

This document has been archived and will no longer be maintained or updated. For more information go to the Storage Solutions Technical Documents page on Dell TechCenter or contact support.

## Using Windows Active Directory for Account Authentication to PS Series Groups

#### ABSTRACT

This document details how administrators can control login authentication to a Dell EqualLogic™ PS Series Group using Windows domain user accounts and RADIUS clients.



TR1035 V2.1 Copyright © 2010 Dell Inc. All Rights Reserved.

Dell EqualLogic is a trademark of Dell Inc.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Possession, use, or copying of the documentation or the software described in this publication is authorized only under the license agreement specified herein.

Dell, Inc. will not be held liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change.

November 2010

WWW.DELL.COM/PSseries



- **PS Series Arrays**
- Setup Poster
- Installation & Setup
- Hardware Maintenance

#### PREFACE

Thank you for your interest in Dell EqualLogic™ PS Series storage products. We hope you will find the PS Series products intuitive and simple to configure and manage.

PS Series arrays optimize resources by automating volume and network load balancing. Additionally, PS Series arrays offer all-inclusive array management software, host software, and free firmware updates. The following value-add features and products integrate with PS Series arrays and are available at no additional cost:

Note: The highlighted text denotes the focus of this document.

#### PS Series Array Software

- **Firmware** Installed on each array, this software allows you to manage your storage environment and provides capabilities such as volume snapshots, clones, and replicas to ensure data hosted on the arrays can be protected in the event of an error or disaster.
  - **Group Manager GUI:** Provides a graphical user interface for managing your array
  - **Group Manager CLI:** Provides a command line interface for managing your array.
- Manual Transfer Utility (MTU): Runs on Windows and Linux host systems and enables secure transfer of large amounts of data to a replication partner site when configuring disaster tolerance. You use portable media to eliminate network congestion, minimize downtime, and quick-start replication.
- Host Software for Windows
  - Host Integration Tools
    - Remote Setup Wizard (RSW): Initializes new PS Series arrays, configures host connections to PS Series SANs, and configures and manages multipathing.
    - Multipath I/O Device Specific Module (MPIO DSM): Includes a connection awareness-module that understands PS Series network load balancing and facilitates host connections to PS Series volumes.
    - VSS and VDS Provider Services: Allows 3<sup>rd</sup> party backup software vendors to perform off-host backups.
    - Auto-Snapshot Manager/Microsoft Edition (ASM/ME): Provides point-in-time SAN protection of critical application data using PS Series snapshots, clones, and replicas of supported applications such as SQL Server, Exchange Server, Hyper-V, and NTFS file shares.
  - **SAN HeadQuarters (SANHQ):** Provides centralized monitoring, historical performance trending, and event reporting for multiple PS Series groups.
- Host Software for VMware
  - **Storage Adapter for Site Recovery Manager (SRM):** Allows SRM to understand and recognize PS Series replication for full SRM integration.
  - Auto-Snapshot Manager/VMware Edition (ASM/VE): Integrates with VMware Virtual Center and PS Series snapshots to allow administrators to enable Smart Copy protection of Virtual Center folders, datastores, and virtual machines.
  - o MPIO Plug-In for VMware ESX: Provides enhancements to existing VMware multipathing functionality.

Current Customers Please Note: You may not be running the latest versions of the tools and software listed above. If you are under valid warranty or support agreements for your PS Series array, you are entitled to obtain the latest updates and new releases as they become available.

To learn more about any of these products, contact your local sales representative or visit the Dell EqualLogic™ site at <u>http://www.equallogic.com</u>. To set up a Dell EqualLogic support account to download the latest available PS Series firmware and software kits visit: <u>https://www.equallogic.com/secure/login.aspx?ReturnUrl=%2fsupport%2fDefault.aspx</u>

### TABLE OF CONTENTS

Revision Information	iii
Introduction	1
Prerequisites	1
Steps Covered in This Document	1
Prepare the Server and PS Group for RADIUS Authentication	2
Configuring a PS Series Group as a RADIUS Client on the NPS Server	2
Configuring the PS Series Group for RADIUS Login Attempts	3
Managing SAN Administration Thorugh Vendor Specific Attributes	5
Creating Users and Groups for SAN Administration	5
Creating Network Policies on the NPS Server	7
Adding the PS Series Vendor-Specific Attributes	13
Creating Additional Network Policies using Optional VSA's	16
Configuring RADIUS for iSCSI Authentication to PS Series Groups	20
Configuring the Windows Server 2008 NPS	21
Configuring the Windows Server 2003 IAS	22
Connecting to Volumes	23
Appendix A – Configuration Steps on Windows Server 2003	26
Configuring a PS Series Group as a RADIUS Client on the IAS Server	26
Creating Remote Access Policies on the IAS Server	27
Adding the EqualLogic Vendor-Specific Attributes	34
Appendix B: Configuring RADIUS on the PS Series Group Using CLI	39
Technical Support and Customer Service	40

#### **REVISION INFORMATION**

The following table describes the release history of this Technical Report.

Report	Date	Document Revision
1.0	January 2008	Initial Release
2.0	May 2010	Added steps for Windows 2008 NPS and PS Series array firmware enhancements in version 5.0.0
2.1	October 2010	Added steps for CHAP authentication through RADIUS

The following table shows the software and firmware used for the preparation of this Technical Report.

Vendor	Model	Software Revision
Dell®	EqualLogic PS Series Array Firmware	V5.x
Dell®	EqualLogic Host Integration Tools for Windows	V3.4
Microsoft®	Windows Server 2008	2008, 2008 SP2, 2008 R2

The following table lists the documents referred to in this Technical Report. All PS Series Technical Reports are available on the Customer Support site at: *support.dell.com* 

Vendor	Document Title
Dell®	EqualLogic PS Series Group Administration Users Guide

### INTRODUCTION

Enterprises of all sizes consolidate user management and authentication into services such as Active Directory. It is common in these environments to want to control administrator accounts in the PS Series SAN from Active Directory. PS Series arrays allow the authentication of administrator (and iSCSI) accounts with AD, by using Windows Server 2003 Internet Authentication Service (IAS) or Windows Server 2008 Network Policy Service (NPS) as a connector between the PS Series SAN and Active Directory.

This paper describes the setup and configuration of RADIUS clients to authenticate to PS Series groups. Using RADIUS allows Active Directory and the PS Series group to administer accounts for SAN management. This configuration can improve security and centralize administrator privileges throughout the PS Series SAN.

This Technical Report describes the steps to configure NPS on Windows Server 2008 (and IAS on Windows 2003 – <u>Appendix A</u>) by creating Network Policies that grant full, partial, and read-only administrative privilege to the PS Series group.

#### Prerequisites

In order to setup and configure remote authentication to a PS Series group using RADUIS clients the following are required:

- A domain controller with network access to the PS Series group.
- Familiarity with Active Directory user and group account management.
- Understanding of PS Series group management.

#### Steps Covered in This Document

- 1. Prepare the server and PS Group for RADIUS authentication
  - Install and configure NPS on Windows Server 2008.
  - Configure the PS Series group as a RADIUS client.
  - Configure the PS Series group to recognize and accept login attempts from the RADIUS server.
- 2. Choose and configure access authentication to the EqualLogic SAN
  - Optionally Use Vendor Specific Attributes to control access to the PS Series Group
    - Create a new group in Active Directory and add select users to that group. The members of this group are those users who will administer the PS Series group and to whom the Network Policy will be applied.
    - Create a Network Policy on the NPS server that specifies conditions to grant administrator privilege to a PS Series group.
    - Add Vendor Specific Attributes to the policy to grant specific access privileges to the PS Series Group.
  - Optionally configure to use CHAP and RADIUS clients for iSCSI access to the PS Series Group

The following sections describe each of these tasks in detail.

#### PREPARE THE SERVER AND PS GROUP FOR RADIUS AUTHENTICATION

This section covers installing Network Policy Services, configuring the PS Series group as a RADIUS client on the NPS server and configuring the PS Series group to recognize and accept login attempts from the RADIUS server.

#### Installing and Configuring Network Policy Services

This procedure assumes you will install and configure these services on the same server hosting Active Directory. We recommend running these services on the same server hosting the Active Directory. If you cannot or choose not to, you must make sure that both servers are members of the same Windows Server domain, or that the service can proxy to another server with domain access to Active Directory.

