



USING ACTIVE DIRECTORY FOR ACCOUNT AUTHENTICATION TO A PS SERIES GROUP

ABSTRACT

This Technical Report describes how to configure Internet Authentication Service to leverage accounts in Active Directory to control login authentication to a PS Series Group.

Copyright © 2008 EqualLogic, Inc.

Jan 2008

EqualLogic is a registered trademark of EqualLogic, 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.

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

PS Series Firmware Version 3.2

Table of Contents

Revision Information	4
Introduction.....	5
Overview of Steps	5
Installing and Configuring Internet Authentication Service (IAS).....	5
Configuring a PS Series Group as a RADIUS Client on the IAS Server	6
Creating Remote Access Policies on the IAS Server	7
Adding the EqualLogic Vendor-Specific Attributes	14
Managing SAN Administrators With Active Directory Groups.....	19
Creating a New Active Directory Group for PS SAN Administrators.....	19
Adding the Active Directory Group to the Remote Access Policy	21
Configuring the PS Series Group.....	22
Using the Group Manager GUI	22
Using the CLI	24
Appendix A.....	26
EqualLogic Documentation and Customer Support	30

REVISION INFORMATION

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

Report	Date	Document Revision
1.0	Jan, 2008	Initial Release

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

Vendor	Model	Software Revision
Microsoft®	Windows® Server 2003 R2	Service Pack 1
EqualLogic	PS Series Firmware	Version 3.2 and higher

All EqualLogic Technical Reports are available on the Customer Support site at:

<https://www.equallogic.com/support/>

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 a server running Internet Authentication Service (IAS) as a connector between the PS Series SAN and Active Directory.

This paper describes the setup of Windows IAS service 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 includes steps to configure IAS by creating a Remote Access Policy that grants full, group-wide administrative privilege to the PS Series group. In Active Directory, you assign users to a new AD group to grant SAN management privileges to individual users.

In addition, remote access policies can be created to authorize pool-only or read-only administrators if desired.

Overview of Steps

The major tasks involved are as follows:

1. Install and configure IAS. See *Installing and Configuring Internet Authentication Service (IAS)*.
2. Configure the PS Series group as a RADIUS client to IAS. See *Configuring a PS Series Group as a RADIUS Client on the IAS Server*.
3. Create a Remote Access Policy in Active Directory that grants administrator privilege to a PS Series group. You need to add two required vendor-specific attributes for EqualLogic to the new policy. See *Creating Remote Access Policies on the IAS Server*.
4. 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 Remote Access Policy will be applied. See *Managing SAN Administrators With Active Directory Groups*.
5. .
6. Configure the PS Series group to recognize and accept login attempts from the RADIUS server. See *Configuring the PS Series Group*.

The following sections describe each of these tasks in detail.

INSTALLING AND CONFIGURING INTERNET AUTHENTICATION SERVICE (IAS)

This section covers installing IAS. We recommend running IAS 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 2003 domain, or that the IAS server can proxy to another IAS server with domain access to Active Directory.

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:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.

3. In the Windows Components dialog box, select **Networking Services**, then click **Details**.
4. In the Networking Services dialog box, check the box for **Internet Authentication Service**, then click **OK**.
5. You return to the Windows Components dialog box. Click **Next**.
6. On the Completing the Windows Components Wizard screen, click **Finish**.

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

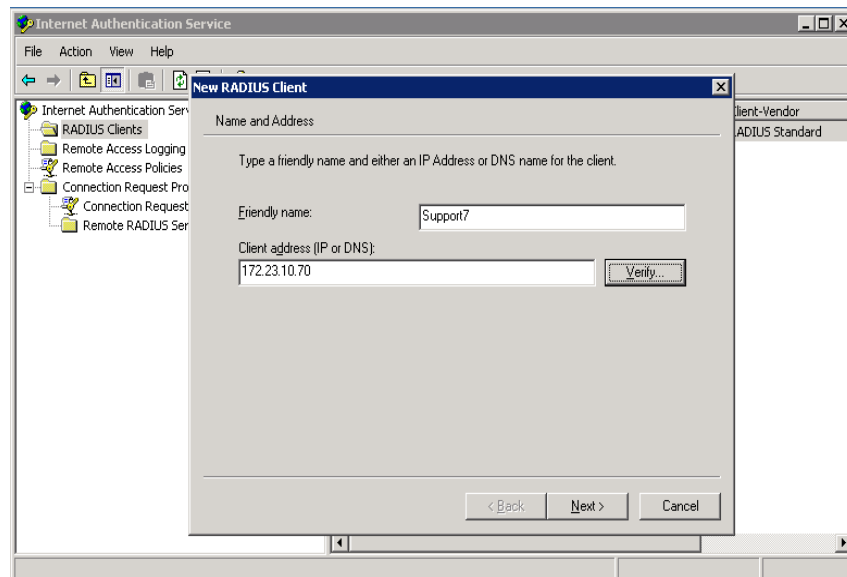
1. Click **Start > Administrative Tools > Internet Authentication Services**.
2. In the Internet Authentication Services console, right-click **Internet Authentication Service (Local)**, then click **Register Server in Active Directory**. This setting allows the IAS Server to authenticate users in the Active Directory domain.
3. 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:

