



## **Acronis® Backup & Recovery for Mac®**

# Acronis Backup & Recovery® & Acronis ExtremeZ-IP®

This document describes the technical requirements and best practices for implementation of a disaster recovery solution for the Mac® using Acronis Backup & Recovery® and ExtremeZ-IP®.

## Table of contents

<b>1</b>	Executive summary .....	3
<b>1.1</b>	Introduction .....	3
<b>1.2</b>	Target environment .....	3
<b>1.3</b>	Known limitations .....	4
<b>2</b>	System requirements .....	4
<b>2.1</b>	Acronis software and licenses required .....	4
<b>2.2</b>	Recommended time machine server configuration .....	5
<b>2.3</b>	Recommended Acronis backup & recovery storage configuration .....	5
<b>2.4</b>	Mac Clients .....	5
<b>3</b>	Architectural Diagrams .....	6
<b>4</b>	Installation .....	7
<b>4.1</b>	Software download .....	7
<b>4.2</b>	ExtremeZ-IP .....	7
<b>4.3</b>	Acronis Backup & Recovery 11.5 .....	7
<b>4.4</b>	Mac Client (Time Machine) .....	8
<b>5</b>	Backup Configuration of Macs .....	9
<b>5.1</b>	ExtremeZ-IP configuration .....	9
<b>5.1.1</b>	Key configuration parameters .....	9
<b>5.1.2</b>	Configuration options .....	9
<b>5.1.3</b>	Set up a volume for Time Machine in ExtremeZ-IP .....	9
<b>5.1.4</b>	Using custom quotas .....	11
<b>5.2</b>	Time Machine client configuration .....	12
<b>5.3</b>	Acronis Backup & Recovery configuration .....	13
<b>6</b>	Recovery of Macs .....	14
<b>6.1</b>	Recover individual files by end user .....	14
<b>6.1.1</b>	Recovery of individual Mac archives .....	14
<b>6.1.2</b>	Recovery from production ExtremeZ-IP to Mac client - file level .....	14
<b>6.2</b>	Disaster recovery of the entire Time Machine server and data .....	15

# 1 - Executive Summary

## 1.1 - Introduction

This reference architecture provides a guide for using Acronis® products to integrate Apple® Mac® machines into a centralized backup and disaster recovery setup:

1. Backup of OS X® machines into a Windows® enterprise environment using Time Machine® and ExtremeZ-IP®.
2. Integration of Time Machine vaults into a complete disaster recovery solution via Acronis Backup & Recovery backing up the ExtremeZ-IP server, optionally using deduplication. Support for different storage targets like disk, SAN, or tape.
3. Storage of Time Machine backups in the cloud via Acronis Backup & Recovery Online Backup. Long-term archiving and retention based on corporate rules.

**Individual steps for setting up the backup:**

1. Install ExtremeZ-IP on a suitable Windows server.
2. Install the Acronis Backup & Recovery agent on the ExtremeZ-IP server.
3. Configure ExtremeZ-IP and set up the backup volumes.
4. Configure Acronis Backup & Recovery to back up the Time Machine volumes. This can be done locally on the ExtremeZ-IP machine for standalone operation or through the central management server as part of a corporate deployment.
5. Connect your Mac clients to the respective backup volume on the ExtremeZ-IP server.
6. Configure Time Machine to back up the Mac to the ExtremeZ-IP volume.

## 1.2 - Target environment

This reference architecture is suitable for deploying between one and 100 Mac workstations and laptops in IT environments utilizing Windows servers. Larger deployments may require multiple instances of ExtremeZ-IP. It is also possible to back up Mac servers through the configuration described in this reference architecture.

However, for an IT organization that primarily uses Windows Servers, the recommended solution here would be to directly use ExtremeZ-IP on Windows with its AD integration as the file-server component instead of a Mac server. Then to protect this ExtremeZ-IP server directly with Acronis Backup & Recovery like any other Windows server.

Existing users of Acronis Backup & Recovery will find this reference architecture especially useful, as it easily integrates with their existing setup.