Perform the following steps to install and configure the NPS on Windows Server 2008:

- Open Server Manager and add a new role.
- Select Network Policy and Access Services to install.
- After installing the NPS role open **Start > Administrative Tools > Network Policy Server**
- Register the NPS server in Active Directory by right clicking **NPS (Local)** > **Register server in Active Directory.** This setting allows the NPS Server to authenticate users in the Active Directory domain.
- Choose **OK** to the dialogue boxes to authorize the computer to read users' dialin properties from the domain.

#### Configuring a PS Series Group as a RADIUS Client on the NPS Server

To set up the PS Series group as a RADIUS client on NPS (in Windows Server 2003 and IAS this will be a two-step process):

- Open the **Network Policy Server** console and right-click **RADIUS Clients**.
- Click **New RADIUS Client** to open the New RADIUS Client wizard, Figure 1.

#### Figure 1: New RADIUS Client

w RADIUS Client	
Enable this RADIUS client	
Name and Address	
Friendly name:	
PSSeriesGroup	
Address (IF or DINS):	1 N M
192.168.1.10	venty
Vendor	
Specify RADIUS Standard for most RADIUS clients, or select the R/ vendor from the list.	ADIUS client
Vendor name:	
RADIUS Standard	•
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive.	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive.	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret:	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual Shared secret:	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual Shared secret: Confirm shared secret:	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual Shared secret: Confirm shared secret:	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual Shared secret: Confirm shared secret: 	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual G Generate Shared secret: Confirm shared secret: Additional Options	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual C Generate Shared secret: Confirm shared secret: Additional Options Access-Request messages must contain the Message-Authentic	nerate a shared he same shared same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual C Generate Shared secret: Confirm shared secret: Additional Options Access-Request messages must contain the Message-Authentic	nerate a shared he same shared same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual C Generate Shared secret: Confirm shared secret: Additional Options Access-Request messages must contain the Message-Authentic RADIUS client is NAP-capable	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual G Generate Shared secret: Confirm shared secret: Additional Options Access-Request messages must contain the Message-Authentic RADIUS client is NAP-capable	nerate a shared he same shared
Shared Secret To manually type a shared secret, click Manual. To automatically ge secret, click Generate. You must configure the RADIUS client with t secret entered here. Shared secrets are case-sensitive. Manual C Generate Shared secret: Confirm shared secret: Additional Options Access-Request messages must contain the Message-Authentic RADIUS client is NAP-capable	nerate a shared he same shared

Enter the following information:

- In the **Friendly name** field, enter a name for the client. We suggest using the PS Series group name.
- In the Client address field, enter the PS Series group IP address. (Verifying the address is optional.)In the Vendor name drop-down list, select RADIUS Standard, if not already selected.
- Check the **Manual** option if not checked already and enter and confirm a **Shared secret** (password). Remember or make a note of the secret, as you will need to specify the same secret (password) in a later step on the PS Series group.
- Select or deselect the checkbox next to **Request must contain the Message Authenticator attribute**, as you prefer. PS Series arrays support this attribute, but whether you require it depends on your security policies.
- Click **Finish**.

#### Configuring the PS Series Group for RADIUS Login Attempts

The PS Series group must be configured to accept login attempts from the RADIUS server. This will allow your administrators to connect to the PS Series SAN (or SANs). You can use either the Group Manager GUI or the CLI to configure the group. See <u>Appendix B</u> for instruction on using the command line interface.

#### Using the Group Manager GUI

To configure the group using the Group Manager GUI:

- Log in to the Group Manager GUI.
- Click Group Configuration > Administration tab (Figure 2).

#### Figure 2: PS Series Group Manager – Administration

🖉 BetaGrp - EqualLogic P5 Series Group Manager - Windows In	ternet Explorer
🚱 🕤 🗢 🔁 http://10.10.5.10/index.html	💌 🗟 🆅 🗙 🗖 Bing
🖕 Favorites 🛛 🚔 🏉 Suggested Sites 🔹 🙋 Web Slice Gallery 🔹	
🔁 BetaGrp - EqualLogic PS Series Group Manager	🏠 🔻 🔝 👻 🖃 Age 🕶 Safety 🕶 Tools 🕶 🕢
EQUALLOGIC	Account: grpadmin – Logged in 4/28/10 10:22:58 AM 🔗 Logout 💆
🚍 Group 🛛 🗐 🗸 💙 Group Configura	tion 🕒 🕤 😌 🚫 🤉
Group EQLSAN Summary	General Administration Notifications iSCSI SNMP VDS/VSS Defaults Advanced
⊕ ● Storage Pools           General Settings           Group name: EQLSAN         IP address: 10.105.10         Address: 10.105.10         Address: enabled	Administration Access     Ø       GUI access     CLI access       I Enable typeb access     I Enable teinet access
Telnet access: enabled SSH access: enabled	Allow only secure SSL connections
E-mail Notifications E-mail alerts: disabled E-mail Home: disabled Syslog: disabled ISCSI Authentication RADUS: disabled Local CHAP: enabled SMMP Settings	RADIUS Authentication       Image: Constraint of Constraints of Constra
SNMP traps: disabled	Administration Accounts
VUSIVISS       Access: restricted       Volumes       Replication       Monitoring	Account       Account type       Pool access       Status       Add
2 ?	
Tools 👔 Alarms 🛞 0 🗥	1 💡 0 🔰 Operations 🛞 0 🚱 0 🤍 🖓 💌
Done	🛛 🚺 🖗 Internet   Protected Mode: Off

- In the RADIUS Authentication panel, select the checkbox: **Enable RADIUS** authentication for login and Require vendor-specific RADIUS attribute.
- Optionally (not recommended), deselect the checkbox: Enable RADIUS accounting for authenticated users.
- Click **RADIUS Settings**, (Figure 3).
- In the RADIUS authentication servers area, click Add.

RAD	IUS settings			×
R	ADIUS authentication servers—		RADIUS accounting servers	
1	0.10.5.130:1812	Add	Add	
1	0.10.5.125:1812	Modify	Modify	
1	0.10.5.164:1812		Delete	
			Up An a	
		Down	Down	
R	equest timeout, seconds:	2 🔶	Request timeout, seconds: 2	
	Number of retries:	•	Number of retries: 1	
		🖊 ок 🛛 🖇	Cancel	
	Add RADIUS authentic	ation se	rver 🔀	
	IP address:		Port 1812	
	RADIUS secret:			
	Confirm secret:			
		ок 🖇	Cancel	

**Figure 3: RADIUS Settings** 

- Enter the IP address for the RADIUS authentication server, and enter and confirm a secret. Click **OK**.
- Adjust the Request timeout value and Number of retries value in the RADIUS settings dialog window as desired. Click **OK**.

Finally, confirm and save all settings by clicking the floppy disk icon in the upper right of the group manager interface.

## MANAGING SAN ADMINISTRATION THORUGH VENDOR SPECIFIC ATTRIBUTES

Depending on the role of the SAN administrator, multiple user groups can be created to use Vendor Specific Attributes to control access privileges to the PS Series SAN. For example some users may have full access to the PS Series group while others may have read-only or volume access to the group.

This section will detail the process of creating users and assigning them to specific groups to manage the PS Series SAN.

#### Creating Users and Groups for SAN Administration

It is recommended to create new Active Directory groups to manage the users that will have SAN privileges. This will help manage SAN administrators and prevent other users from accessing the PS Series SAN.

To add a new group to manage the PS Series group administrators and add users to that group:

• Open the Using Active Directory Users and Computers panel and create a new group to manage SAN Administrators (Figure 4).

Create in: DMLi	abnet.com/Users
Group name:	
SAN Admins	
Group name (pre-Windows 2)	000):
SAN Admins	
Group scope	Group type
C Domain local	Security
Global	C Distribution
C Universal	•

Figure 4: New Group

 Now you can add users to the new group that will manage the PS Series SAN. Make sure the Remote Dial-in properties for each user is set to Control access through NPS Network Policy (Figure 5).

Figure 5: Remote Dial-in Properties

SAN User Properties
Remote control         Terminal Services Profile         COM+           General         Address         Account         Profile         Telephones         Organization           Member Of         Dial-in         Environment         Sessions
Network Access Permission     Allow access     Deny access     C Deny access     C Control access through NPS Network Policy
Venfy Caller-ID:     Callback Options     No Callback     Set by Caller (Routing and Remote Access Service only)     Aways Callback to:
Assign Static IP Addresses     Define IP addresses to enable for this     Dial-in connection.     Apply Static Routes     Define routes to enable for this Dial-in     Static Routes
OK Cancel Apply Help

**Note:** If you are currently running in mixed mode you will have to **allow** each user Remote Access Permission (Figure 6).

