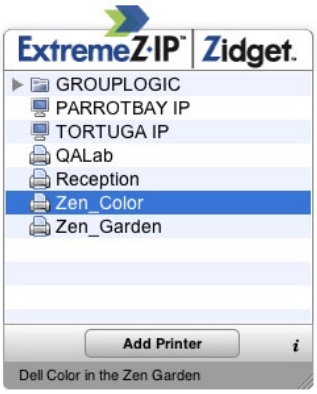
The advantages and disadvantages are similar to the ones stated above for Mac OS X. The built-in Chooser is simple and well understood by Macintosh users, but the custom client has more features and is several times faster than printing with AppleTalk.

ExtremeZ-IP Zidget

Zidget is the easiest and fastest way to add an ExtremeZ-IP printer from the Macintosh. More information about using Zidget can be found in the Zidget section.

To add a printer using Zidget, do the following:

1. Press the **F12** key to invoke **Dashboard**.
2. Select the **ExtremeZ-IP Zidget**.



3. Double-click a location/zone if necessary.
4. Select a printer from that location/zone.
5. Click **Add Printer** and the printer will be created on the Macintosh with the proper PPD if one is available from the server.
6. The status section of the Zidget updates to say the printer was successfully created.

Printer Setup Utility

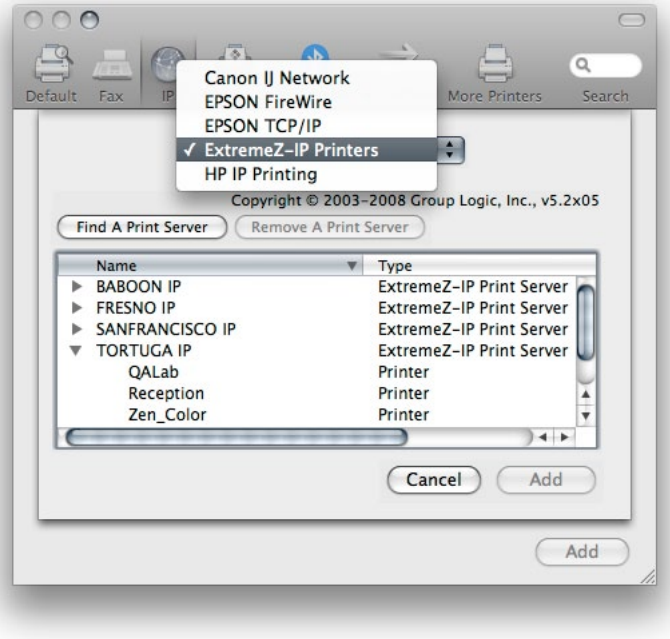
You can add an ExtremeZ-IP print queue from the **Printer Setup Utility** in two ways. The most common way is to use the optional Macintosh print components that come with ExtremeZ-IP. However, if you do not want to install any additional software on the Macintosh, you can use the built-in Bonjour browse capability to add a printer.

Adding a Printer using the optional ExtremeZ-IP Print Components

If you have installed the Macintosh Print Components on the Macintosh, you can use the custom ExtremeZ-IP Printer

To use the ExtremeZ-IP components to add a printer, do the following:

1. Use the Printer Browse Module (PBM) to locate an ExtremeZ-IP print queue.
2. Select **ExtemeZ-IP Printers** on the pop-up list. A list of the ExtremeZ-IP Printers on the network appears.



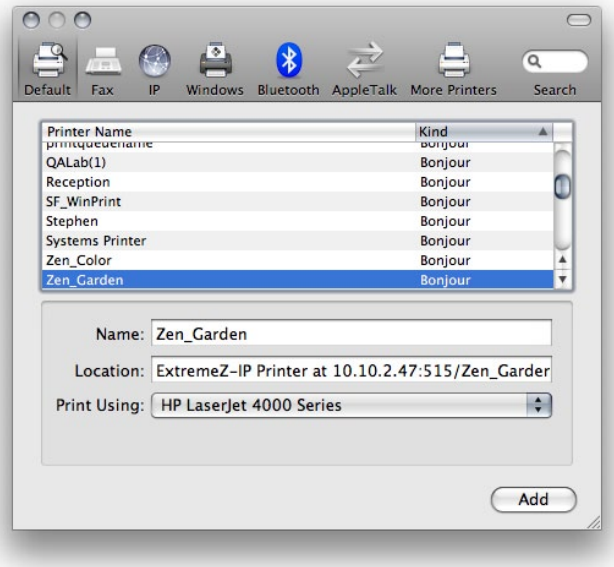
3. Select the queue you want to use.
4. Click **Add**.

Adding a Printer using Bonjour from the Printer Setup Utility

To add a printer using Bonjour from the Printer Setup Utility, do the following:

1. Open the **Printer Setup Utility** or the **Print & Fax** System Preferences pane depending on what version of Mac OS X you are using.
2. Choose **Add.**
3. Pick your printer from the **Printer Browser**.

NOTE If a PPD was specified in the ExtremeZ-IP print queue configuration on the server, ExtremeZ-IP sends a printer PPD hint to the client Mac. If the client Macintosh already contains a valid PPD for the printer type, the Print Using dropdown is set to the correct printer type automatically.

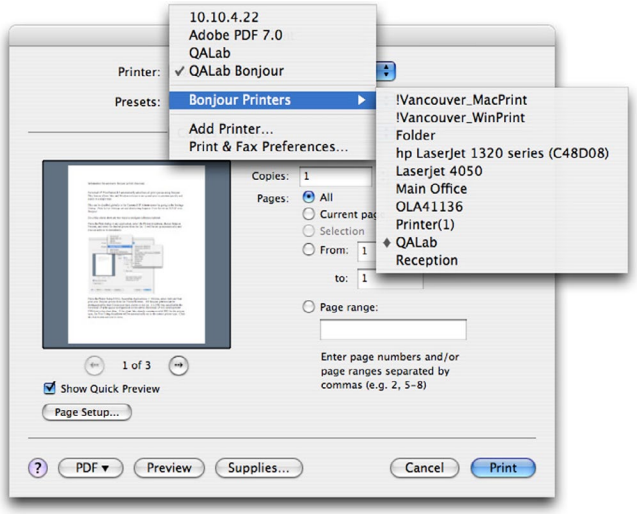


4. Click the **Add** button.

Using Bonjour Within the Print Dialog

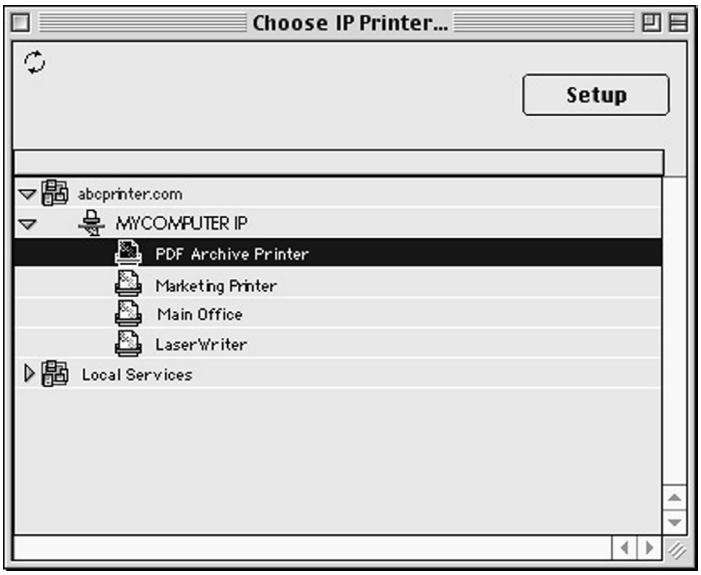
To set up a printer from within the print dialog using Bonjour on Mac OS 10.4, Tiger (Apple removed the feature in Leopard), do the following:

1. Choose **Print** from any application
2. From the **Printer** dropdown menu, choose **Bonjour Printers.**
3. Select the desired printer from the list.