### 1.3 - Known limitations

There is no simple and secure way to automatically configure Time Machine on a large number of machines from a central location. This means that for larger deployments, the configuration can be cumbersome. The approach described in this reference architecture only provides basic integration. It uses Time Machine to back up the Mac onto an ExtremeZ-IP server and, in turn, Acronis Backup & Recovery to protect the Time Machine files. As a result, there is no integrated catalog for the individual files in the Acronis tools and the solution will rely on a two-step process for recovery of versions that are not in the primary Time Machine backup. First, use Acronis Backup & Recovery on the ExtremeZ-IP server to restore the respective Time Machine files for the date requested, then use Time Machine to restore the data to the Mac. Full-system or bare-metal recovery requires that your network be set up to support Bonjour services, which is a multicast protocol typically designed to work in a single IP subnet. Wi-Fi networks are often assigned separate IP subnets and thus require additional configuration for Bonjour to work. You can configure your network routers and switches to support multicast or you can follow the instructions for setting up cross-subnet Bonjour at the following link: [http://www.grouplogic.com/Knowledge/PDFUpload/Info/WanBonjour\\_1.pdf](http://www.grouplogic.com/Knowledge/PDFUpload/Info/WanBonjour_1.pdf)

Performing a full system restore over a Wi-Fi connection can take a long time. We recommend that you use wired Ethernet connections when performing full system restores.

## 2 - System Requirements

### 2.1 - Acronis software and licenses required

**Minimum configuration for a small number of Mac systems and small amounts of data with direct backup from the ExtremeZ-IP server:**

1. At a minimum, a license for ExtremeZ-IP matching the number of clients is required to enable Time Machine backup to a central Windows server.
2. In order to add disaster recovery for the ExtremeZ-IP server stand-alone, a single license of Acronis Backup & Recovery Server for Windows is required.

**Recommended configuration for larger deployments (e.g. 10 or more Mac clients) or multi-site installations with one or more dedicated instances of Acronis Storage Node:**

1. An ExtremeZ-IP license for each Time Machine server host matching the number of clients that will be using the backup server.
2. Acronis Backup & Recovery Advanced Server for Windows license for each Time Machine server host. The minimum version of Acronis Backup & Recovery for this configuration is 11.5.
3. Deduplication license is required for each Acronis Storage Node that will use the deduplication feature.

For convenience, Acronis offers a bundle of the required licenses: Acronis Backup & Recovery Advanced Server Bundle for Mac Backup.

For cloud storage capability, an Acronis Backup & Recovery® Online subscription can be added in both scenarios.

Further information on how to buy Acronis products can be found at <http://www.Acronis.com/products/tryorbuy.html>.  
[Recommended System Environment](#)

### 2.2 - Recommended time machine server configuration

ExtremeZ-IP software must be installed on the Windows server that will hold Time Machine backups in order to enable Time Machine server functionality.

The Time Machine server will store Time Machine backups of Macs and it will be protected by Acronis Backup & Recovery software.

The recommended server CPU configuration is: 2x CPU 2.4 GHz, 4 cores or higher per 100 clients.

It is recommended to have a separate partition on RAID dedicated to Time Machine backups. The recommended size of the partition is 2x the size of the data that is going to be backed up.

Windows Server 2008 R2 or later operating system, with Active Directory® enabled and configured.

The recommended configuration corresponds to the recommended configuration for the Acronis Backup & Recovery Agent for Windows. Please see Acronis Backup & Recovery 11.5 documentation for further details at <http://www.Acronis.com/download/docs/abr11.5a/installguide>.

### 2.3 - Recommended Acronis backup & recovery storage configuration

Time Machine server can be backed up with Acronis Backup & Recovery for disaster recovery purposes. Any storage supported by Acronis Backup & Recovery can be used to store the backups of the Time Machine server.

This includes directly attached storage, tape drive, the cloud via Acronis Backup & Recovery Online (requires subscription), Acronis Storage Node with deduplication in the case that Acronis Backup & Recovery Advanced Server used.

For larger deployments using the Acronis Storage Node, it is recommended to run it on a separate machine of similar size as the above server. When using de-duplication, the following minimum configuration is recommended: SSD - 100 GB for Database of Hash Table, 20 GB RAM.

The Acronis Storage Node can also be used to stage local backups to the cloud and enable a hybrid backup configuration combining the advantages of both local and cloud backup.