AN-User Properties	? :
Remote control Termin General Address Account Member Of Dial-in	al Services Profile COM+ Profile Telephones Organization Environment Sessions
Remote Access Permission (Dial-in     Allow access     Deny access     C Deny access through Remote	or VPN) Access <u>P</u> olicy
✓erify Caller-ID;         Callback Options         Image: Comparison of the second sec	ote Access Service only)
Assign a Static IP Address Apply Static Boutes Define routes to enable for this Dia connection.	al-in Static Roytes
0	K Cancel <u>Apply</u>

Figure 6: Adding Remote Access Permissions (Mixed mode domain)

#### **Creating Network Policies on the NPS Server**

A network policy applies to a user profile (in Active Directory) and tells the RADIUS server what type of privilege to grant a user who attempts to log in to a PS Series group. You must create a network policy for each type of account configured on the PS Series group. All PS Series Firmware versions support group administrator full access and read-only accounts.

When the user is authenticated, the policy also specifies the authentication information to return from the RADIUS server to the PS Series group. For example, it indicates whether the user is a group administrator or a pool administrator, and which pools they are allowed to manage.

Pool administrators can manage the objects in their designated pools, and optionally can have read-only permission on all other objects in the group (members, pools, and volumes). Volume administrators can manage a specific amount of storage or quota value in a designated pool. For more information on pool administrators, see the Group Administration guide.

Table 1 list some of the most common used attribute values for network policies as well as new values introduced in PS Series firmware v5.0.x. For a complete list of all supported attribute values and PS Series firmware requirements see Table 2 in <u>Creating</u> Additional Network Policies Using Optional VSAs.

# Table 1: Common PS Series Supported Vendor Specific Attributes and Firmware Versions

Attribute	Field	Value	PS Series Supported Firmware	
EQL-Admin	Attribute Number Attribute Format (Syntax)	6 Decimal	Value 0 – All Versions Values 1, 2 –	
	Attribute Value	<b>0</b> = Global Admin, <b>1</b> =Pool Admin only, <b>2</b> =Pool Admin with group read access, <b>3</b> =Volume Admin	Version 3.2.x and higher Value 3 – Version 5.0.x	
EQL-Pool-	Attribute Number	7	Version 3.2 and	
Access	Attribute Format (Syntax)	String (Max. length: 247)	higher	
	Attribute Value	Value is the pool name. The quota for volume administration accounts is expressed as <i>PoolName Quota</i> , with G and M appended to the quota representing GB and MB, respectively. For example: Pool1 25G sets the quota for Pool1 to 25GB and Pool1 500M sets a quota of 500MB.	*Use unlimited to set an unlimited quota for the pool, (example: Pool1 unlimited). If no unit is specified, the default capacity unit is MB.	
EQL-	Attribute Number	8	Version 5.0 and	
Site-Access	Attribute Format (Syntax)	String (Max. length: 249)	ligher	
	Attribute Value	Indicating a comma-separated list of replication site names		
EQL-Admin-	Attribute Number	9	Version 5.0 and	
Account-Type	Attribute Format (Syntax)	String (Max. length: 249)	*To create a read-	
	Attribute Value	RO or RW - Indicating whether the account is read-only or read-write	the EQL-Admin value to 0 and the EQL_Admin- Account-Type to RO.	

This section describes creating a Network Policy for group administrators (those with full, group-wide privileges).

To create a Network Policy for PS Series group administrators on the NPS Server:

• Click Start > Administrative Tools > Network Policy Server.

- Expand the **Policies** section, right-click **Network Policies**, and click **New**.
- The New Network Policy Wizard starts (Figure 7).
- Give the policy a name and leave the *Type of network access server* button checked with **Unspecified** in the box and click **Next**.

#### Figure 7: NPS – Create New Network Policy

😔 Network Policy Server		
File Action View Help		
🗢 🔿 🔰 📰 🔽 🖬	New Network Policy	×
NPS (Local)	Specify Network Policy Name and Connection Type	
RADIUS Clients	You can specify a name for your network policy and the type of connections to which the policy is applied.	
Connection Request P	Policy name:	_
Health Policies		
Accounting	Network connection method	
reconning	Select the type of network access server that sends the connection request to NPS. You can select either the network access serve type or Vendor specific.	r
	Type of network access server:	
	C. Vendor specific:	
	10	
	Previous Next Finish Cancel	

- The Specify Conditions screen starts.
- Click **Add** to add the conditions that need to be met in order to access the PS Series Group.
- In the **Select Condition** view, scroll down to **Client Friendly Name** and click **Add** (Figure 8).

#### Figure 8: Policy Conditions

New Network F	Policy X
	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.
Select conditi	on 🚬
Select a condi	tion, and then click Add.
Serv The S Point	ice Type Fervice Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or to Point Protocol connections.
Tunr The T	iel Type unnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or
RADIUS Clie	ent
Calli The C	ing Station ID alling Station ID condition specifies the network access server telephone number dialed by the access client.
Clier The C	nt Friendly Name Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to
The C	ht IPv4 Address Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request S.
	Add Cancel
	Add Edit Remove
	Previous Next Finish Cancel

• In the **Client Friendly Name** window add the name of the RADIUS Client created for the PS Series group admins in the previous section (Figure 9).

Figure 9: Client Friendly Name

New Network P	olicy	×
	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for of one condition is required.	a connection request. A minimum
Select conditio	n	×
Select a conditi	ion, and then click Add.	
Tunne The Tu	el Type unnel Type condition restricts the policy to only clients that create a specific type of tur	nnel, such as PPTP or
RADIUS Clier	t Client Friendly Name	×
The Callin	19 Station alling Stat syntax.	ng access client.
Clien The Cl	lient Friendly  PSSeriesGroup	ection request to
The Client The Client to NPS	t IPv4 Adk lient IP Ad 5. OK Cance	nection request
The Client	t IPv6 Add litent IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwa st to IPF5.	rded the connection
		Add Cancel

- Verify the information is correct in the Specify Conditions list and click **Add** to add the next condition. The next condition needed will be the user group account with logon permissions.
- In the **Select Condition** view, choose **Windows Groups** and click **Add** (Figure 10).

#### Figure 10: Adding Windows Groups

New Netwo	k Policy 🔀
	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.
c	
Select cond	ition 📃 🕺
Select a co	ndition, and then click Add.
Wi Wi Th	ndows Groups e Windows Groups condition specifies that the connecting user or computer must belong to one of the selected
Ma See Th	Ichine Groups e Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.
State	.er Groups e User Groups condition specifies that the connecting user must belong to one of the selected groups.
HCAP Lo Th rec ne	cation Groups e HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups jurred to match this policy. The HCAP protocol is used for communication between NPS and some third party twork access servers (NASs). See your NAS documentation before using this condition.
C HO	CAP User Groups
	Add Cancel
	Add Edit Remove
	Previous Next Finish Cancel

• Specify the Windows Groups by adding the "SAN Admins" group created in the previous section (Figure 11).

Figure 11: Specify Windows Groups

🔊 Network Policy Server	<u>- 🗆 ×</u>
File Action View Help	
	न
The MPS (local)	<u>الا</u>
🖻 🛅 RADIUS C 🦰 Specify Conditions	inces under
RADII Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum	
Fremo of one condition is required.	be Source
Cons	ess Unspecified
Netwood Select condition	ss Unspecified
Healt	ss Unspecified
Accountin Genue	ss Unspecified
Specify the group membership required to match this policy.	
The Windows Gro	
Machine Groups	
The Machine Gro scted groups.	
👩 User Groups Select Group ? 🗙	
The User Groups Select this object type	
HCAP Group Object Types	
The UCARL cost in Groups	
required to match DMI above com	
HCAP User Grc Enter the object name to select (examples):	
SAN Admins Check Names	
Advanced OK Cancel	-
Previous Next Finish Cancel	
	-
Acon: in progress	J.

- Click **OK** to confirm the selection and complete the conditions entry. Verify the new network policy conditions are correct and choose **Next** to continue.
- Grant network access by checking the **Access granted** button in the **Specify Access Permission** window and click **Next**.
- In the Configure Authentication Methods window only check the **Unencrypted authentication (PAP, SPAP)** box and uncheck all others (Figure 12).