Choosing a Printer with Mac OS 9

Once they have installed the **Choose IP Printer** program, Mac OS 9 clients use **Choose IP Printer** on the Apple menu instead of the **Chooser** to find the ExtremeZ-IP printers and set up desktop printers.

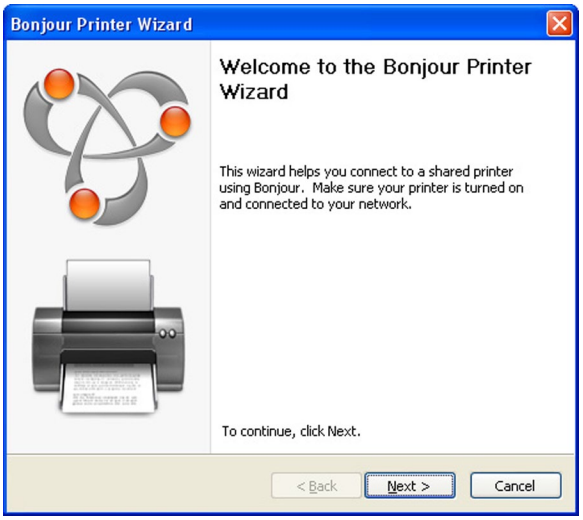


Using Bonjour from Windows

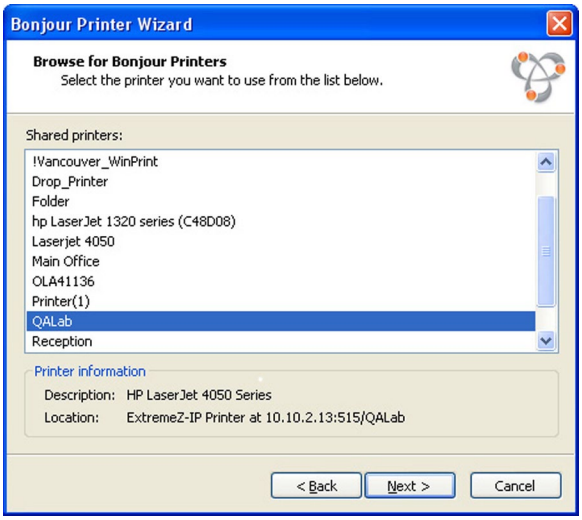
To set up a Bonjour printer from Windows, do the following:

1. Install **Apple Bonjour for Windows**, available at: http://www.apple.com/support/downloads/bonjourforwindows.html

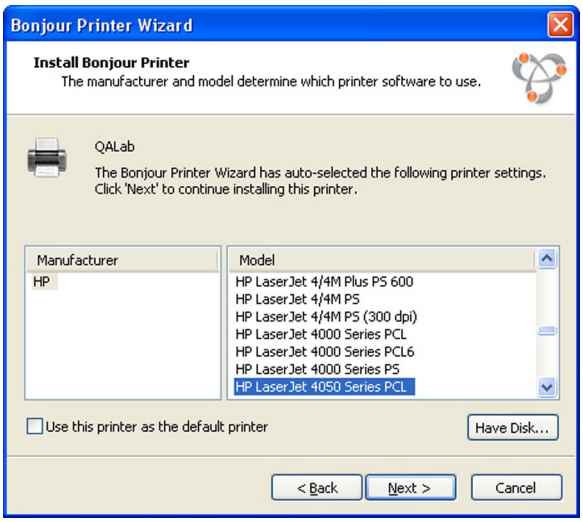
2. Once installed, run the **Bonjour Printer Wizard**.



3. Click **Next**.

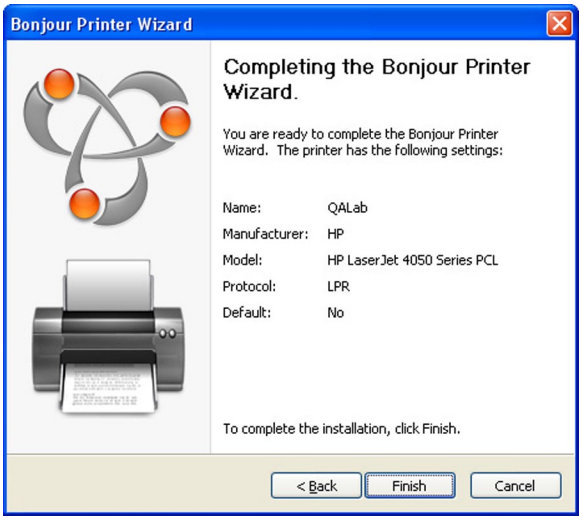


4. Select the printer you would like to install, then, click **Next**.



If a PPD was specified in the ExtremeZ-IP print queue configuration on the server, ExtremeZ-IP sends the printer model listed in the PPD to the Windows client. If the Windows client already contains a valid driver for the printer type, the printer manufacturer and model should be automatically selected.

5. If a PPD was not selected automatically, select the appropriate manufacturer and model and click **Next**.



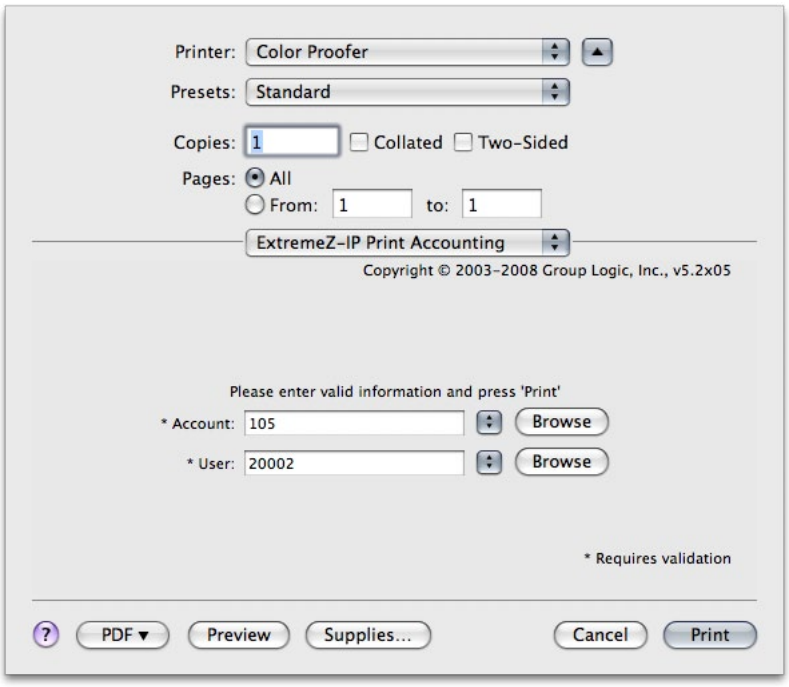
Using Print Accounting Features from a Client

When a Macintosh user prints from a program and sends the job to a print queue to which you have assigned codes using ExtremeZ-IP Print Accounting, their Print dialog box displays the information you assigned.

To use Print Accounting, do the following:

1. Print to an available ExtremeZ-IP Print Server print queue.

If print accounting is enabled for that print queue, a special dialog box appears. The following is an example:



2. Type in the information requested by the server.

In the example above, the ExtremeZ-IP Administrator has enabled **Browse** buttons for each field, so the Macintosh user can browse the list of codes for that field. Fields that have asterisks (*) before their names are required and must be completed before the job can be sent.