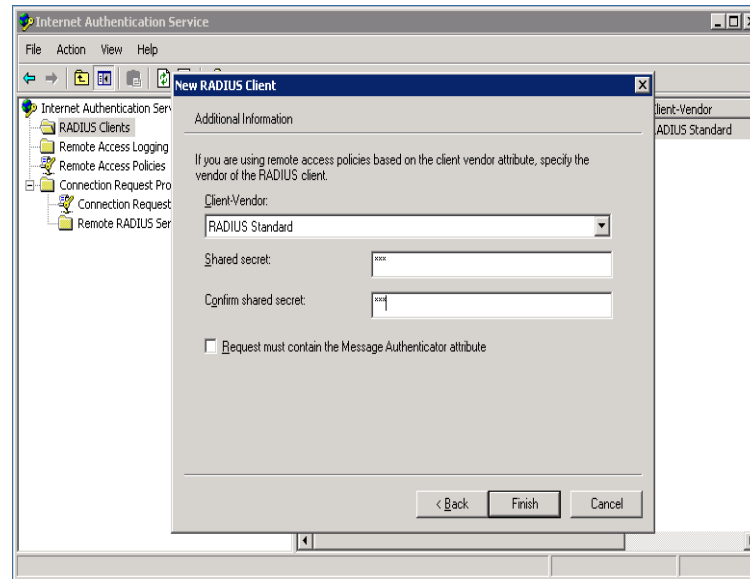
1. Click **Start > Administrative Tools > Internet Authentication Service**.
2. Right-click the **RADIUS Clients** folder.
3. Click **New > RADIUS Client**.

Figure 1: New RADIUS Client



4. 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.)
5. Click **Next**. The Additional Information dialog box is displayed.

Figure 2: New RADIUS Client – Additional Information



6. 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.
7. Click **Finish**.

Creating Remote Access Policies on the IAS Server

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.

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.

You must create an access policy for each type of account configured on the PS Series group. All PS Series Firmware versions support group administrator accounts and read-only accounts. In PS Series Firmware Version 3.2, you can also create a new type of account for pool administrators. 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). For more information on pool administrators, see the Group Administration guide.

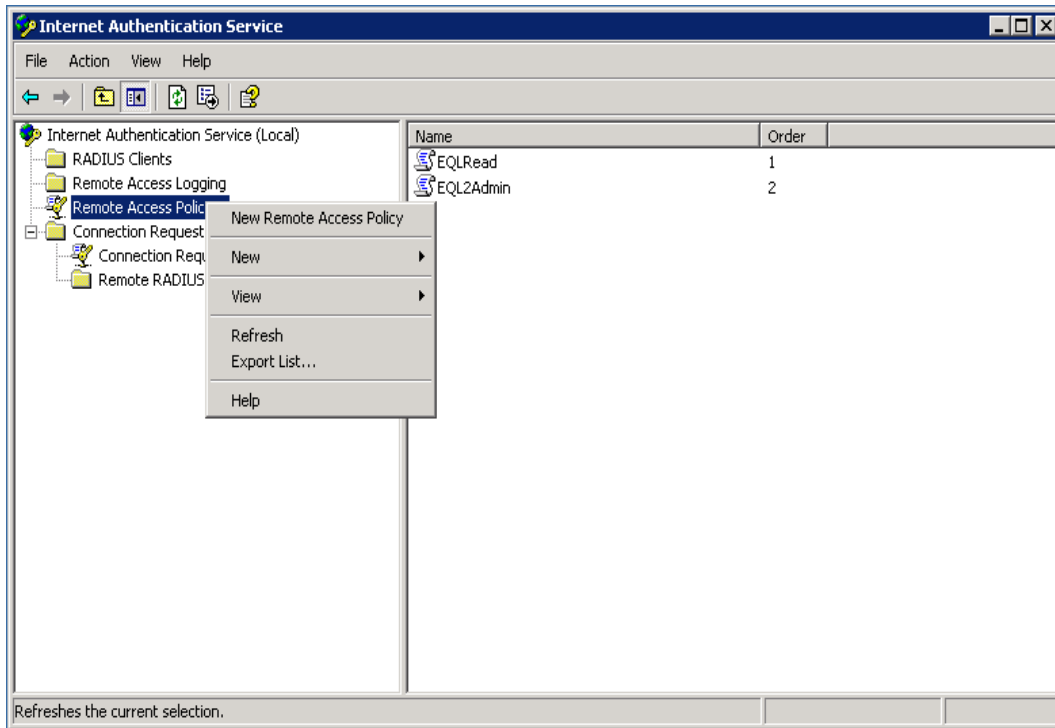
This section describes creating a Remote Access Policy for group administrators (those with full, group-wide privileges). See Appendix A for information on other types of account policies.