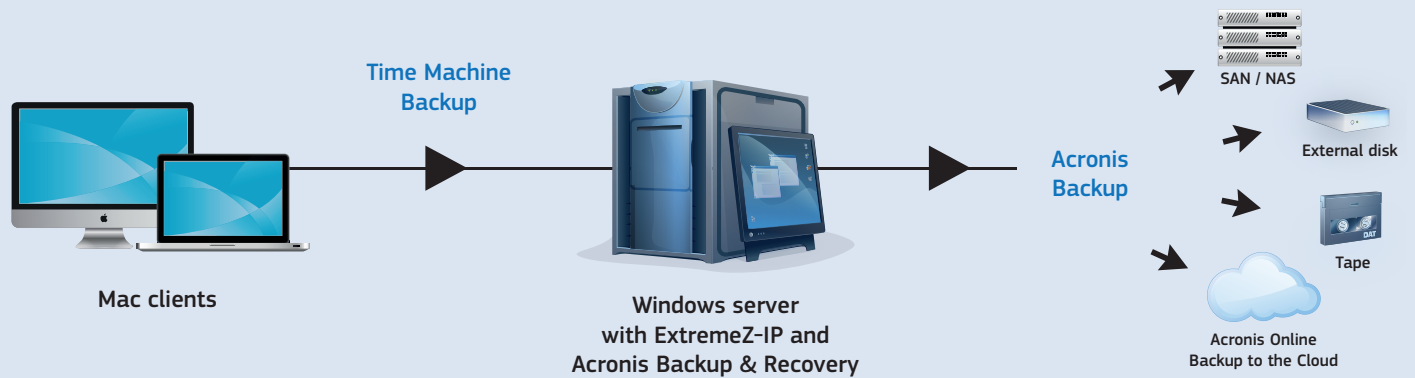
Please see deduplication best practices for more information: <http://www.acronis.com/support/documentation/ABR11.5/#14080.html>

### 2.4 - Mac clients

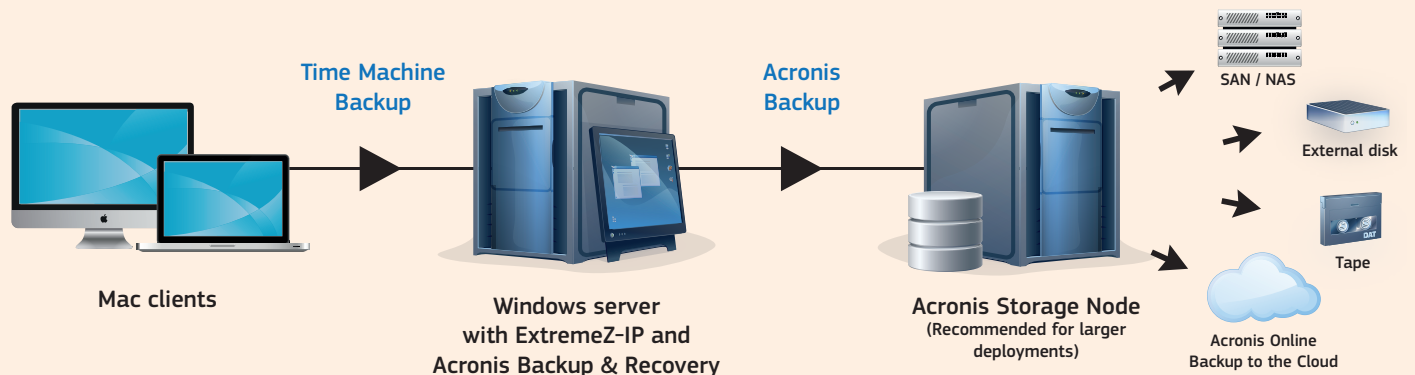
Mac OS X 10.4 (Tiger) or later clients are supported.

### 3 - Architectural Diagrams

#### Acronis Backup & Recovery for Mac minimum configuration:



#### Acronis Backup & Recovery for Mac recommended configuration for larger deployments:



## 4 - Installation

### 4.1 - Software download

ExtremeZ-IP software download at <http://www.Acronis.com/enterprise/products/extremez-ip/>.

Acronis Backup & Recovery software download at <http://www.Acronis.com/backup-recovery/>.

### 4.2 - ExtremeZ- IP

Follow these steps to install ExtremeZ-IP:

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

For further details, please see the Installation Quick Start PDF for step-by-step instructions:

<http://www.grouplogic.com/files/ez/EZIPQuickStartGuide.pdf>.

The full user manual can be found at <http://www.grouplogic.com/files/ez/EZIPManual.pdf>.