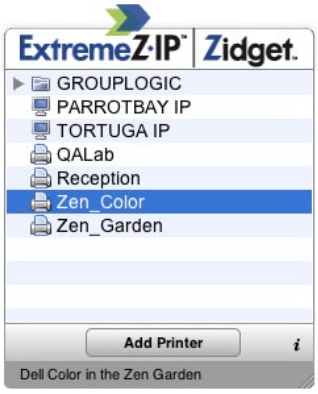
3. Click **Print** to send the job to the selected print queue.


ExtremeZ-IP®
Zidget®

ExtremeZ-IP Zidget

The ExtremeZ-IP Zidget is a new way of connecting to ExtremeZ-IP file and print servers. Zidget is a Dashboard Widget that the Macintosh user can use to discover and connect to a file server whether or not the server is in the user's local subnet. Zidget also allows the Macintosh user to browse DFS namespaces that are shared through the ExtremeZ-IP server. Using Zidget, the Macintosh user can also browse for and add ExtremeZ-IP printers. Zidget will automatically download the PPD for the printer, and set up the print queue without the user having to use the Print Center. The Zidget can also be used to add queues on the print server that receive jobs directly, or *direct print* printers that are advertised by the ExtremeZ-IP server but do not route jobs through the print server.

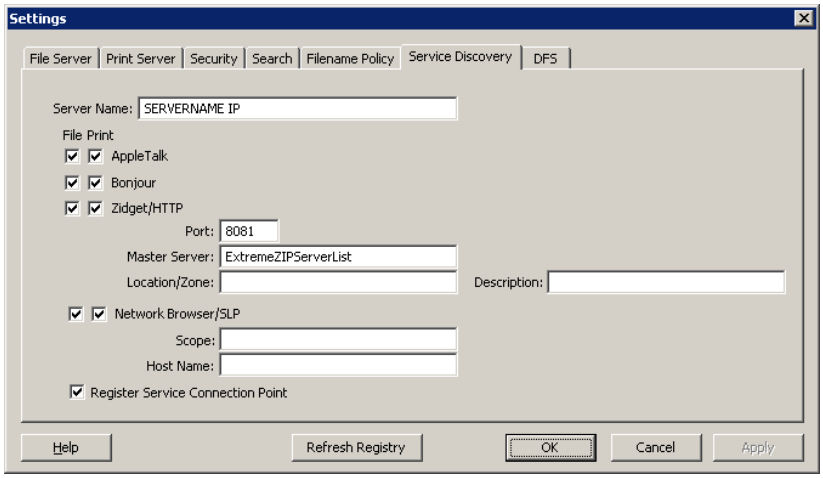
Zidget contacts a server called the ExtremeZ-IP master server to retrieve a list of all the ExtremeZ-IP servers in your organization. It then contacts each of those servers to find out whether they are just file servers or if they also are print servers. If the server is a print server it then retrieves a list of all the print queues on that server. The servers as well as individual print queues can be assigned to locations or *zones*. Once the Zidget has retrieved information from all the servers it merges them into a list of locations for the user to choose from.



Although many customers may choose to mimic their existing AppleTalk zone structure, they can also use a more complex location-based method for organizing their print queues. For that matter, they can use any other hierarchical arrangement they would like, such as Color and Black and White. The location-based method can be hierarchical such as building, floor, and room.

Configuring the ExtremeZ-IP server for Zidget access

By default, ExtremeZ-IP is configured to support the Zidget with no additional configuration. In the **Service Discovery** tab of the Administrator you can change the settings related to Zidget/HTTP. By default ExtremeZ-IP servers are configured to use a master server called ExtremeZIPServerList. Since this name is not a fully qualified DNS name, the ExtremeZ-IP servers and Zidget clients will append their default DNS suffix to the name. This allows the Zidget to be deployed in most environments without needing any additional configuration beyond creating a DNS CNAME record of ExtremeZIPServerList.yourdomain.com for your ExtremeZ-IP server.



If you would like, you can also assign a server to a specific location. A location is composed of locations separated by colons that contains the hierarchy of zones/locations that the Zidget should use to display them. An example for single level zone is “GLIHQ” and a multi-level location might be “Virginia:Arlington:1st Floor”. In addition to the location property of a print queue or file server, an administrator can also assign them descriptions. When a queue is selected, the status area of Zidget displays any description that the administrator has set for the queue. However, locations and descriptions are optional. If no servers or print queues have locations assigned to them, then they are all displayed in Zidget as a list without any additional hierarchy. If only some of the servers do not have a location, they will be displayed at the end of the list below the locations.

Adding additional servers to the Master Server

If you have multiple ExtremeZ-IP servers you designate one server as the master server that the Zidget will contact to discover the other ExtremeZ-IP servers on the network. The master server has an XML file on it called MasterServerList.xml that lists the other servers on the network. If you only have one server on your network you may use the MasterServerList.xml that is auto-generated by that server. An auto-generated MasterServerList.xml file is identical to the ServerList.xml file that the server would return. The format of the ServerList.xml and auto-generated MasterServerList.xml is as follows:

```
http://ExtremeZIPServerList:8081/ServerList.xml
<?xml version=”1.0” encoding=”UTF-8”?>
<servers>
        <serverListVersion>1.0</serverListVersion>
        <minimumClientVersion>1.4</minimumClientVersion>
        <server>
                <AFPPort>548</AFPPort>
                <LPRPort>515</LPRPort>
                <display_name>EXAMPLE IP</display_name>
                <hostname>example.grouplogic.com</hostname>
                <port>8081</port>
                <description/>
                <location/>
                <protocol>afp</protocol>
                <protocol>ezip</protocol>
        </server>
</servers>
```

To make a manually generated MasterServerList.xml, you take the information from each server and put it in one file. The HTML Files folder inside the ExtremeZ-IP program folder also contains a TemplateMasterServerList.xml that you can modify to contain the information specific to your organization.

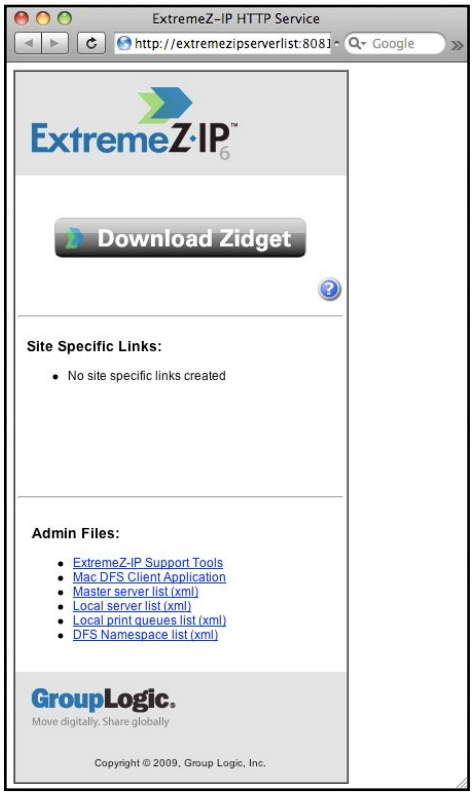
Installing and Configuring the Zidget on the Client

In order to make deployment of the Zidget as easy as possible, it can be downloaded directly from the HTTP server that is built into ExtremeZ-IP. You can link to the URL for the Zidget from any web page, send it in an email, have users manually type it into a web browser, or distribute it any other way that you see fit. The Zidget could also be made part of the standard corporate deployment or installed in /Library/Widgets on multiple Macintoshes using technologies such as Apple Remote Desktop.