#### Figure 12: Configure Authentication Methods

New Network P	Policy	×
	Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.	
EAP types are n EAP Types:	negotiated between NPS and the client in the order in which they are listed.  Move Up  Move Down	
Add	Edt Remove	
Microsoft E User ca Microsoft E User ca User ca Encrypted a User ca	Incrysted Authentication version 2 (MS-CHAP-v2) in change password after it has expired morphed Authentication (MS-CHAP) in change password after it has expired authentication (CHAP) ed authentication (PAP, SPAP)	
<ul> <li>Allow client</li> <li>Perform ma</li> </ul>	s to connect without negotisting an authentication method. chine health check only Previous Next Finish Cancel	

**Note:** By default, all passwords are encrypted by the RADIUS protocol. Choosing the unencrypted authentication here is simply for tunneling into the NPS server.

- A Connection Request Policy pop up may appear. Choose **No** to disregard the help topic.
- Optionally configure constraints in the next window and click **Next**.
- In the **Configure Settings** window click on **Standard** in the RADIUS Attributes section.
- Remove the **Framed-Protocol** attribute and change the **Service-Type** to Administrative (Check **Others** and choose **Administrative** in the drop down box, Figure 13). Click **OK** when done.

#### Configure Settings NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched Configure the settings for the Attribute Information of the Attribute Info × Attribute name Service-Type Settings: RADIUS Attributes ndard attribute, and DIUS clients. See Attribute number 🏐 Standard Vendor Specific Attribute format: Enumerator Network Access Protection Attribute Value: NAP Enforcement C Commonly used for Dial-Up or VPN Extended State Framed -Routing and Remote C Commonly used for 802.1x Access 🥐 Multilink and <none> Bandwidth Allocatic Protocol (BAP) <none> • 🔒 IP Filters <none> Login Callback Login A Encryption IP Settings Outbound Administrative NAS Promot Callback Nas Prompt Callback Administrative Authorize only Previous Next Cancel

#### Figure 13: Service Type Attribute

#### Adding the PS Series Vendor-Specific Attributes

Vendor-specific attributes tailor the remote access policy to the vendor. For PS Series arrays, there are two required attributes, and several optional ones. The required attributes control what objects on the PS Series group users can manage once they log in. Group administrators can manage all objects on the group, including adding and removing members, and creating storage pools.

If you configure the optional attributes, the values will be supplied automatically to the PS Series group and will appear in the Contact Information fields (except for EQL-Admin-Poll-Interval) in the Group Manager GUI for each contact. Every time a user logs in, their information will be updated if it has changed since the last login.

The following procedure continues from Creating Network Policies on the NPS Server, and assumes the **Configure Settings** screen is still displayed.

- On the same screen click **Vendor Specific** in the RADIUS Attributes area and **Add** a new Vendor Specific attribute.
- In the Add Vendor Specific Attribute window leave the Vendor at All and scroll down in the Attributes to Vendor-Specific – RADIUS Standard (Figure 14) and click Add.

#### Figure 14: Vendor Specific Attribute

👶 Network Polic	y Server		- 🗆 🗵
File Action Vie	ew Help		
(= =) 2 m	New Network Delies	V	
NPS (Local)	NEW NELWORK POlicy		
🖃 🚞 RADIUS C	Configu	inces university of the settings and setting	der
RADI	NPS applies s	settings to the connection request if all of the network policy conditions and constraints for the policy	
Remo	are matched.		Ince
Conne		ess Uns	specified
interview 🖄 🖄	Configure the settings for this r	network policy. ess Uns	specified
Healt	If conditions and constraints m	natch the connection request and the policy grants access, settings are applied.	specified
	Settings:	iss Uns	specified
	RADIUS Attributes	Add Vendor Specific Attribute	×
	Standard	To add an attribute to the settings, select the attribute, and then click Add.	
	🗾 Vendor Specific	To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.	
	Network Access		
	Protection	Vendor:	
	NAP Enforcement	Al	F
	Extended State		-
	Routing and Remote	Attributes:	_
	Access	Name Vendor	<u> </u>
	Multilink and Bandwidth Allocation	USR-Tunnet-Switch-Endpoint U.S. Robotics, Inc.	
	Protocol (BAP)	USR-VPN-Encryptor U.S. Robotics, Inc.	
		USR-VPN-GW-Location-Id U.S. Robotics, Inc.	
	IP Filters	USR-VTS-Session-Key U.S. Robotics, Inc.	
	Recryption	Vendor-Specific RADIUS Standard	키느
	IP Settings		1
			l l
		Description:	
		Specifies the support of proprietary NAS features.	ľ
1		Add Close	1
	I		
Action: In progress	J.		
Action: In progress	IP Filters	USR-VTS-Session-Key U.S. Robotics, Inc. Vendor-Specific RADIUS Standard	

- In the Attribute Information window click Add.
- In the next window check Enter Vendor Code and enter 12740 in the field. This is the vendor code for PS Series arrays. Select Yes, It conforms button and click Configure Attribute (Figure 15).

Vendor-Specific		
Specify network access :	server vendor.	
Select from list:	RADIUS Standard	~
Enter Vendor Code: Specify whether the attrib vendor specific attributes.	12740 ute conforms to the RADIUS RFC spe	ecification for
<ul> <li>Enter Vendor Code:</li> <li>Specify whether the attributes.</li> <li>Yes. It conforms.</li> <li>No. It does not conformation of the second second</li></ul>	12740 ute conforms to the RADIUS RFC spe m.	ecification for

#### Figure 15: Vendor-Specific Attribute Information

• The Configure VSA dialog box is displayed (Figure 16).

Figure 16: Configure VSA

Configure VSA (RFC compliant)	?	x
Vendor-assigned attribute number: 6		
Attribute format: Decimal		•
Attribute value:		_
· · · · · · · · · · · · · · · · · · ·		
	OK Cancel	

- Enter the following information for the PS Series group administrator attribute:
  - o In the Vendor-assigned attribute number field, enter 6
  - o In the Attribute format drop-down list, select **Decimal**.
  - $\circ$  In the Attribute value field, enter **0** (for a group administrator).
- When finished click OK twice and Close the Add Vendor Specific Attribute window and verify the information is correct in the Configure Settings screen.
- Refer to <u>Table 1</u> for optional Vendor Specific Attributes for PS Series arrays.
- To finish the Configure Settings section click on **Encryption** at the bottom of the Settings section.
- Uncheck all the boxes except **No encryption** and click **Next**. This will allow the Network Policy to rout through to the RADIUS server.
- Complete the New Network Policy by verifying the setting and clicking Finish.

#### Creating Additional Network Policies using Optional VSA's

This section will discuss optional vendor specific attributes that can be used to add more granular access to a PS Series group. An example of an administration account with more granular access would be a pool administrator. Pool administrators have management privileges only for specific pools on a PS Series group. To allow those users to log in yet restrict their privileges to only the pools appropriate to them, you must create a unique Active Directory group and a Remote Access Policy on the NPS server specific to each type of pool administration account you need.

Another example might be a volume administrator. Volume administrators have access to a specific pool and a quota value that they can use for volume creation. These are some of the examples that will be discussed in this section.

Follow the steps laid out in the previous sections to add new user groups for the new administration roles and refer to <u>Creating Network Policies on the NPS Server</u> to add the new policy attributes for administrators.

**Note:** Attribute values are supported at specific PS Series firmware levels. Refer to Table 2 in this section for a complete list of supported attribute values and firmware levels.

#### **Example 1: Configuring Attributes Values for Pool Administrators:**

For example, you might have pool administrators for Pools A and B on a PS Series group, and others for Pools C and D. Additionally, you might have pool administrators who also have group-wide read-only privilege. These users can see, but not change, all the other objects in the group.

When adding the Vendor Specific Attributes for the new Network Policy, follow the steps below. Add a vendor-specific attribute with the following fields:

- Vendor-specific attribute number: enter 6
- Attribute format drop-down: select Decimal
- Attribute value field: enter 1

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number:		
6		
<u>Attribute format:</u>		
Decimal		-
Attri <u>b</u> ute value:		
1		
	OK Ca	ncel

- Click **OK** twice to get back to the Attribute Information window.
- Add another Attribute Value to specify the PS Series pool attributes. Use the same Vendor Code for network access server (12740) and choose "Yes. It conforms." Configure the attribute values as follows:

- Vendor-assigned attribute number: enter 7
- Attribute format drop-down: select **String**
- Attribute value field: enter the **pool name** for the account. Repeat this process if more than one pool will be accessed by the account.

