

Group Logic White Paper | August 2008

Active Directory Compatibility with ExtremeZ-IP

A Technical Best Practices White Paper



About This Document

The purpose of this technical paper is to discuss how ExtremeZ-IP™ supports Microsoft® Active Directory. It is intended for systems administrators, technical evaluators and decision-makers who are considering upgrading or purchasing ExtremeZ-IP for the first time.

Active Directory Compatibility in ExtremeZ-IP

ExtremeZ-IP – An Overview

ExtremeZ-IP is a robust Windows-based file and print server supporting all releases of the Mac operating system from Mac OS 9 to Mac OS X 10.5 (Leopard). ExtremeZ-IP allows your organization to preserve the innovative “Mac experience” for your end users, while simultaneously integrating them fully into your Windows Server infrastructure. Whether it’s security policies, Active Directory integration, performance, scalability or manageability and monitoring options, ExtremeZ-IP allows you to deliver the enterprise-class services that your Mac users require. As a software service that runs on Windows, if your Windows server is bound to the domain, ExtremeZ-IP seamlessly integrates your Macs into Active Directory.

ExtremeZ-IP is the only fully-supported, server-side solution for delivering seamless Mac to Windows connectivity. ExtremeZ-IP allows your Windows Administrators to treat Macs on the network like PCs, while allowing your Mac users to continue operating in their native environment while also participating fully in your existing file server and storage infrastructure. The result is better scalability, service delivery, performance, and compliance and fewer calls to your help desk.

As the proven standard for file sharing between Mac desktops and Windows servers, ExtremeZ-IP is the most trusted solution for ensuring compatibility without compromise and a “must have” for mixed Mac and Windows computing environments.

User Authentication and ExtremeZ-IP

ExtremeZ-IP leverages the Active Directory plug-in built into every Mac OS X client to provide Single Sign-on (SSO) authentication using Kerberos in the same way that normal Windows clients behave.

Connecting to ExtremeZ-IP

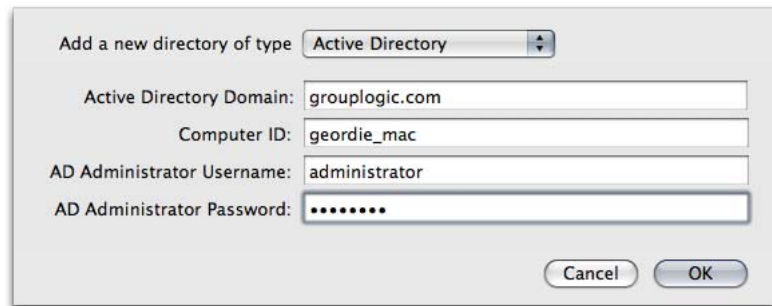
ExtremeZ-IP fully supports Active Directory and provides two authentication options - Diffie-Hellman Key Exchange (DHX) for Mac OS 9 and Mac OS X and Kerberos Single Sign-on for Mac OS X. Kerberos is the standard authentication for Active Directory.

With Active Directory and Extreme-IP, the Mac user can log into a Mac, and get a Kerberos ticket, that then permits them secure, controlled access to all resources in the domain. Diffie-Hellman Key Exchange (DHX) provides single server authentication which permits secure, controlled access to all resources on that server.

Which option is used for logins depends upon how the Mac is configured and how the user logged into the Mac.

Option 1:

If the Mac is bound to the domain via the Active Directory plug-in, how Kerberos operates depends on the type of account used to log into the Mac:



Connecting a Mac to Active Directory

- a. If the user logs into Mac with an Active Directory account, a ticket is retrieved at login time from Active Directory and is accepted seamlessly by all ExtremeZ-IP servers
- b. Or, if the user logs into Mac with a local account, the user is prompted for their login credentials the first time they access an ExtremeZ-IP share, and the ticket they retrieve is then used to seamlessly access all other ExtremeZ-IP servers



File server login

Option 2:

If the Mac is not bound to the domain, the Mac logs in using the encrypted DHX protocol built into the AFP protocol.

Password Policies

ExtremeZ-IP honors all password policies - expiration, complexity rules on client change, and rules for changing passwords. Therefore, password policies are consistent among all platform clients. In addition, ExtremeZ-IP can warn the user a configurable number of days before his or her password is going to expire.