If you have not already installed Zidget, the ExtremeZ-IP server lets you download Zidget directly from the URL http://your-server:8081. Because the Zidget is HTTP based, it is trivial to add a Download Zidget link to your company's intranet or support website. If the Zidget is downloaded by Safari, the download will automatically present the user with a dialog asking them if they want to install it. By default, Zidget will resolve ExtremeZIPServerList.yourdomain.com in DNS in order to find the Master Server from which it will retrieve a list of the available printers and file servers. If you are using the default setup and have created this DNS CNAME record to point to your ExtremeZ-IP server, no further steps are required on the Macintosh to configure the Zidget after it has been installed.

To install Zidget on a Macintosh client, do the following:

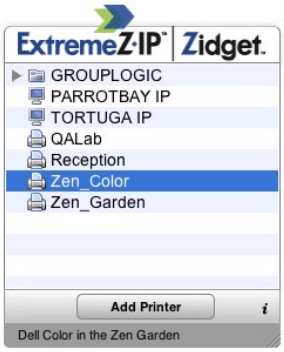
1. In a web browser such as Safari, navigate to the ExtremeZ-IP server (e.g. http://your-server:8081).



2. Click on the **Download Zidget** link. The file Zidget.wdgt.zip will be downloaded.

3. Click **Install** to confirm the dialog asking if you want the Zidget installed (if you have not disabled auto installation of widgets in Safari).

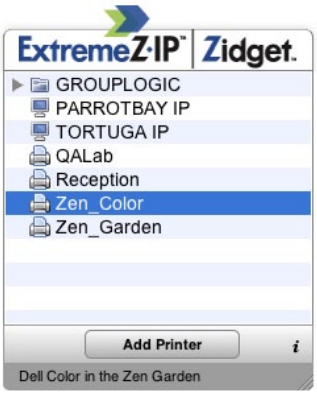
4. If your **Master Server** is something other than the default ExtremeZIPServerList, click the "**i**" icon to modify this setting. The **Refresh Interval** determines how often the available file servers, printers, and DFS namespaces in the Zidget are refreshed.



Adding a printer with the Zidget

To add a printer with Zidget, do the following:

1. Press the **F12** key to invoke **Dashboard.**
2. Select the **ExtremeZ-IP Zidget.**



3. Double-click a location/zone if necessary.
4. Select a printer from that location/zone.
5. Click the **Add Printer** button and the printer will be created on the Macintosh with the proper PPD if one is available from the server.
6. The status section of the Zidget updates to say the printer was successfully created.

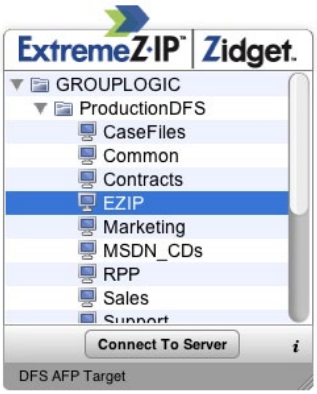
Mounting ExtremeZ-IP shared volumes with the Zidget

1. Press the **F12** key to invoke **Dashboard**.
2. Select the **ExtremeZ-IP Zidget**.

3. Double-click a location/zone if necessary.
4. Select a server from that location/zone.
5. Click the **Connect to Server** button.

Mounting DFS shared volumes with the Zidget

1. Press the **F12** key to invoke **Dashboard**.
2. Select the **ExtremeZ-IP Zidget**.



3. Double-click the DFS domain or server, in this example **GROUPLOGIC**.
4. Double-click the DFS root, in this example **ProductionDFS**.
5. Select a DFS target.
6. Click the **Connect to Server** button.

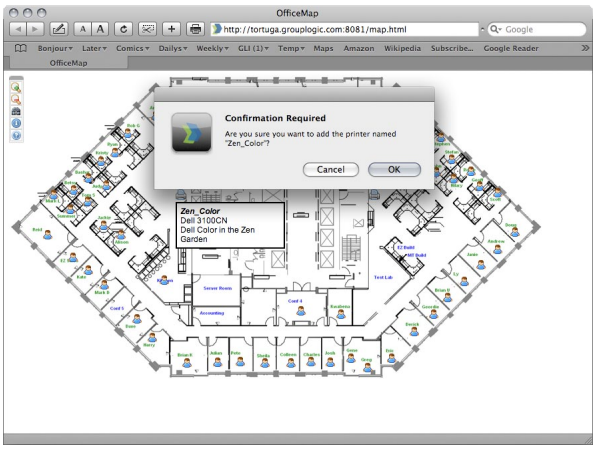
Adding a printer from a Web Page

Dashboard widgets have limited ability to interact with the operating system and cannot natively add printers to the Macintosh. Therefore the Zidget includes an application—Dashboard widgets are implemented as Macintosh packages—that the Zidget invokes to download the PPD and create the printer on the Macintosh.

The helper application can also be used as an Internet protocol helper for ezip:// URLs. This enables Safari or another web browser to create a printer when you click on a specially formatted link from a standard web page such as an office map with links for different areas. If you click on a URL to invoke the helper application, it asks if you want to add the printer. Whereas when Zidget invokes the helper application, the helper application operates silently. Creating a web-based Printer Location Map is a very effective way to let users easily find and add printers. Taking a scan of the map and making a PDF in Adobe Acrobat is one simple way to create a web page with a map of the user's floor. Acrobat will let you add links for areas of the picture without having to know any HTML.

To add a printer from a Web page, do the following:

1. Click the icon of the nearest printer on the map.
2. Click **OK** to confirm the dialog asking if the printer should be added.



ExtremeZ-IP®

MACINTOSH CLIENT CONFIGURATION FOR DFS SUPPORT

In order for Macintosh clients to access ExtremeZ-IP DFS volumes, each client needs to be configured so that it can properly locate and mount DFS resources. This configuration can be accomplished through the installation of the ExtremeZ-IP Zidget, a Macintosh client application, or by updating the existing Macintosh auto_master configuration file.

Zidget DFS support is compatible with Mac OS X 10.4 or later. DFS Client application and auto_master DFS support require Mac OS X 10.5 or later.

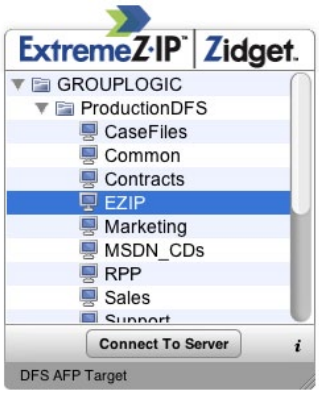
If Macintosh clients are using home directories located on DFS volumes, the Mac DFS Client application must be installed. The Zidget and auto_master modification options do not support DFS home directories.

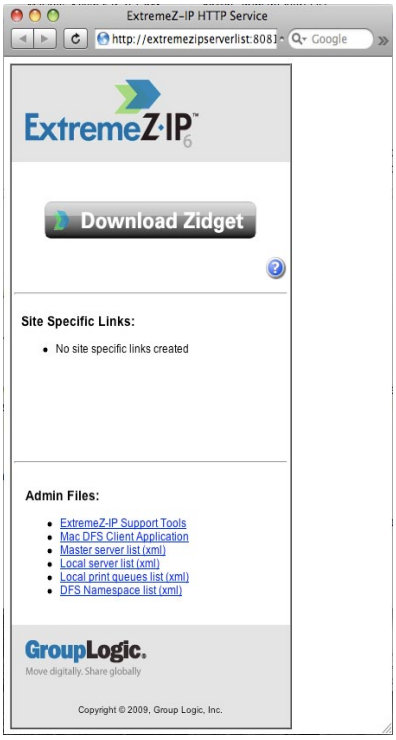
When using the DFS Client application or auto_master configuration options, the Macintosh client requires Kerberos authentication to browse resources in the DFS namespace. For this reason, both of these options require that your Macintosh clients are bound to Active Directory. This is done on the Macintosh client using the Directory Utility located in /Applications/Utilities/.