Configure VSA (RFC compliant)	? ×
Vendor-assigned attribute number:	
7	
<u>Attribute format:</u>	
String	▼
Attri <u>b</u> ute value:	
Pool1	
	OK Cancel

The Attribute Information window should look as follows:

Attribute Informatio	n	×
Attribute name: Vendor-Specific		
Attribute number: 26		
Attribute format: OctetString		
Attribute values:		
Vendor	Value	Add
Vendor Code: 12740	1	
Vendor Code: 12740	Pool1	Edit
Vendor Code: 12740	Pool2	Remove
		Move Up
		Move Down
	ОК	Cancel

#### Example 2: Configuring Attribute Values for Volume Administrators

Similar to Pool Administrators the attributes for Volume Administrators use the same arguments with the exception of the administrative access level and a quota value after the pool name.

Configure the administrative level for the volume admin:

- Vendor-specific attribute number: enter 6
- Attribute format drop-down: select **Decimal**
- Attribute value field: enter **3**

Configure VSA (RFC Compliant)
Vendor-assigned attribute number:
Attribute format:
Decimal
Attribute value:
3
OK Cancel

- Click **OK** twice to get back to the Attribute Information window.
- Add another Attribute Value to specify the PS Series pool and quota attributes. Use the same Vendor Code for network access server (12740) and choose "Yes. It conforms." Configure the attribute values as follows:
  - Vendor-assigned attribute number: enter 7
  - Attribute format drop-down: select **String**
  - Attribute value field: enter the **pool name** and **quota value** for the account. For this example the pool name is 450–15k and the quota is
    - 100GB. **Note:** The quota value is case insensitive.

Configure VSA (RFC Comp	oliant)	×
Vendor-assigned attribute nu	umber:	
Attribute format:		
String		•
Attribute value:		
450-15k 100GB		
	OK	Cancel

The attribute information should now look similar to the following:

Attribute Informatio	n		×
Attribute name: Vendor-Specific			
Attribute number: 26			
Attribute format: OctetString			
Attribute values:			
Vendor	Value		Add
Vendor Code: 12740	3		
Vendor Code: 12740	450-15k 100GB		Edit
			Remove
			Move Up
			Maus Daws
I			Move Down
		ОК	Cancel

To add any additional or other optional vendor-specific attributes such as making this pool admin account read only, refer to Table 2 for their values.

Attribute	Field	Value	PS Series Supported Firmware
EQL-Admin- Full-Name	Attribute Number	1	All Versions
	Attribute Format (Syntax)	String (Max. length: 247)	
	Attribute Value	Name of person assigned to the account	
EQL-Admin- Email	Attribute Number	2	All Versions
	Attribute Format (Syntax)	String (Max. length: 247)	
	Attribute Value	Email address of person assigned to the account	
EQL-Admin- Phone	Attribute Number	3	All Versions
	Attribute Format (Syntax)	String (Max. length: 247)	
	Attribute Value	Phone number of person assigned to the account	
EQL-Admin- Mobile	Attribute Number	4	All Versions
	Attribute Format (Syntax)	String (Max. length: 247)	
	Attribute Value	Mobile number of person assigned to the account	
EQL-Admin- Poll-Interval	Attribute Number	5	All Versions
	Attribute Format (Syntax)	Integer (Max length: 6 numerals)	
	Attribute Value	Number of seconds until the group configuration data must be re-polled by the GUI. Default is 30 seconds.	
EQL-Admin	Attribute Number	6	Value 0 – All Versions
	Attribute Format (Syntax)	Decimal	Values 1, 2 – Version 3.2.x and

 Table 2: PS Series Optional Vendor Specific Attribute Values

	Attribute Value	<b>0</b> = Global Admin, <b>1</b> =Pool Admin only, <b>2</b> =Pool Admin with group read access, <b>3</b> =Volume Admin	higher Value 3 – Version 5.0.x
EQL-Pool- Access	Attribute Number	7	Version 3.2 and higher
	Attribute Format (Syntax)	String (Max. length: 247)	*Use unlimited to
	Attribute Value	Value is the pool name. The quota for volume administration accounts is expressed as <i>PoolName</i> <i>Quota</i> , with G and M appended to the quota representing GB and MB, respectively. For example: Pool1 25G sets the quota for Pool1 to 25GB and Pool1 500M sets a quota of 500MB.	set an unlimited quota for the pool, (example: Pool1 unlimited). If no unit is specified, the default capacity unit is MB.
EQL- Replication-	Attribute Number	8	Version 5.0 and higher
Sile-Access	Attribute Format (Syntax)	String (Max. length: 249)	
	Attribute Value	Indicating a comma-separated list of replication site names	
EQL-Admin- Account-Type	Attribute Number	9	Version 5.0 and higher
	Attribute Format (Syntax)	String (Max. length: 249)	*To create a read- only account, set
	Attribute Value	RO or RW - Indicating whether the account is read-only or read-write	value to 0 and the EQL_Admin- Account-Type to RO.

#### CONFIGURING RADIUS FOR ISCSI AUTHENTICATION TO PS SERIES GROUPS

CHAP, Challenge-Handshake Authentication Protocol can also be used for authentication with RADIUS clients to a PS Series group. This is useful for controlling standard iSCSI authentication to PS Series volumes through Active Directory services.

Using iSCSI authentication with RADIUS requires passwords to be stored using reversible encryption. This setting may need to be changed for the domain policy using the Group Policy editor for the domain profile. Once in the group policy editor navigate to Computer Configuration – Windows Settings – Security Settings – Account Policies – Password Policy and enable this setting for the domain group policy.

**Note:** It is recommended to add RADIUS Clients for each of the enabled PS array IP ports. This includes the PS Series group IP and all the enabled controller port IPs on the arrays in the group. This allows CHAP connections through multiple ports for redundancy and performance benefits.

Follow these steps to configure RADIUS with CHAP authentication:

#### **Configuring the Windows Server 2008 NPS**

On the Windows Server 2008 NPS server navigate to **NPS – Policies – Connection Request Policies** 

Open the built-in default policy – **Use Windows authentication for all users**, (Figure 17).

Figure 17: Built-in Policy 'Use Windows authentication for all users'



Open the policy and verify the policy is enabled. Under **Network connection method**, be sure the **Type of network access server** radial button is selected and **Unspecified** is shown in the drop down box.

Select the **Settings** tab. In the settings window check the box next to **Encrypted authentication (CHAP)** and uncheck everything else, (Figure 18).

conditions and constraints match the	connection request and the policy grants access, settings are applied.
ttings: Required Authentication	
Methods	Veride network policy authentication settings
Authentication Methods	These authentication settings are used rather than the constraints and authentication
Forwarding Connection Request	configure PEAP authentication here.
Authentication	EAP types are negotiated between NPS and the client in the order in which they
National Accounting	are listed.
Specify a Realm Name	EAP Types:
Attribute	Move Up
RADIUS Attributes	Move Down
🚯 Standard	
Vendor Specific	Add Edit Remove
<u></u>	Less secure authentication methods:
	Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
	User can change password after it has expired
	Microsoft Encrypted Authentication (MS-CHAP)
	User can change password after it has expired
	Encrypted authentication (CHAP)
	Unencrypted authentication (PAP, SPAP)
	Allow clients to connect without negotiating an authentication method.

Figure 18: Configure the Policy with CHAP Authentication

Click OK when finished to close the window.

Create new users to use the policy. The new users will be the CHAP username given to the PS Series volume access control. Set the users up the same way described in the section <u>Creating Users and Groups for SAN Administration</u>. Make sure you check the box to *Store password using reversible encryption* in the **Account** tab. There is no need to create additional user groups in this case because the CHAP users will use the default **Domain Users** group for authentication.

#### **Configuring the Windows Server 2003 IAS**

In Windows Server 2003 IAS the steps are slightly different. A remote access policy will need to be created similar to those described in Appendix A in this document.

On the Windows 2003 IAS server open Internet Authentication Services and create a new remote access policy. Select a custom policy and give the policy a recognizable name.

In the policy conditions **Add** a new condition and select **Authentication-Type** as the attribute.