Disk Quotas

ExtremeZ-IP enforces a user's disk quotas by controlling the amount of disk space reported available to the Mac client and enforcing disk space limitations in file I/O operations.

Permissions and ExtremeZ-IP

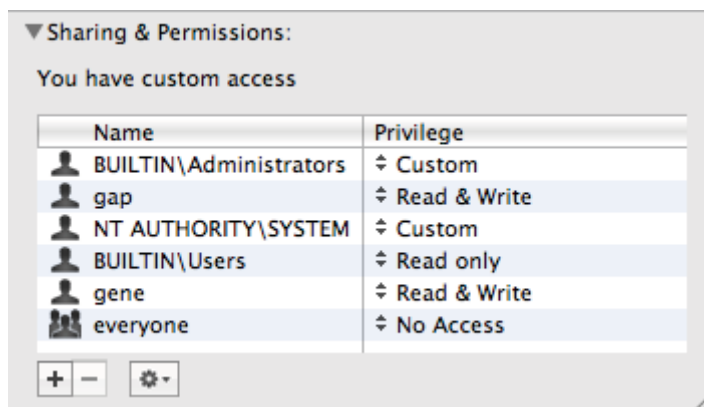
Mac and UNIX permissions are traditionally more narrow than Active Directory permissions. Common permissions are owner, group, everyone, read, write, and execute. Active Directory provides many more possibilities for permission groups. Using ExtremeZ-IP, users can take advantage of these possibilities.

ExtremeZ-IP strictly honors the Active Directory file permissions for a user and maps those permissions to the "effective" permission the Mac will understand. This is accomplished without any client software or special tools to manipulate permissions on the server.

Support for Mac ACLs

For Mac computers that are bound to the Active Directory domain, ExtremeZ-IP maps the Windows permissions to the Mac OS X permissions model for Access Control Lists (ACLs). This allows Macs to see the permissions on specific files or folders, and manipulate them if they have rights to do so.

Mac OS X 10.5 ("Leopard") provides a user interface directly in the Finder for manipulating these permissions.



Adjusting permissions in the Finder

Support for UNIX Permissions

ExtremeZ-IP can be configured to properly report and allow manipulating of UNIX permissions to the Mac client. This is important for Mac applications that expect the proper representation of UNIX permissions, especially lower level utilities and general UNIX software.

ExtremeZ-IP supports UNIX permissions relating to the owner, group and everyone group. ExtremeZ-IP represents UNIX permissions on the Windows file system by a combination of effective Windows ACLs as well as additional, more explicit Access Control Entries (ACEs) that are added to the ACLs for the UNIX permissions. In every case, the Windows ACLs take precedence over all UNIX permissions so the underlying Windows permissions model is always honored while providing a more compatible environment for Mac applications.

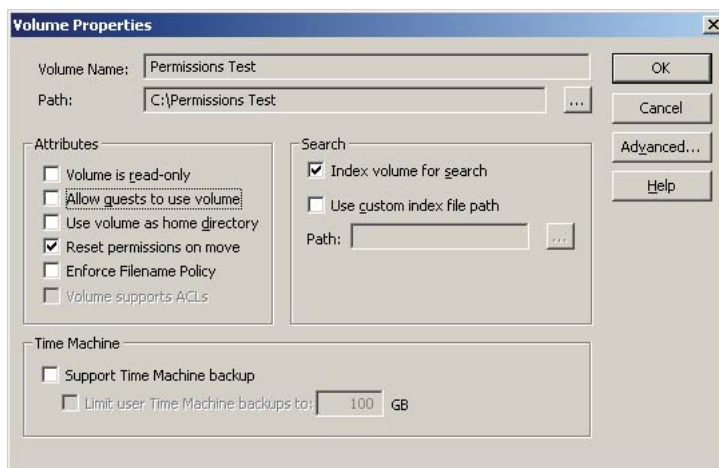
More information on how ACLs and UNIX permissions are handled in ExtremeZ-IP can be found in this knowledge base article:

<http://www.grouplogic.com/knowledge/index.cfm/fuseaction/view/docID/10>

Flexible Permissions

ExtremeZ-IP provides a per-volume option to enable “flexible permissions”. Flexible permissions are useful for collaboration workflows where one user who creates files in a folder with restrictive permissions needs to share those files with other users. Normally when files are moved from a more restrictive to a less restrictive folder, the permissions remain restrictive. This can create user frustration and help desk calls because users cannot access the files even though they were moved to a more public part of the file server.