Macintosh Client Configuration

ExtremeZ-IP Zidget Option

The ExtremeZ-IP Zidget is the simplest way to configure a Macintosh client to access DFS. The Zidget allows Mac users to browse the DFS namespace and mount individual DFS target volumes. Once mounted, the user can access the chosen DFS target volumes through the Finder, as they would traditional shared volumes. The Zidget's primary advantage over the DFS Client application and auto_master modification options is that it is compatible with Mac OS X 10.4 or later and that it allows users full file search capabilities. Full details on installing, configuring, and accessing DFS with the Zidget can be found beginning on page 64 of this manual.





DFS Client Application Option

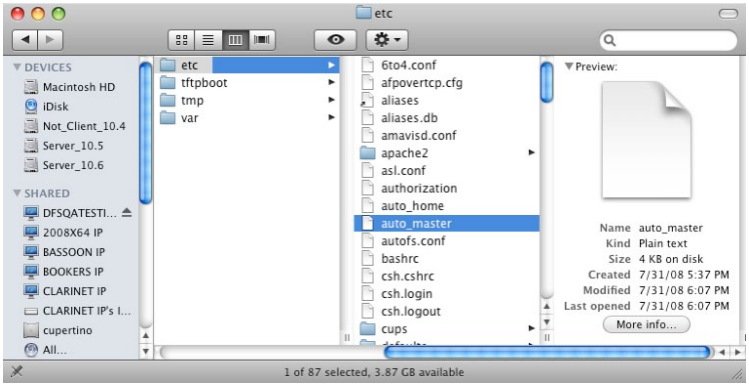
If you require DFS home directory support or your Macintosh clients must be able to browse your DFS namespace using the Finder, the DFS Client application is required. This application automates most of the steps required to make Finder integrated browsing and DFS home directories work on the Macintosh. The only additional step beyond installing the software is to edit the application's configuration file with the DNS name of the ExtremeZ-IP DFS root server(s) you will be using.

To install the ExtremeZ-IP DFS Client, open a web browser on the Macintosh client and navigate to http://yourservername:8081 (unless you changed the HTTP port of the server). Click the **Mac DFS Client Application** link to download the installer zip file, containing a standard Mac OS Installer and an example dfsservers.conf file. Edit the dfsservers.conf file to contain the address for your ExtremeZ-IP DFS root server(s) and copy it to the /etc directory of the Macintosh. Then, run the DFS Client installer on the Macintosh client. If a dfsservers.conf file is not present in the /etc directory before the DFS Client is first launched, a template file will be created but will still need to have the proper ExtremeZ-IP DFS root server(s) added to it. This completes the Macintosh client configuration and the client can then access DFS volumes.

Manually Modifying auto_master Option

If you prefer not to install the DFS client application, some manual editing of Macintosh configuration files is required. While these files must be updated on every client machine that needs access to DFS, they are not client specific. These files can be updated on one client and then pushed out to other clients using a tool such as Apple Remote Desktop.

In Mac OS X 10.5 or later, the client's auto_master file, located in /etc, must be modified to invoke the automount of the DFS targets. The TextEdit program included with the Mac OS does not allow editing root system files. It is recommended you use the free TextWrangler application available at: http://www.barebones.com/products/textwrangler/

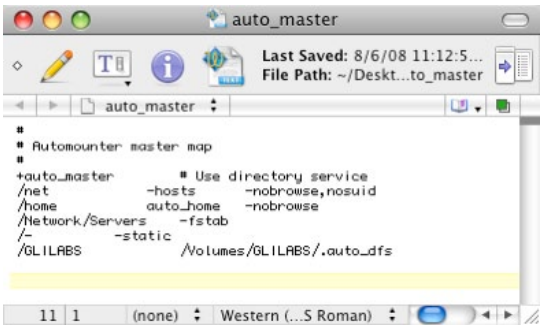


In the auto_master file, add the following line:

/<new volume name> /Volumes/<new volume name>/.auto_dfs

The 'new volume name' is the name of the ExtremeZ-IP DFS volume that was created in the **Namespace** setup process on the **DFS** tab of the **Settings** dialog. Example: if the volume to be used for DFS roots is called 'GLILABS' then the auto_master line would be:

/GLILABS /Volumes/GLILABS/.auto_dfs



Be sure there is a new, blank line at the end of this file. If this new line does not exist, DFS will fail to function on the client. This file can be copied to any other Macintosh clients that need access to DFS; it is not necessary to manually edit the file on each client.

It is recommended that the AUTOMOUNT_TIMEOUT parameter in /etc/autofs.conf be changed to 300 (seconds) in order for changes in the DFS namespace to be reflected by AutoFS. AutoFS is used by the Macintosh client to automatically mount DFS targets as they are accessed.

Once you've completed these steps on the Macintosh client, reboot the client so the automount changes will take effect.

At this point, you will be able to mount the ExtremeZ-IP DFS volume from the Macintosh client and browse and utilize your DFS structure.

Additional Configuration for Home Directories

If you plan to use home directories, you must also make one additional change on the server side. On the ExtremeZ-IP DFS root server, in addition to the automatically created DFS root volume, you must also separately share the home directory subfolder inside of that DFS root volume.

For our example we will be using a DFS path home directory of \\GLILABS\DFSHOMES\Sales\phd which from the Macintosh side looks like the following:

```
webinar:~ phd$ sudo dscl . read /Users/phd | grep Home
NFSHomeDirectory: /Users/phd
OriginalHomeDirectory: <home_dir><url>afp://GLILABS.glilabs.com/DFSHOMES</url><path>Sales/phd</path></home_dir>
OriginalNFSHomeDirectory: /Network/Servers/GLILABS.glilabs.com/DFSHOMES/Sales/phd
SMBHome: \\GLILABS\DFSHOMES\Sales\phd
SMBHomeDrive: H:
```

For home directories, unlike the basic solution where we have a DFS Root Emulator volume represent the namespace(s), we have a server represent the first half of the namespace (the DomainHost portion). An example will probably make this clear. If the DFS path to the user's home directory is \\GLILABS\DFSHOMES\Sales\phd, at login that will be converted to afp://GLILABS.glilabs.com/DFSHOMES/Sales/phd, therefore we have to have a volume called DFSHomes on a server named GLILABS. The DFSClient script takes care of the first part but you need to make sure there is a volume on the server that matches the second portion of the DFS namespace. In this example, you would share the Sales folder. This folder should already exist In C:\Program Files\Group Logic\ExtremeZ-IP\DFS Volumes\namespace\ and just needs to be shared as an ExtremeZ-IP volume. This volume represents the specific DFS namespace on the DFS DomainHost where the user's home directory is located. With this subvolume shared out, the Macintosh user will be able to use their DFS home directory.

ExtremeZ-IP®

APPENDICES

Appendix A: Using the Registry Keys

You can use Windows registry keys to change some settings in ExtremeZ-IP beyond what can be configured using the ExtremeZ-IP Administrator. This section describes some of the more commonly used registry keys. You can view a full list of registry settings in the ExtremeZ-IP Administrator Online Help.