This will open the Authentication-Type window. Select **CHAP** and add it to the **Selected types:** area and click OK.

Select **Next >** to progress to the next screen. In the **Permissions** screen, select **Grant remote access permission** to enable remote access for the policy and click **Next >**.

Select the Edit Profile... option to start the Dial-in Profile configuration.

In the Dial-in Profile settings navigate to the **IP** tab and verify that the **Server settings determine IP address assignment** option is the only option checked.

Now navigate to the **Authentication** tab and uncheck everything except the **Encrypted authentication (CHAP)** option. If this box is not checked, check it now.

Navigate to the **Encryption** tab and uncheck everything except **No encryption**. If this box is not checked, check it now.

Finally navigate to the **Advanced** tab and remove the **Framed-Protocol** attribute. Edit the **Service-Type** attribute and change it to **Administrative**.

Finish the policy by clicking **OK** and **OK** to save and close the policy wizard.

Create new users to use the policy. The new users will be the CHAP username specified when configuring access control to the PS Series volume. Set the users up the same way described in the section <u>Creating Users and Groups for SAN Administration</u>. Make sure you check the box to *Store password using reversible encryption* in the **Account** tab. There is no need to create additional user groups in this case because the CHAP users will use the default **Domain Users** group for authentication.

#### **Connecting to Volumes**

Depending on what operating system is being used the volume connection steps may vary.

#### From a server or host running Windows Server 2008 or Windows 7:

- Open the iSCSI Initiator Properties
- Select the **RADIUS** tab and add the IP or DNS name of the RADIUS server granting access to the PS Series volumes.
- If a shared secret was used then verify authentication by providing the secret.
- Select the **Discovery** tab and verify the PS group IP is in the Target portals window.
- Select the **Targets** tab and refresh to view volumes. Any configured volumes should show up.
- Log onto a configured volume by selecting **Log on**...
- Choose the **Advanced**... button to open the **Advanced Settings** window.
- In the Advanced Settings window select the box next to **CHAP logon information** and add the CHAP user name and target secret for authentication.
- Select the box next to **Use RADIUS to authenticate target credentials** (Figure 19) and hit **OK** and **OK** to complete the process.

erai   IPsec	
Connect by using	
.ocal adapter:	Default
Source IP:	Default 💌
Target portal:	Default
CRC / Checksum -	
✓ Data digest ✓ CHAP logon in CHAP helps ensurn nitiator. To use it, for this initiator.	Formation e data security by providing authentication between a target and an , specify the same target CHAP secret that was configured on the target
Data digest CHAP logon in CHAP helps ensur initiator. To use it, for this initiator. Jser name:	Formation e data security by providing authentication between a target and an , specify the same target CHAP secret that was configured on the target chap-user
Data digest CHAP logon in CHAP helps ensur initiator. To use it, for this initiator. User name: Target secret:	Formation e data security by providing authentication between a target and an specify the same target CHAP secret that was configured on the target chap-user
Data digest CHAP logon in CHAP helps ensur nitiator. To use it, for this initiator. User name: Iarget secret: Use RADIUS to	Header digest formation e data security by providing authentication between a target and an specify the same target CHAP secret that was configured on the target chap-user o generate user authentication credentials
Data digest CHAP logon in CHAP helps ensur initiator. To use it, for this initiator. User name: Iarget secret: Use RADIUS to Perform mutua	Header digest  formation e data security by providing authentication between a target and an specify the same target CHAP secret that was configured on the target  chap-user  o generate user authentication credentials al authentication
Data digest CHAP logon in CHAP helps ensur initiator. To use it, for this initiator. User name: User name: User RADIUS to Perform mutua To use mutual CHI RADIUS. The sam	Header digest  formation  e data security by providing authentication between a target and an , specify the same target CHAP secret that was configured on the target  chap-user  o generate user authentication credentials al authentication  AP either specify an initiator secret on the Initiator Settings page or use the secret must be configured on the target.

Figure 19: Volume Log-On Using CHAP – Windows 2008

#### From a server or host running Windows Server 2003 or Windows XP

- Open the iSCSI Initiator Properties
- Select the **Discovery** tab and verify the PS group IP is in the Target portals window.
- Select the **Targets** tab and refresh to view volumes. Any configured volumes should show up.
- Log onto a configured volume by selecting **Log on...**
- Choose the **Advanced**... button to open the **Advanced Settings** window.
- In the Advanced Settings window modify the **Connect by using** section as follows:
  - O Local adapter: Microsoft iSCSI Initiator
  - Source IP: [This is the IP of the RADIUS server]
  - Target Portal: [The portal IP of the PS group]
- Select the box next to **CHAP logon information** and add the CHAP user name and target secret for authentication (Figure 20).
- Hit **OK** and **OK** to complete the process.

Advanced Setting	s ?X
General IPSec	l,
Connect by usi	ng
Local <u>a</u> dapter:	Microsoft iSCSI Initiator
Source <u>I</u> P:	10.10.5.125
<u>T</u> arget Portal:	10.10.5.50 / 3260
CRC / Checks	ım
🔲 <u>D</u> ata diges	E <u>H</u> eader digest
CHAP logo	n information
CHAP helps er a target and ar specify the san for this initiator.	sure data security by providing authentication between initiator trying to establish a connection. To use it the target CHAP secret that was configured on the target
<u>U</u> ser name:	chapuser1
Target <u>s</u> ecret:	••••••
Perform mu	tual authentication
To use mutual page and confi	CHAP specify an initiator secret on the Initiator Settings gure that secret on the target.
	OK Cancel Apply

Figure 20: Volume Log-On Using CHAP – Windows 2003

#### **APPENDIX A – CONFIGURATION STEPS ON WINDOWS SERVER 2003**

This procedure assumes you will install and configure IAS on the same server hosting Active Directory.

Perform the following steps to install and configure the IAS Server:

- Click Start > Control Panel > Add or Remove Programs.
- Click Add/Remove Windows Components.
- In the Windows Components dialog box, select **Networking Services**, then click **Details**.
- In the Networking Services dialog box, check the box for **Internet Authentication Service**, then click **OK**.
- You return to the Windows Components dialog box. Click **Next**.
- On the Completing the Windows Components Wizard screen, click **Finish**.

After installing IAS, you must make some modifications to the configuration, as follows:

- Click Start > Administrative Tools > Internet Authentication Services.
- In the Internet Authentication Services console, right-click **Internet Authentication Service (Local)**, then click **Register Server in Active Directory**. This setting allows the IAS Server to authenticate users in the Active Directory domain.
- Click **OK**.

#### Configuring a PS Series Group as a RADIUS Client on the IAS Server

To set up the PS Series group as a RADIUS client on IAS:

- Click Start > Administrative Tools > Internet Authentication Service.
- Right-click the **RADIUS Clients** folder.
- Click **New** > **RADIUS Client**.

#### Figure 1: New RADIUS Client

💖 Internet Authentication S	ervice	_ 🗆 🗵
File Action View Help		
⇔ → 🗈 🖬 💼 🔮	New RADIUS Client	
P Internet Authentication Service	Name and Address	lient-Vendor
RADIUS Clients	Type a friendly name and either an IP Address or DNS name for the client.	ADIUS Standard
Connection Request	Eriendly name: Support7	
	Client address (IP or DNS): 172.23.10.70	
	< Back Next > Cancel	
		Þ

Enter the following information:

- In the **Friendly name** field, enter a name for the client. We suggest using the PS Series group name.
- In the **Client address** field, enter the PS Series group IP address. (Verifying the address is optional.)
- Click **Next**. The Additional Information dialog box is displayed.

Internet Authentication S	ervice	_ 🗆 ×
File Action View Help		
⇔ ⇒ 🗈 🖪 👩	New RADIUS Client	
Internet Authentication Server	Additional Information	lient-Vendor ADIUS Standard
Remote Access Logging Remote Access Policies Connection Request Pro	If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client. Client-Vendor:	
	Shared secret:	
	Confirm shared secret:	
	$\square$ Request must contain the Message Authenticator attribute	
	< <u>B</u> ack Finish Cancel	
<u> </u>		Þ

Figure 2: New RADIUS Client – Additional Information

In the Additional Information dialog box, do the following:

- In the **Client-Vendor** drop-down list, select **RADIUS Standard**, if not already selected.
- Enter and confirm a **shared secret** (password). Remember or make a note of the secret, as you will need to specify the same secret (password) in a later step on the PS Series group.
- Select or deselect the checkbox next to **Request must contain the Message Authenticator attribute**, as you prefer. EqualLogic supports this attribute, but whether you require it depends on your security policies.
- Click **Finish**.