### 4.3 - Acronis Backup & Recovery 11.5

Acronis Backup & Recovery 11.5 needs to be installed on the backup server. Acronis Backup & Recovery Management Console can be installed on any Windows (or Linux) machine in the same network.

Below is the step-by-step description of typical interactive installation. For other options or for additional details please see Acronis Backup & Recovery Installation Guide: <http://www.Acronis.com/download/docs/abr11.5a/installguide>.

1. Log on as an administrator and start the Acronis Backup & Recovery setup program.
2. Click Install Acronis Backup & Recovery 11.5.
3. Accept the terms of the license agreement.
4. Select one or more machine roles, depending on what you want this machine to do:
  - To install the Acronis Backup & Recovery agent please select Back up this machine's data role.
  - To install the Acronis Backup & Recovery Management Console please select Connect to remote machines or centrally monitor and configure the backing up of physical and virtual machines role.

5. When installing the Acronis Backup & Recovery agent you will be prompted to specify license:
  - a. If you want to back up the machine to Acronis online backup storage only, click Next and then click Yes in the confirmation window. Otherwise, skip this step.
  - b. Choose whether to take licenses from a license server or to store them locally on the machine. To take licenses from a license server, click Specify and then specify the name or IP address of the license server.
  - c. To store the machine's licenses on the machine itself, make sure that the license server is not selected.
6. When installing the Acronis Backup & Recovery agent you will be prompted to register it on the management server:
  - a. If you have an Acronis Backup & Recovery Management Server installed, specify the name or IP address of the machine with the management server. Specify the user name and password of a user who is a member of the Acronis Centralized Admins group on the management server's machine.
  - b. To skip registration click I will register the machine later.
7. Choose whether the machine will participate in the Acronis Customer Experience Program (CEP).
8. On the summary page, review the list of components that will be installed, and the installation settings for those components. Click Install to start the installation.

Acronis Storage Node (ASN) can be installed on the same machine as ExtremeZ-IP or on a different server to enable deduplication. For larger deployments, it is strongly recommended to use a dedicated server and the Acronis Management Server (AMS).

Please see the Acronis Backup & Recovery documentation: <http://www.Acronis.com/download/docs/abr11.5a/installguide>.

### **4.4 - Mac client (Time Machine)**

Time Machine is present on Mac OS 10.4 (Tiger) and later by default and doesn't require separate installation.

You can enable and configure Time Machine from the Mac OS System Preferences.

## 5 - Backup Configuration of Macs

### 5.1 - ExtremeZ-IP configuration

#### 5.1.1 - Key configuration parameters

- The recommended size of the storage for backup is 2x the amount of data to back up.
- We recommend that you keep at least 30 days of Time Machine backups.
- We recommend that you have separate disk/volume allocated only to Time Machine backups.
- There is no need to share individual volume/folder in ExtremeZ-IP for each Mac; you can have one volume/folder shared for all/group of Macs.
- We recommend using AD authentication for security of backups.
- We recommend that you use user quotas on ExtremeZ-IP server.
- Time Machine can be configured for full bare-metal recover or as a simple self-service file-level backup and recovery tool.

#### 5.1.2 - Configuration options

##### Configuring a single time machine volume for all users (recommended)

Using a single Time Machine volume for all users will simplify the configuration and maintenance of your deployment. In this configuration you only need to create a single Time Machine volume in the ExtremeZ-IP Administrator. Each Time Machine backup is automatically secured using the Windows NTFS permissions for that Active Directory user. This is a recommended option.

\* One consideration with using a single volume for all users is that Apple's System Restore Utility will place a file lock on every user's backup during the time it takes to do a full system recovery. This will prevent backups and restores for users while the Apple System Restore Utility is running.

##### Configuring a time machine volume for each user.

Some configurations may require that you create a unique volume for each Time Machine user or computer. The primary benefit of this configuration is to work around the limitation in Apple's System Restore Utility described above.