When flexible permissions are enabled on a volume, ExtremeZ-IP resets the permissions when files are moved so that the permissions of the destination are applied to all files being moved. This eliminates the need for end users or administrators to manually change the permissions. The configuration setting to enable flexible permissions in the image shown below is called “Reset permissions on move”.



Shared volume settings showing flexible permissions

Home Directories and ExtremeZ-IP

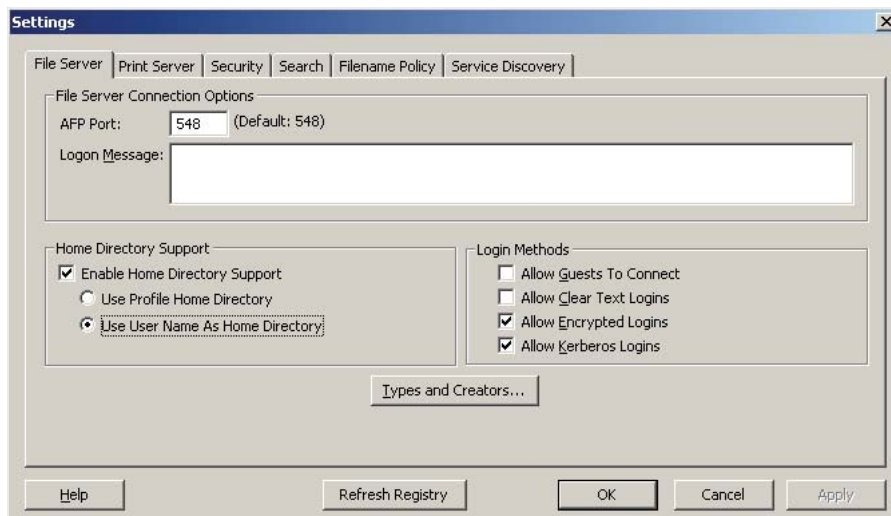
Special challenges exist when Macs are configured to use network-based home directories. When the user tries to access a home directory on a server hosting a large number of users, the Mac lists all of the folders on the server and looks in every folder for special preview metadata. This process can require a considerable amount of time and the user has to go through the entire list to find his or her folder.

ExtremeZ-IP includes two optimizations called Access Based Enumerations (ABE) that mitigate this problem. The first optimization uses the user's profile and lists only folders in that profile. In the second optimization, for users that do not want to use Active Directory, the Mac equates the user name with the home directory and, when the user logs on, displays only the folder that matches his or her user name.

Mac users with a home directory profile in Active Directory can seamlessly connect to ExtremeZ-IP for both network and portable home directories. ExtremeZ-IP has features that optimize the performance and minimize server load when acting as a home directory server. Additionally, ExtremeZ-IP caching algorithms are designed based on how the Mac operates and provide additional performance and server load optimization benefits.

Mac clients can be configured using their built-in Active Directory plug-in to be bound to domain and to retrieve home directory locations from the user profile in Active Directory at login time.

ExtremeZ-IP can optionally be configured so that individual volumes that host home directories have special filtering applied so that only a user's home directory is visible during file system operations:



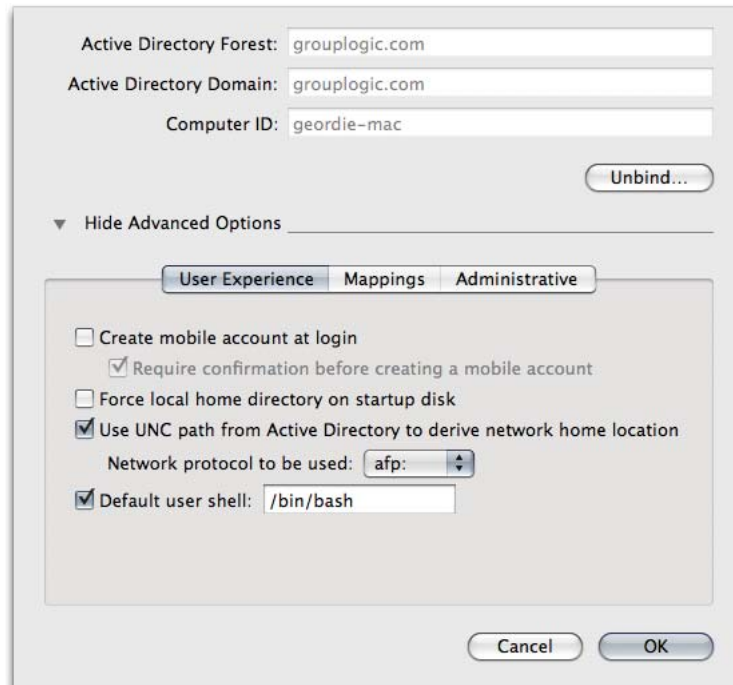
File server settings showing home directory options

This minimizes the client access time during logons and reduces the server load when there are many home directories hosted on a server.



View of home directories when using Access Based Enumerations

This home directory filter can be based on either the user’s name or their Active Directory profile.



Active Directory plug-in home directory configuration

For more sophisticated control over client authentication and group policy, ExtremeZ-IP is also compatible with the DirectControl™ product from Centrify. ExtremeZ-IP and DirectControl complement each other by providing best of breed Mac file sharing with Mac authentication and group policy, respectively.

For instructions on how to configure ExtremeZ-IP to work with home directories, please review the following knowledge base article:
<http://www.grouplogic.com/knowledge/index.cfm/fuseaction/view/docID/167>.

For instructions on how to integrate ExtremeZ-IP with Centrify DirectControl see this knowledge base article:

<http://www.grouplogic.com/knowledge/index.cfm/fuseaction/view/docID/288>

DFS and ExtremeZ-IP

Microsoft Distributed File System (DFS) is a powerful set of technologies used to present a single virtual interface to a collection of Windows file servers and manage replication of data between those servers. Microsoft DFS consists of two technologies:

DFS Replication: which provides facilities for replicating file server data between locations and servers.

DFS Namespaces: which allows administrators to group file server shares on disparate machines into a single virtual name space so end users can access files without needing to know exactly where the files are located.

There are many benefits that come with using DFS such as:

- Providing replication and failover in the case of server failure
- Distributing data geographically so that users get better performance by working with local copies
- Giving administrators the flexibility to reconfigure their file server infrastructure without retraining users, and
- Providing end users with a single view into the file sharing space.

ExtremeZ-IP seamlessly supports DFS replication. Mac-specific file information is stored as alternative data streams in the NTFS file system, and this information is replicated by DFS so that Mac information is preserved.

To support DFS namespaces, ExtremeZ-IP can be configured to present the DFS namespace to Mac users by leveraging native Mac aliases in a special "DFS Root" volume created on the ExtremeZ-IP server. This allows Macs to see a representation of the DFS structure and be redirected to the appropriate target server. When used in conjunction with Active Directory single sign-on support the user will seamlessly mount the target volume. For many workflows this setup is sufficient for providing equivalent DFS support to Mac clients. Documentation of this method can be found in this knowledge base article:

<http://www.grouplogic.com/knowledge/index.cfm/fuseaction/view/docID/288>.

The next version of ExtremeZ-IP, due out in Q4 2008 will support full dynamic presentation and navigation of the DFS namespace to Mac OS X 10.5 clients, while preserving the benefits of true Mac compatibility with the AFP protocol. For more information on this upcoming feature please contact Group Logic.

Conclusion

ExtremeZ-IP is the most effective and reliable method for sharing files between Macs and Windows servers. ExtremeZ-IP supports the network protocol specifically designed for the Mac and maintains the performance and security levels that Windows administrators expect.

ExtremeZ-IP also resolves the sharing problems of file structure, naming conventions, and server performance and provides added benefits that include sophisticated authentication, file name policies, and caching. ExtremeZ-IP works easily with clusters and facilitates use of network home directories.

Most importantly, Group Logic maintains, updates, and supports ExtremeZ-IP so that Mac users can take advantage of all the Macintosh features and enjoy the enterprise level convenience and benefits of sharing files on Windows servers.