#### **Creating Remote Access Policies on the IAS Server**

Similar to a Network Policy, a remote access policy applies to a user profile (in Active Directory) and tells the RADIUS server what type of privilege to grant a user who attempts to log in to a PS Series group.

To create a Remote Access Policy for PS Series group administrators on the IAS Server:

- Click Start > Administrative Tools > Internet Authentication Service.
- Right-click **Remote Access Policy**, and click **New Remote Access Policy** (Figure 3).

🍫 Internet Authentication	Service		_ 🗆 X
File Action View Help			
⇐ ⇒ 🗈 🖪 🔂	E?		
Internet Authentication Ser     RADIUS Clients     Remote Access Logging     Remote Access Polic     Connection Request     Connection Request     Remote RADIUS	vice (Local) New Remote Access Policy New View Refresh Export List Help	Name SEQLRead EQL2Admin N	Order 1 2
Refreshes the current selection.			

Figure 3: IAS – Create New Remote Access Policy

• The New Remote Access Policy Wizard starts (Figure 4).

#### Figure 4: New Remote Access Policy Wizard

New Remote Authentication Service Remote Access Policy W	vice izard	_ <b>_</b> . ×
	Welcome to the New Remote Access Policy Wizard This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server. To continue, click Next.	Order 1 2
	<back next=""> Cancel</back>	

• Click **Next**. The Policy Configuration Method screen appears (Figure 5).

#### Figure 5: Policy Configuration Method

ew Remote Acce	ss Policy Wizard
Policy Configu The wizard o	ration Method an create a typical policy, or you can create a custom policy.
How do you v	vant to set up this policy?
⊖ <u>U</u> se th	e wizard to set up a typical policy for a common scenario
Set up	a custom policy
Type a name t	hat describes this policy.
Delieuweere	
Policy name:	EQL Group Administrators
	Example: Authenticate all VPN connections.
	< <u>B</u> ack <u>N</u> ext> Cancel

- Select **Set up a custom policy**, and enter a name for the policy; for example, EQL Group Administrators. Then, click **Next**.
- The Policy Conditions screen appears (Figure 6).

#### Figure 6: Policy Conditions

New Remote Access Policy Wizard	×
Policy Conditions To be authenticated, connection requests must match the conditions you specify.	Ŷ
Specify the conditions that connection requests must match to be granted or denied access. Policy conditions:	
	ŕ
Add	
< Back Next > Can	cel 1

- Under the Policy Conditions field, click Add.
- The Select Attribute screen appears (Figure 7).

Name	Description
Authentication-Type	Specifies the authentication scheme that is u
Called-Station-Id	Specifies the phone number dialed by the use
Calling-Station-Id	Specifies the phone number from which the c
Client-Friendly-Name	Specifies the friendly name for the RADIUS c
Client-IP-Address	Specifies the IP address of the RADIUS clier
Client-Vendor	Specifies the manufacturer of the RADIUS pr
Day-And-Time-Restric	Specifies the time periods and days of week
Framed-Protocol	Specifies the protocol that is used.
MS-RAS-Vendor	Description not yet defined
NAS-Identifier	Specifies the string that identifies the NAS the
NAS-IP-Address	Specifies the IP address of the NAS where the
NAS-Port-Type	Specifies the type of physical port that is use
Service-Type	Specifies the type of service that the user ha-
Tunnel-Type	Specifies the tunneling protocols used.
Windows-Groups	Specifies the Windows groups that the user t

Figure 7: Select Attribute

- Select Client-Friendly-Name and click Add.
- The Client-Friendly Name screen appears (Figure 8). Figure 8: Client-Friendly Name

Client-Friendly-Name		? ×
<u>Iype a word or a wild card (for example, al</u>	bc.*):	
eng1-grp		
	OK	Cancel

- Enter the PS Series group name you specified in Overview of Steps
- Optionally repeat this process and enter the Windows Group that the policy will be created for here.
- Verify the information is correct in the Policy conditions list (Figure 9), then click **Next**.

#### Figure 9: Policy Conditions (Completed)

Remote Access Policy Wizard	
Policy Conditions To be authenticated, connection requests must match the conditions you specify.	Ŷ
Specify the conditions that connection requests must match to be granted or deni access.	ed
Policy conditions:	
Client-Friendly-Name matches "group01"	
0,0 0,000 R1	
Add Edit <u>R</u> emove	
Distance in the second s	Concel

• The Permissions screen appears (Figure 10).

#### Figure 10: Permissions

New Remote Access Policy Wizard	×
Permissions A remote access policy can either grant or deny access to users who match the specified conditions.	ŷ
If a connection request matches the specified conditions: $\bigcirc \ \underline{D}$ env remote access permission	
C Grant remote access permission	
< Back Next >	Cancel

- Select Grant remote access permission, and click Next.
- The Profile screen appears (Figure 11).

Figure 11: Profile

New Remote Access Policy Wizard	×
Profile You can make changes to the profile for this policy.	Ŷ
A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile.	
<u>E</u> dit Profile	
< <u>B</u> ack <u>Next</u> → Canc	;el

- Click Edit Profile, and do the following:
- On the Authentication tab (Figure 12), select **Unencrypted authentication** and deselect everything else.
- **Note:** By default all passwords are encrypted by the RADIUS protocol. Choosing the unencrypted authentication here is simply for tunneling into the IAS server.

dit Dial-in Profile		<u>? ×</u>
Dial-in Constraints	IP	Multilink
Authentication	Encryption	Advanced
Select the authentication m	ethods you want to allo	w for this connection.
EAP Methods		
Microsoft Encrypted.	Authentication version <u>2</u>	(MS-CHAP v2)
🔲 User can <u>c</u> har	ige password after it has	expired
Microsoft Encrypted.	Authentication (MS-CHA	P)
🔲 Uger can char	ige password after it has	expired
Encrypted authentica	ation (CHAP)	
Unencrypted authen	tication (PAP, SPAP)	
Unauthenticated access		
Allow clients to conn method.	ect without negotiating a	an authentication
	ок с	Cancel Apply

Figure 12: Edit Profile: Authentication

On the Encryption tab (Figure 13), select **No encryption** and deselect everything else.

dit Dial-in Profile		<u>? ×</u>	
Dial-in Constraints	IP IP	Multilink	
Authentication	Encryption	Advanced	
The following encryption lev Routing and Remote Access make sure the encryption le If No encryption is the only- using data encryption.	vels are supported by serv ss. If you use a different re vvels you select are suppo option selected, then use	ers running Microsoft mote access server, rted by that software. 's cannot connect by	
Basic encryption (MPF	°E 40-bit)		
Strong encryption (MPPE 56 bit)			
Strongest encryption (MPPE 128 bit)			
✓ No encryption			
	OK Ca	ncel Apply	

Figure 13: Edit Profile: Encryption

- On the Advanced tab (Figure 14), select **Framed-Protocol** and click **Remove**.
- Then select **Service-Type** and click **Edit** (Figure 14). **Figure 14: Edit Profile: Advanced**

Ec	lit Dial-in Profile			? ×
	Dial-in Constraints Authentication	IP Encryption	) Multilink Advanced	
	Specify additional connection Access server.	attributes to be return	ned to the Remote	
	Attrigutes: Name Service-Type Framed-Protocol	Vendor RADIUS Standard RADIUS Standard	Value Framed PPP	-
	▲	<u>R</u> emove	<u>.</u>	
		OK (	Cancel Apply	,

• The Enumerable Attribute Information screen appears (Figure 15).

Enumerable Attribute Information		? ×
Attribute name:		
Service-Type		
Attribute number:		
6		
Attribute format:		
Enumerator		
<u>Attribute value:</u>		
Administrative		
	OK	Cancel

#### Figure 15: Enumerable Attribute Information

- In the Attribute value list, select **Administrative** and click **OK**. The Administrative attribute grants full read-write access to the PS Series group.
- You return to the Edit Profile: Advanced screen, **w**hich should now look like Figure 16.