#### 5.1.3 - Set up a volume for time machine in ExtremeZ-IP

Please refer to the instructions in the ExtremeZ-IP Manual or Quick Start Guide for creating a volume:

<http://www.grouplogic.com/files/ez/EZIPQuickStartGuide.pdf>

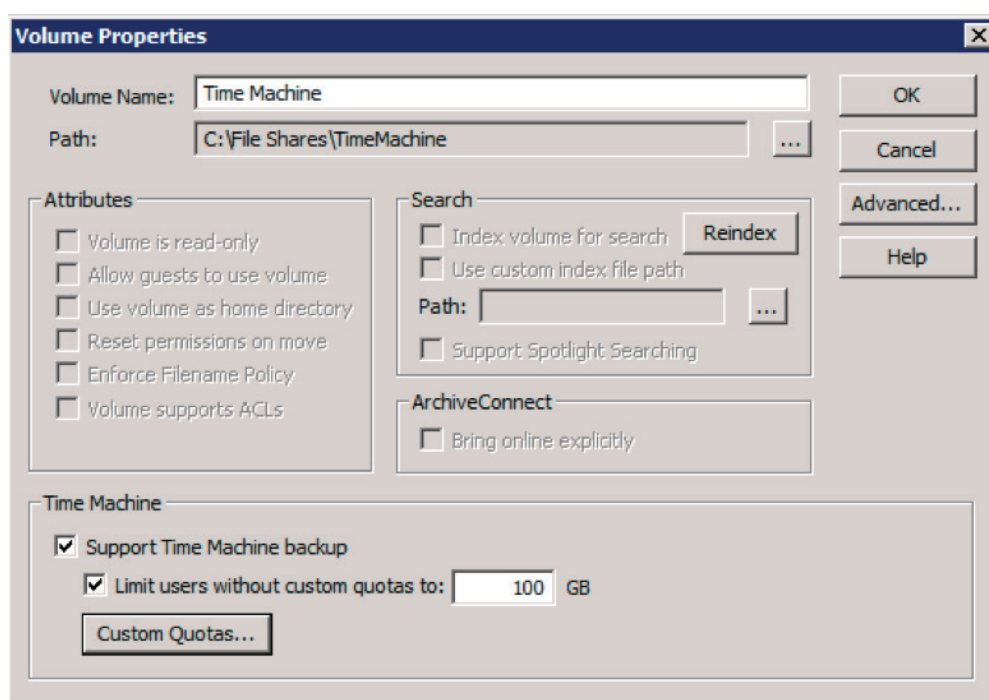
<http://www.grouplogic.com/files/ez/EZIPManual.pdf>

It is recommended that you store your Time Machine data on a separate volume from your operating system or other storage.

After you have created the ExtremeZ-IP volume that will be used for Time Machine backups, you will change the volume settings to support Time Machine.

In the ExtremeZ-IP volume properties, when you check the Allow Time Machine Backup box, Mac 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. When you select a Time Machine destination volume on a Mac, Time Machine will create a disk image for the backup. By default, the Support Time Machine backup setting is disabled for ExtremeZ-IP 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 the “Volume is read-only” option and uses the volume as home directory.



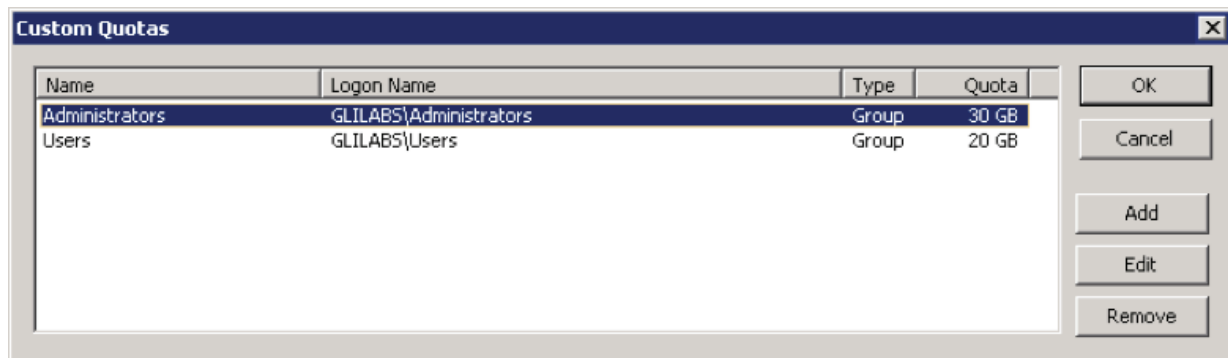
Limit users without custom quotas to x GB Check this box and enter a value to limit the size of Time Machine backups per user. When the Mac client connects to the server for the first time it sees the available space on the drive as whatever the quota was set to. On subsequent logins it will see the 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 Mac client 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.