The registry settings for the ExtremeZ-IP service are located in the \HKLM\System\CurrentControlSet\Services\ExtremeZ-IP\ section of the registry. In the examples below this will be abbreviated as ...\RegistryKeyName. There are two main kinds of registry keys; refreshable and nonrefreshable. Refreshable keys take effect when you click the Refresh Registry button in the ExtremeZ-IP Administrator. Nonrefreshable keys on the other hand will not take effect until the service is restarted.

Reconnecting a dropped session

ExtremeZ-IP supports reconnecting user sessions in the event of a network outage, server crash, or cluster failover. In addition, it supports automatically closing locked files after a Macintosh client crash or reboot. You can use the following registry keys to affect the way ExtremeZ-IP reconnects after a session is disconnected:

`...\Parameters4\Refreshable\`

- ServerSupportsReconnectUAM
- ReconnectTimeout
- ServerSupportsAFP3Reconnect
- ReconnectServerKeyLifetime
- ServerEmbedsPasswordInReconnectCredential
- MaxDuplicateSessionsWaiting
- ReconnectUAMExpirationInterval

Sending password expiration notifications during session

In addition to notifying Macintosh client users that their password is expiring at initial login, ExtremeZ-IP can also be configured to notify users during their session. Notification during a session requires that notification at initial login is enabled. To do this, select the **Notify Mac clients of password expiration** option on the **Security** tab of the **Settings** dialog in the **ExtremeZ-IP Administrator**. Here, you will also specify the number of days from expiration that the notification should begin.

Next, you will edit the registry key named `PasswordExpirationReminderInterval` in:
`...\Parameters4\Refreshable\`

The value of this registry key determines the interval at which the client is notified of the upcoming password expiration in minutes. The interval can be configured from 1 minute to 1440 minutes (1 day).

Scheduling re-indexing with EZIPUTIL

By default, ExtremeZ-IP automatically re-indexes file entries for its indexed search. But you can use EZIPUTIL in a batch file or script to schedule re-indexing on a set schedule during off-hours and trigger it with a scheduling service of your choice.

1. First, disable automatic re-indexing by removing the check in the **Automatically rebuild sparse indexes** checkbox found in the **Search Settings** dialog box (see section above "Settings").

2. EZIPUTIL.exe is located in the chosen ExtremeZ-IP program installation directory on the server. Use the following command, which is included in the EZIPUTIL utility, to trigger the re-indexing of a volume manually. You can also use it in a script or batch file to schedule re-indexing during off-hours:

```
EZIPUTIL VOLUME /REINDEX /NAME:volumename /PATH:root directory path  [/SERVICENAME:servicename]
```

SERVICENAME is needed only if ExtremeZ-IP is running on a cluster.

Adding print log entries to text files

To configure the ExtremeZ-IP server to add each new print log entry to a specified text file automatically, do the following.

`..\Parameters4\PrintRefreshable`

1. Modify the PrintAccountingLogFilePath in the registry.
2. Set the value to the full path where you want the logs (e.g., C:\Logs\Log.txt)

Customizing ExtremeZ-IP Print Processing Log columns

You can use registry keys to override the default configuration and customize your view of the Print Processing Log to display various columns in any order. The two formats are IP Printing for regular ExtremeZ-IP print support and Print Accounting for print accounting use. Both formats are configured in the same manner, but Print Accounting has more options and some special considerations. See page 52 for instructions on using the Print Processing Log.

Columns

job_id	a unique ID generated by ExtremeZ-IP for this print job
job_name	name of the file being printed
job_user	name of user generating the print job
job_host	name of computer that submitted the print job
job_ip	IP address of computer that submitted the print job
job_datetime	month/day/year and time of day job was submitted
job_size	size of the file being printed
job_pagecount	number of pages in the print job
job_pagesize	the type of paper the job is being printed on
job_numcopies	number of copies in this print job
job_queue	name of the print queue that is processing the print job
job_printer	name of the printer processing the print job
job_date	month/day/year of submitted print job
job_time	time of day job was submitted
job_imagesize	dimensions in pixels of submitted print job
job_code1	Print Accounting information submitted with print job
job_code2	Print Accounting information submitted with print job
job_code3	Print Accounting information submitted with print job
job_code4	Print Accounting information submitted with print job
job_code5	Print Accounting information submitted with print job

A REG_SZ string entry in the registry controls custom configuration. The format for the string is to add types of data separated by a forward slash '/'. The format respects the order and number of types in the string value. For example, if you wanted to restrict your view to job_name, job_dateandtime, and job_printer only, you would enter 'job_name/job_dateandtime/job_printer' as your string value.

By default, ExtremeZ-IP has a specific column order. If no registry key is present, that order will be used. The following examples illustrate keys that would set up the default columns. They can be used as a starting point for customization.

`..\Parameters4 \PrintRefreshable`

Registry Path: PrintAccountingLogFormat

Type: REG_SZ

Data(by default): job_name/job_user/job_host/job_ip/job_date/job_time/job_size/job_pagecount/job_pagesize/job_imagesize/job_numcopies/job_queue/job_printer/job_code1/job_code2/job_code3/job_code4/job_code5

Appendix B: Monitoring ExtremeZ-IP

ExtremeZ-IP allows administrators and Group Logic's support staff to "look inside" ExtremeZ-IP to watch the load on the server, detect problems with shares and print queues, and diagnose performance bottlenecks. ExtremeZ-IP supports counters for Windows Performance Monitor, Microsoft Operations Manager (MOM), and other instrumentation platforms that support Windows Management Interface (WMI), Microsoft's generic interface for monitoring applications in production. WMI-aware applications alert administrators to errors and help diagnose problems.

Most of the counters provided in ExtremeZ-IP are global for the ExtremeZ-IP instance or the server. For some of the users and volume counters, however, an administrator can choose to view a single instance. For example, "instance" could be the number of bytes per second for an individual user.

ExtremeZ-IP performance counters are compatible with both 32-bit and 64-bit versions of Windows 2003 Server, Windows Server 2008, Windows XP, and Windows Vista.

ExtremeZ-IP Performance Counters

Counters for ExtremeZ-IP File Server

Users (Total) - The number of currently-connected users, including users that are idle or sleeping
Users (Idle) - The number of currently-connected users that have been idle for at least 10 minutes
Users (Sleeping) - The number of currently-connected users that are sleeping
Users (Active) - The number of currently-connected users that are active (neither idle or sleeping)
Users (Waiting For Reconnect) - The number of sessions representing connections that have been terminated but are waiting for users to reconnect
AFPCommands Replied To - The number of AFP commands replied to
AFP Commands Replied To/sec - The number of AFP commands replied to per second
Volumes (Total) - The number of ExtremeZ-IP volumes
Volumes (Offline) - The number of ExtremeZ-IP volumes that are currently offline
Volumes (Online) - The number of ExtremeZ-IP volumes that are currently online
User Disconnects - The number of times users have disconnected from the server in an ungraceful manner
Failed Logons - The number of times users have failed to login because of an invalid password, username or Kerberos ticket
Reconnects - The number of times users have reconnected to the server
Max Files Open - The maximum number of file forks that have been open at any one time
Max File Locks - The maximum number of files locks that have been in place at any one time
Max Users (Active) - The maximum number of users that have been active at any one time
Max Users (Idle) - The maximum number of users that have been idle at any one time
Max Users (Sleeping) - The maximum number of users that have been sleeping at any one time
Max Users (Total) - The maximum number of users logged-in at any one time
Max Users (Waiting For Reconnect) - The maximum number of sessions waiting for users to reconnect at any one time
Thread Pool Size - The total number of threads that are in the thread pool
Thread Pool (Working) - The number of threads in the thread pool that were actively working at the time of sampling
Thread Pool (Quiet) - The number of threads in the thread pool that have not done any work in over a minute
Thread Pool (Stalled) - The number of threads in the thread pool that have been processing a task for more than one minute
Max Thread Pool Size - The maximum number of threads in the thread pool at any one time
Max Thread Pool (Working) - The maximum number of threads in the thread pool that were actively working during any sample
User Licenses Used - The current number of user licenses being used

Counters for ExtremeZ-IP File Server Users

Open Forks - Number of open forks

File Locks - Number of file locks
Bytes Received/sec - Number of bytes read from the network per second
Bytes Transmitted/sec - Number of bytes sent on the network per second

NOTE Users' counters can be viewed as an individual user or as a total of all activity.