Figure 16: Edit Profile: Advanced (Modified)

Ec	Edit Dial-in Profile	? ×
	Dial-in Constraints IP Authentication Encryption	Multilink Advanced
	Specify additional connection attributes to be return Access server.	ed to the Remote
	Attri <u>b</u> utes:	
	Name Vendor Service-Type RADIUS Standard	Value Administrative
	▼	
	Add <u>E</u> dit <u>R</u> emove	
	OK C	ancel <u>Apply</u>

Leaving this screen visible, continue with Adding the PS Series Vendor-Specific Attributes.

#### Adding the EqualLogic Vendor-Specific Attributes

The following procedure continues from Creating Network Policies on the NPS Server, and assumes the Edit Dial-In Profile screen is still displayed.

To add vendor-specific attributes for EqualLogic:

• On the Edit Dial-In Profile – Advanced tab, click Add.

 In the Add Attribute dialog box (Figure 17), select Vendor-Specific and click Add.

dd Athuib

To add an attribute that is not listed, s	select the Vendor-Specific attr	ibute.
Attri <u>b</u> ute:		
Name	Vendor	Description
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.
Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.
Vendor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.
Allowed-Certificate-OID	Microsoft	Specifies the certificate purpose or usage object identifiers
Generate-Class-Attribute	Microsoft	Specifies whether IAS automatically generates the class at
Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session
Ignore-User-Dialin-Properties	Microsoft	Specifies that the user's dial-in properties are ignored.
MS-Quarantine-IPFilter	Microsoft	Specifies the IP traffic filter that is used by the Routing and
MS-Quarantine-Session-Timeout	Microsoft	Specifies the time (in seconds) that the connection can rer
Tunnel-Tag	Microsoft	Description not yet defined
USR-ACCM-Type	U.S. Robotics, Inc.	Description not yet defined
USR-AT-Call-Input-Filter	U.S. Robotics, Inc.	Description not yet defined
USR-AT-Call-Output-Filter	U.S. Robotics, Inc.	Description not yet defined
USR-AT-Input-Filter	U.S. Robotics, Inc.	Description not yet defined
USR-AT-Output-Filter	U.S. Robotics, Inc.	Description not yet defined
USR-AT-RTMP-Input-Filter	U.S. Robotics, Inc.	Description not yet defined
USR-AT-RTMP-Output-Filter	U.S. Robotics, Inc.	Description not yet defined
•		•

#### Figure 17: Add Attribute

2 1

• In the Multivalued Attribute Information dialog box (Figure 18), click Add.

Figure 18: Multivalued Attribute Information

Multivalued Attribute	Information		? >
Attribute name:			
Vendor-Specific			
Attribute purpher:			
26			
1			
Attribute format:			
UctetString			
A <u>t</u> tribute values:			
Vendor	Value		Move <u>U</u> p
			Move <u>D</u> own
			<u>Add</u>
			<u>R</u> emove
			<u>E</u> dit
•		F	
		0K.	Cancel

• In the Vendor-Specific Attribute Information dialog box (Figure 19), do the following:

- Select **Enter Vendor Code**, and enter **12740** in the field. This is the vendor code for EqualLogic, Inc.
- Select Yes, It conforms, then click Configure Attribute.

Figure 19: Vendor-Specific Attribute Inform	nation
---	--------

Vendor-Specific Attribute	Information	? X
Attribute name:		
Vendor-Specific		
Specify network access serve	er vendor.	
○ <u>S</u> elect from list:	RADIUS Standard	7
Enter Vendor Code:	12740	
Specify whether the attribute overdor specific attributes. • Yes. It conforms. No. It does not conform. Configure Attribute	conforms to the RADIUS RFC specific	ation for
	OK Ca	ncel

• The Configure VSA dialog box is displayed (Figure 20).

Figure 20: Configure VSA

Configure VSA (RFC compliant)	<u>? ×</u>
⊻endor-assigned attribute number: 6	
Attribute format: Decimal	
Attribute value:	
	OK Cancel

- Enter the following information for the EQL-Admin attribute:
  - In the Vendor-assigned attribute number field, enter 6.
  - In the Attribute format drop-down list, select **Decimal**.
  - In the Attribute value field, enter **0** (for a group administrator).
- Click **OK**.
- Continue to close windows until you reach the Edit Dial-in Profile screen.
- On the Advanced tab (Figure 21), verify the information is correct, then click **OK**.

lit Dial-in Profile			?)
Dial-in Constraints	Í IP	Multilink	
Authentication	Encryption	Advanced	
Specify additional connectio Access server. Attri <u>b</u> utes:	n attributes to be retur	ned to the Remote	
Name	Vendor	Value	_
Service-Type Vendor-Specific	RADIUS Standard RADIUS Standard	Administrative 0	
A <u>d</u> d <u>E</u> dit	<u>R</u> emove		

Figure 21: Edit Dial-In Profile: Advanced (with new VSA)

• The Dial-in Settings confirmation box is displayed (Figure 22), asking if you want to view online help about protocol configuration. Click **No**.

#### Figure 22: Dial-In Settings

Dial-in Se	ttings
⚠	You selected one or more authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.
	View the corresponding Help topic?
	<u>[Xes</u> ]No

• On the Profile screen (Figure 23), click **Next**.

Figure 23: Profile

Remote Access Policy Wizard	
Profile You can make changes to the profile for t	his policy.
A profile is a collection of settings applied authenticated. To review or change the d	to connection requests that have been efault profile for this policy, click Edit Profile.
Edit Profile	

• On the Completing the New Remote Access Policy Wizard screen (Figure 24), click **Finish**.

New Remote Access Policy W	izard	×
	Completing the New Remote Access Policy Wizard You have successfully completed the New Remote Access Policy Wizard. You created the following policy: EQL Group Administrators Conditions: Service-Type matches "Administrative" AND Client-Friendly-Name matches "eng1-grp" The policy was set up manually.	
	To close this wizard, click Finish.	
	< <u>B</u> ack Finish Cance	

Figure 24: Completing the Wizard

#### APPENDIX B: CONFIGURING RADIUS ON THE PS SERIES GROUP USING CLI

To configure the PS Series group using the command-line interface log in to the Command Line Interface for the group using the group IP address and a group administrator account, such as grpadmin.

Enter the following command to enable RADIUS logins: grpparams login-radius-auth enable

Enter the following command to add the IP address of the RADIUS server (or servers), separated by commas and no spaces. The servers will be consulted in the order they are listed.

```
grpparams radius-auth-list 123.45.6.789,234.5.67.89
```

Enter the following command to add the password (secret) you configured in Overview of Steps

grpparams radius-auth-secrets secret

Optionally, enter the following command to disable the requirement for the EQL-Admin RADIUS return attribute. Disabling this requirement treats every user who attempts to log in as though they have group administration permission; effectively, this allows unrestricted logins from all users in the RADIUS database to the PS Series group (and is not recommended).

```
grpparams login-radius-attr disable
```

Optionally, enter the following command to increase the timeout interval for login attempts through the RADIUS server. The default is 2 seconds. Increase the timeout interval if you are having performance issues with login requests.

```
grpparams radius-auth-timeout 5
```

Optionally, enter the following command to increase the allowed number of login retries before blocking the user from logging in again interval for login attempts through the RADIUS server. The default is 2 seconds. Increase the timeout interval if you are having performance issues with login requests.

```
grpparams radius-auth-retries 3
```

Optionally, verify your RADIUS settings by running the following command and checking the output:

#### TECHNICAL SUPPORT AND CUSTOMER SERVICE

Dell's support service is available to answer your questions about PS Series SAN arrays. If you have an Express Service Code, have it ready when you call. The code helps Dell's automated-support telephone system direct your call more efficiently.

#### **Contacting Dell**

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services might not be available in your area.

For customers in the United States, call 800-945-3355.

Note: If you do not have access to an Internet connection, contact information is printed on your invoice, packing slip, bill, or Dell product catalog.

Use the following procedure to contact Dell for sales, technical support, or customer service issues:

- 1. Visit support.dell.com or the Dell support URL specified in information provided with the Dell product.
- 2. Select your locale. Use the locale menu or click on the link that specifies your country or region.
- 3. Select the required service. Click the "Contact Us" link, or select the Dell support service from the list of services provided.
- 4. Choose your preferred method of contacting Dell support, such as e-mail or telephone.

#### **Online Services**

You can learn about Dell products and services using the following procedure:

- 1. Visit www.dell.com (or the URL specified in any Dell product information).
- 2. Use the locale menu or click on the link that specifies your country or region