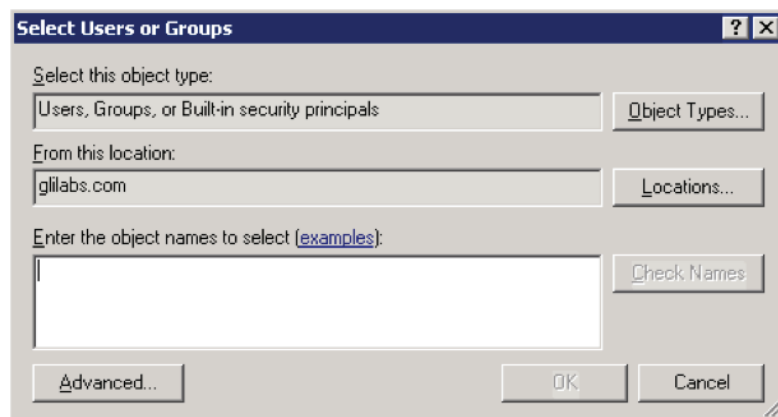
### 5.1.4 - Using custom quotas

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.

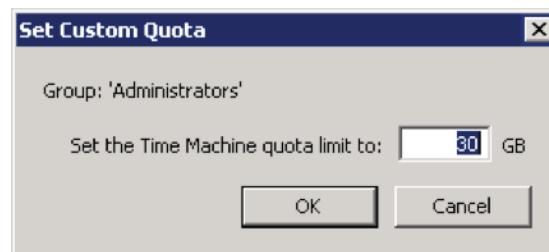
1. Click the Custom Quotas button on the Volume Properties dialog box to open the Custom Quotas window.



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 want to set them all to the same quota value.



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



### 5.2 - Time Machine client configuration

This reference architecture supports the standard Time Machine defaults.

To configure Time Machine backup point Time Machine to the ExtremeZ-IP server on each Mac you want to protect:

1. From the Apple menu, choose System Preferences.
2. Click Time Machine.
3. Set Time Machine to On (if it is Off).
4. Choose your ExtremeZ-IP volume as the backup destination. (If you do not automatically see your ExtremeZ-IP Volume you may first need to mount the drive in the Mac OS Finder. Time Machine can use the “Bonjour” auto-discovery protocol to locate resources. Bonjour typically works on a single subnet. If you would like to configure Time Machine to use Bonjour on your network and have multiple subnets, please refer to the support documentation for configuring multi-subnet Bonjour: [http://www.grouplogic.com/Knowledge/PDFUpload/Info/WanBonjour\\_1.pdf](http://www.grouplogic.com/Knowledge/PDFUpload/Info/WanBonjour_1.pdf).)
5. In the alert window that appears, enter your Active Directory username and password.
6. Click Connect.

Time Machine will start your initial backup after a countdown timer. You should let the backup process finish without interruption.

**We recommend using exclusion lists to reduce the size of the backup:**

- Exclude System and Applications directories
- Exclude items that don't often change

If encrypted Time Machine backups are used, the deduplication will not be very efficient. This does not apply if Acronis encryption is used on the backend.

**Here are some links from Apple on how to set up Time Machine:**

<http://support.apple.com/kb/HT1175>

<http://support.apple.com/kb/HT1427>

### 5.3 - Acronis Backup & Recovery configuration

Acronis Backup & Recovery is configured through the management console application. If Acronis Backup & Recovery is used standalone to back up the ExtremeZ-IP server, the console can be installed on the same machine and pointed to the local host.

In larger deployments, it should be started on the administrator's workstation and connected to the Acronis Management Server.

It is recommended to have a disk-level backup task to back up the entire volume where ExtremeZ-IP stores all Time Machine backups.