Counters for ExtremeZ-IP File Server Volumes

Cache Hit Rate - The node table cache hit rate
Bytes Read/sec - Number of bytes read from disk per second and returned to clients
Bytes Written/sec - Number of bytes written from disk per second

NOTE Volume counters can be viewed per volume or as a total.

Counters for ExtremeZ-IP Printing

Print Queues - The number of print queues
Print Queues Online - The number of print queues currently online
Print Queues Offline - The number of print queues currently offline
Jobs Spooling - Current number of print jobs spooling
Bytes Printed/sec - The number of bytes printed per second

Counters for ExtremeZ-IP Print Queues

Print Jobs Offline - The number of print jobs currently offline
Job Errors - The number of print errors since ExtremeZ-IP launch
Total Jobs Printed - The total number of jobs printed since ExtremeZ-IP launch
Total Pages Printed - The total number of pages printed since ExtremeZ-IP launch
Is Queue Online - Indication if the queue is online - 1 if yes, 0 if no

NOTE Print Queue counters can be viewed per queue or as a total for all queues.

Appendix C: Configuring Guest Access

Configuring Guest Access for Windows XP and Above

To support guest access when running under Windows XP and later operating systems you must change a Windows default security setting. Starting with Windows XP, the **Anonymous Logon** group is no longer a member of the **Everyone** group by default. Microsoft made this change because, if system administrators did not realize that anonymous users were members of the **Everyone** group, they might inadvertently grant them access to resources only intended for authenticated users.

In order to enable guest access, ExtremeZ-IP requires that the **Anonymous Logon** group be a member of the **Everyone** group. For operating systems that do not support this behavior by default, a system-wide setting needs to be changed.

To change this setting, do the following:

1. Open Local Security Policy. Go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Local Security Policy.**
2. Navigate to **Local Policies** -> **Security Options**.
3. Set the **Network access: Let Everyone permissions apply to anonymous users** setting to **Enabled**.

Appendix D: Legal Notices

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

http://www.openssl.org/source/license.html

1.7 “Original Code” means (a) the Source Code of a program or other work as originally made available by Apple under this License, including the Source Code of any updates or upgrades to such programs or works made available by Apple under this License, and that has been expressly identified by Apple as such in the header file(s) of such work; and (b) the object code compiled from such Source Code and originally made available by Apple under this License

1.8 “Source Code” means the human readable form of a program or other work that is suitable for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an executable (object code).

1.9 “You” or “Your” means an individual or a legal entity exercising rights under this License. For legal entities, “You” or “Your” includes any entity which controls, is controlled by, or is under common control with, You, where “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

2. Permitted Uses; Conditions & Restrictions. Subject to the terms and conditions of this License, Apple hereby grants You, effective on the date You accept this License and download the Original Code, a world-wide, royalty-free, non-exclusive license, to the extent of Apple’s Applicable Patent Rights and copyrights covering the Original Code, to do the following:

2.1 Unmodified Code. You may use, reproduce, display, perform, internally distribute within Your organization, and Externally Deploy verbatim, unmodified copies of the Original Code, for commercial or non-commercial purposes, provided that in each instance:

(a) You must retain and reproduce in all copies of Original Code the copyright and other proprietary notices and disclaimers of Apple as they appear in the Original Code, and keep intact all notices in the Original Code that refer to this License; and

(b) You must include a copy of this License with every copy of Source Code of Covered Code and documentation You distribute or Externally Deploy, and You may not offer or impose any terms on such Source Code that alter or restrict this License or the recipients’ rights hereunder, except as permitted under Section 6.

2.2 Modified Code. You may modify Covered Code and use, reproduce, display, perform, internally distribute within Your organization, and Externally Deploy Your Modifications and Covered Code, for commercial or non-commercial purposes, provided that in each instance You also meet all of these conditions:

(a) You must satisfy all the conditions of Section 2.1 with respect to the Source Code of the Covered Code;

(b) You must duplicate, to the extent it does not already exist, the notice in Exhibit A in each file of the Source Code of all Your Modifications, and cause the modified files to carry prominent notices stating that You changed the files and the date of any change; and

(c) If You Externally Deploy Your Modifications, You must make Source Code of all Your Externally Deployed Modifications either available to those to whom You have Externally Deployed Your Modifications, or publicly available. Source Code of Your Externally Deployed Modifications must be released under the terms set forth in this License, including the license grants set forth in Section 3 below, for as long as you Externally Deploy the Covered Code or twelve (12) months from the date of initial External Deployment, whichever is longer. You should preferably distribute the Source Code of Your Externally Deployed Modifications electronically (e.g. download from a web site).

2.3 Distribution of Executable Versions. In addition, if You Externally Deploy Covered Code (Original Code and/or Modifications) in object code, executable form only, You must include a prominent notice, in the code itself as well as in related documentation, stating that Source Code of the Covered Code is available under the terms of this License with information on how and where to obtain such Source Code.

2.4 Third Party Rights. You expressly acknowledge and agree that although Apple and each Contributor grants the licenses to their respective portions of the Covered Code set forth herein, no assurances are provided by Apple or any Contributor that the Covered Code does not infringe the patent or other intellectual property rights of any other entity. Apple and each Contributor disclaim any liability to You for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, You hereby assume sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow You to distribute the Covered Code, it is Your responsibility to acquire that license before distributing the Covered Code.

3. Your Grants. In consideration of, and as a condition to, the licenses granted to You under this License, You hereby grant to any person or entity receiving or distributing Covered Code under this License a non-exclusive, royalty-free, perpetual, irrevocable license, under Your Applicable Patent Rights and other intellectual property rights (other than patent) owned or controlled by You, to use, reproduce, display, perform, modify, sublicense, distribute and Externally Deploy Your Modifications of the same scope and extent as Apple’s licenses under Sections 2.1 and 2.2 above.

4. Larger Works. You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In each such instance, You must make sure the requirements of this License are fulfilled for the Covered Code or any portion thereof.

5. Limitations on Patent License. Except as expressly stated in Section 2, no other patent rights, express or implied, are granted by Apple herein. Modifications and/or Larger Works may require additional patent licenses from Apple which Apple may grant in its sole discretion.

6. Additional Terms. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations and/or other rights consistent with the scope of the license granted herein (“Additional Terms”) to one or more recipients of Covered Code. However, You may do so only on Your own behalf and as Your sole responsibility, and not on behalf of Apple or any Contributor. You must obtain the recipient’s agreement that any such Additional Terms are offered by You alone, and You hereby agree to indemnify, defend and hold Apple and every Contributor harmless for any liability incurred by or claims asserted against Apple or such Contributor by reason of any such Additional Terms.

7. Versions of the License. Apple may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Once Original Code has been published under a particular version of this License, You may continue to use it under the terms of that version. You may also choose to use such Original Code under the terms of any subsequent version of this License published by

Apple. No one other than Apple has the right to modify the terms applicable to Covered Code created under this License.

8. NO WARRANTY OR SUPPORT. The Covered Code may contain in whole or in part pre-release, untested, or not fully tested works. The Covered Code may contain errors that could cause failures or loss of data, and may be incomplete or contain inaccuracies. You expressly acknowledge and agree that use of the Covered Code, or any portion thereof, is at Your sole and entire risk. THE COVERED CODE IS PROVIDED "AS IS" AND WITHOUT WARRANTY, UPGRADES OR SUPPORT OF ANY KIND AND APPLE AND APPLE'S LICENSOR(S) (COLLECTIVELY REFERRED TO AS "APPLE" FOR THE PURPOSES OF SECTIONS 8 AND 9) AND ALL CONTRIBUTORS EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. APPLE AND EACH CONTRIBUTOR DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE COVERED CODE, THAT THE FUNCTIONS CONTAINED IN THE COVERED CODE WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE COVERED CODE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE COVERED CODE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY APPLE, AN APPLE AUTHORIZED REPRESENTATIVE OR ANY CONTRIBUTOR SHALL CREATE A WARRANTY. You acknowledge that the Covered Code is not intended for use in the operation of nuclear facilities, aircraft navigation, communication systems, or air traffic control machines in which case the failure of the Covered Code could lead to death, personal injury, or severe physical or environmental damage.

9. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL APPLE OR ANY CONTRIBUTOR BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LICENSE OR YOUR USE OR INABILITY TO USE THE COVERED CODE, OR ANY PORTION THEREOF, WHETHER UNDER A THEORY OF CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCTS LIABILITY OR OTHERWISE, EVEN IF APPLE OR SUCH CONTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Apple's total liability to You for all damages (other than as may be required by applicable law) under this License exceed the amount of fifty dollars ($50.00).

10. Trademarks. This License does not grant any rights to use the trademarks or trade names "Apple", "Apple Computer", "Mac", "Mac OS", "QuickTime", "QuickTime Streaming Server" or any other trademarks, service marks, logos or trade names belonging to Apple (collectively "Apple Marks") or to any trademark, service mark, logo or trade name belonging to any Contributor. You agree not to use any Apple Marks in or as part of the name of products derived from the Original Code or to endorse or promote products derived from the Original Code other than as expressly permitted by and in strict compliance at all times with Apple's third party trademark usage guidelines which are posted at http://www.apple.com/legal/guidelinesfor3rdparties.html.

11. Ownership. Subject to the licenses granted under this License, each Contributor retains all rights, title and interest in and to any Modifications made by such Contributor. Apple retains all rights, title and interest in and to the Original Code and any Modifications made by or on behalf of Apple ("Apple Modifications"), and such Apple Modifications will not be automatically subject to this License. Apple may, at its sole discretion, choose to license such Apple Modifications under this License, or on different terms from those contained in this License or may choose not to license them at all.

12. Termination.

12.1 Termination. This License and the rights granted hereunder will terminate:

(a) automatically without notice from Apple if You fail to comply with any term(s) of this License and fail to cure such breach within 30 days of becoming aware of such breach;

(b) immediately in the event of the circumstances described in Section 13.5(b); or

(c) automatically without notice from Apple if You, at any time during the term of this License, commence an action for patent infringement against Apple; provided that Apple did not first commence an action for patent infringement against You in that instance.

12.2 Effect of Termination. Upon termination, You agree to immediately stop any further use, reproduction, modification, sublicensing and distribution of the Covered Code. All sublicenses to the Covered Code which have been properly granted prior to termination shall survive any termination of this License. Provisions which, by their nature, should remain in effect beyond the termination of this License shall survive, including but not limited to Sections 3, 5, 8, 9, 10, 11, 12.2 and 13. No party will be liable to any other for compensation, indemnity or damages of any sort solely as a result of terminating this License in accordance with its terms, and termination of this License will be without prejudice to any other right or remedy of any party.

13. Miscellaneous.

13.1 Government End Users. The Covered Code is a "commercial item" as defined in FAR 2.101. Government software and technical data rights in the Covered Code include only those rights customarily provided to the public as defined in this License. This customary commercial license in technical data and software is provided in accordance with FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for Department of Defense purchases, DFAR 252.227-7015 (Technical Data -- Commercial Items) and 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). Accordingly, all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

13.2 Relationship of Parties. This License will not be construed as creating an agency, partnership, joint venture or any other form of legal association between or among You, Apple or any Contributor, and You will not represent to the contrary, whether expressly, by implication, appearance or otherwise.

13.3 Independent Development. Nothing in this License will impair Apple's right to acquire, license, develop, have others develop for it, market and/or distribute technology or products that perform the same or similar functions as, or otherwise compete with, Modifications, Larger

Works, technology or products that You may develop, produce, market or distribute.

13.4 Waiver; Construction. Failure by Apple or any Contributor to enforce any provision of this License will not be deemed a waiver of future enforcement of that or any other provision. Any law or regulation which provides that the language of a contract shall be construed against the drafter will not apply to this License.

13.5 Severability. (a) If for any reason a court of competent jurisdiction finds any provision of this License, or portion thereof, to be unenforceable, that provision of the License will be enforced to the maximum extent permissible so as to effect the economic benefits and intent of the parties, and the remainder of this License will continue in full force and effect. (b) Notwithstanding the foregoing, if applicable law prohibits or restricts You from fully and/or specifically complying with Sections 2 and/or 3 or prevents the enforceability of either of those Sections, this License will immediately terminate and You must immediately discontinue any use of the Covered Code and destroy all copies of it that are in your possession or control.

13.6 Dispute Resolution. Any litigation or other dispute resolution between You and Apple relating to this License shall take place in the Northern District of California, and You and Apple hereby consent to the personal jurisdiction of, and venue in, the state and federal courts within that District with respect to this License. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded.

13.7 Entire Agreement; Governing Law. This License constitutes the entire agreement between the parties with respect to the subject matter hereof. This License shall be governed by the laws of the United States and the State of California, except that body of California law concerning conflicts of law.

Where You are located in the province of Quebec, Canada, the following clause applies: The parties hereby confirm that they have requested that this License and all related documents be drafted in English. Les parties ont exigé que le présent contrat et tous les documents connexes soient rédigés en anglais.

EXHIBIT A.

“Portions Copyright (c) 1999-2003 Apple Computer, Inc. All Rights Reserved.

This file contains Original Code and/or Modifications of Original Code as defined in and that are subject to the Apple Public Source License Version 2.0 (the ‘License’). You may not use this file except in compliance with the License. Please obtain a copy of the License at http://www.opensource.apple.com/apsl/ and read it before using this file.

The Original Code and all software distributed under the License are distributed on an ‘AS IS’ basis, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, AND APPLE HEREBY DISCLAIMS ALL SUCH WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT OR NON-INFRINGEMENT. Please see the License for the specific language governing rights and limitations under the License.”

Support for Unicode includes software copyright (c) 1995-2005 International Business Machines Corporation and others. All rights reserved.

http://www-306.ibm.com/software/globalization/icu/license.jsp

ICU License

The ICU project is licensed under the X License (see also the x.org original), which is compatible with GPL but non-copyleft.

The license allows ICU to be incorporated into a wide variety of software projects using the GPL license. The X license is compatible with the GPL, while also allowing ICU to be incorporated into non-open source products.

License

ICU License - ICU 1.8.1 and later COPYRIGHT AND PERMISSION NOTICE Copyright (c) 1995-2003 International Business Machines Corporation and others All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Some Zidget icons are licensed under the Creative Commons Attribution 2.5 License:

http://creativecommons.org/licenses/by-sa/2.5/legalcode

These icons are the original the work of:

http://www.famfamfam.com/lab/icons/silk/

http://www.jodriozola.com/blog/?p=10

ExtremeZ-IP®

INDEX

Index