#### Steps-by-step guide in Acronis Backup & Recovery User Interface:

1. Navigate to "Backup plans and tasks"
2. New "Backup plan"
3. "Items to back up": choose the disk-level backup of the volume with ExtremeZ-IP Time Machine share
4. "Where to back up": any destination supported by Acronis Backup & Recovery 11.5
5. "How to back up": GFS
6. "Plan parameters": leave default

#### General recommendations:

1. It is not recommended to back up more than once per day, because Time Machine removes hourly slices after 24 hours.
2. There is no need to always conduct full backups; instead it is recommended to use incremental/differentials regularly. Full backups take a lot of space.
3. It is recommended to use image-level backup instead of file-level. File-level backup incrementals can take twice as much space on average as image-level incrementals because of the block size.
4. Deduplication is quite efficient and can be used with disk-level backups.
5. You can create a custom backup scheme instead of GFS. In this case consider having monthly full and weekly (or daily) incrementals. You can find the details on custom schemes in Acronis Backup & Recovery documentation. <http://www.acronis.com/support/documentation/ABR11.5/#776.html>
6. It is also recommended that you back up ExtremeZ-IP server setup for disaster recovery.

The full documentation for Acronis Backup & Recovery can be found here: <http://www.Acronis.com/support/documentation/>.

## 6 - Recovery of Macs

### 6.1 - Recover individual files by end user

If you need to recover individual files from Time Machine backups, the first thing to do is to check if the files are still present in the backups. You need to open the Time Machine browser and locate the files.

#### 6.1.1 - Recovery of individual mac's archives

If Time Machine has already deleted user files from the server, the administrator can recover the user backups from Acronis Backup & Recovery backups.

This scenario is potentially dangerous because you risk overwriting backups from other Mac's Time Machine archive.

##### Steps:

1. In ExtremeZ-IP suspend file sharing on the Time Machine share in order to avoid data corruption
2. Select data: Browse the vault <screen>
3. Choose archive <screen>
4. Choose recover <screen>
5. Select data -> select the required folder; if you recover backup of individual Mac you only need to recover its Time Machine folder <screen>
6. Destination: original (to recover to the shared folder)
7. Overwriting: overwrite the existing files must be enabled
8. Start recovery task <screen>
9. Go to Mac
10. Select slice and recover the needed files from Time Machine.

#### 6.1.2 - Recovery from production ExtremeZ-IP to Mac client - file level

If you need to recover Mac files from a backup that is present on the Time Machine server, please use regular Time Machine recovery. Refer to Time Machine manual. <http://www.grouplogic.com/files/ez/EZIPManual.pdf>.

## 6.2 - Disaster recovery of the entire time machine server and data

In the recommended configuration, Acronis Backup & Recovery also protects the whole ExtremeZ-IP file server used for Time Machine backups. In case of failure of the machine, you can recover it using the Acronis Backup & Recovery bare-metal recovery features. This includes recovery to dissimilar hardware. Please refer to the Acronis Backup & Recovery documentation for details on how to use the bare-metal recovery feature.

You can also just recover the data on a different machine. If you recover to a machine with a different network configuration please don't forget to point to a new server in Time Machine settings on the client Macs.

## Summary

Although the use of Apple products in the enterprise presents many benefits, including total lifecycle cost savings and more satisfied and productive employees, the hurdle of integrating Macs into existing Windows-based server environments poses many challenges for IT organizations. ExtremeZ-IP addresses these problem by enabling the simple and rapid support and integration of the Mac into Windows server environments.

Among its many capabilities, ExtremeZ-IP provides Mac users with the ability to safely and securely utilize the built-in Time Machine backup feature of the Mac OS to perform backups directly to a Windows server. These network-based backups can be accessed by the user at any time to perform self-service restoration of anything from a single file to the entire contents of their Mac.

Acronis Backup and Recovery allows an ExtremeZ-IP server's network Time Machine client backups to be included in a standard enterprise backup routine, providing disaster recovery for the Windows server and Time Machine backup content. Together, Acronis Backup and Recovery and ExtremeZ-IP provide an end-to-end solution for protecting Mac users from data loss.



For additional information please visit <http://www.acronis.com>

To purchase Acronis products, visit [www.acronis.com](http://www.acronis.com) or search online for an authorized reseller.

Acronis office details can be found at <http://www.acronis.com/company/worldwide.html>

Copyright © 2002-2013 Acronis, Inc. All rights reserved. "Acronis", "Backup & Recovery" and the Acronis logo are trademarks of Acronis, Inc. "ExtremeZ-IP" is a registered trademark of GroupLogic. Windows is a registered trademark of Microsoft Corporation. Other mentioned names may be trademarks or registered trademarks of their respective owners and should be regarded as such. Technical changes and differences from the illustrations are reserved; errors are excepted. 2013-02