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

1. Click **Start > Administrative Tools > Internet Authentication Service**.

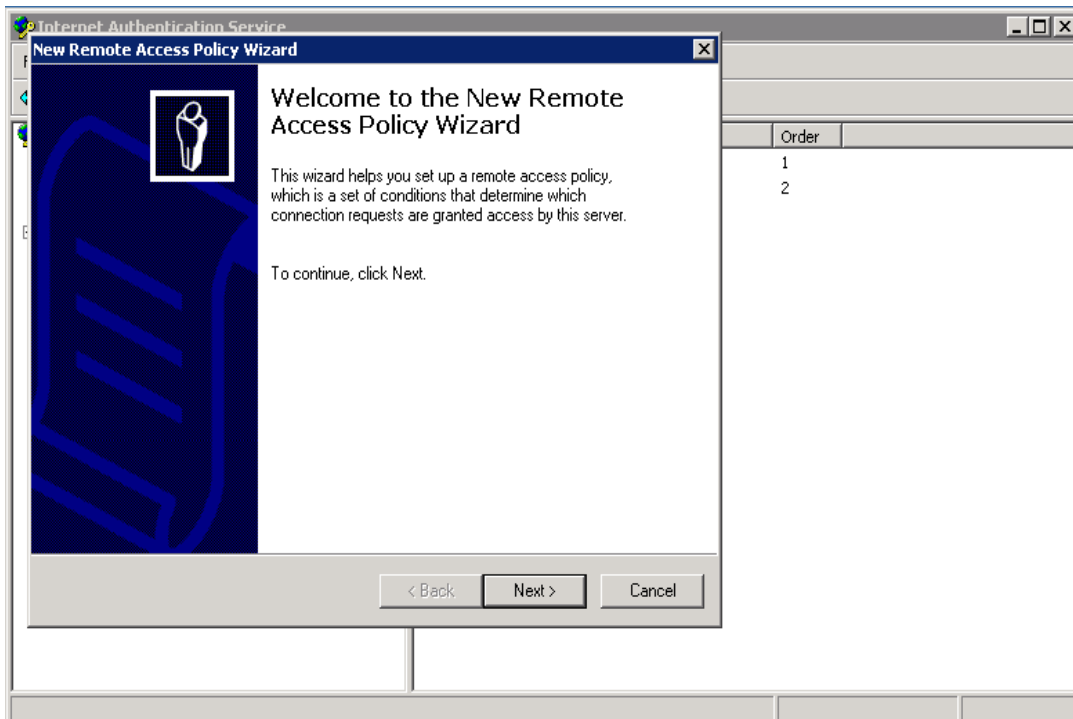
2. Right-click **Remote Access Policy**, and click **New Remote Access Policy** (Figure 3).

Figure 3: IAS – Create New Remote Access Policy



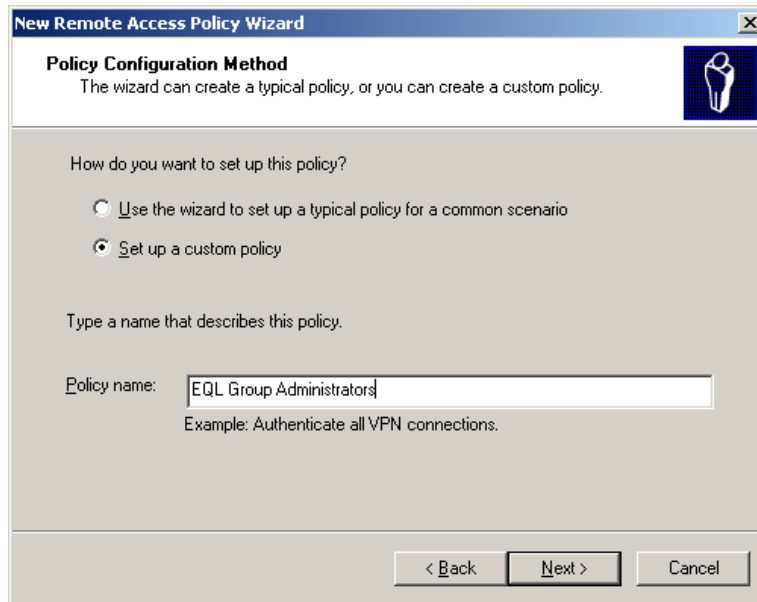
The New Remote Access Policy Wizard starts (Figure 4).

Figure 4: New Remote Access Policy Wizard



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

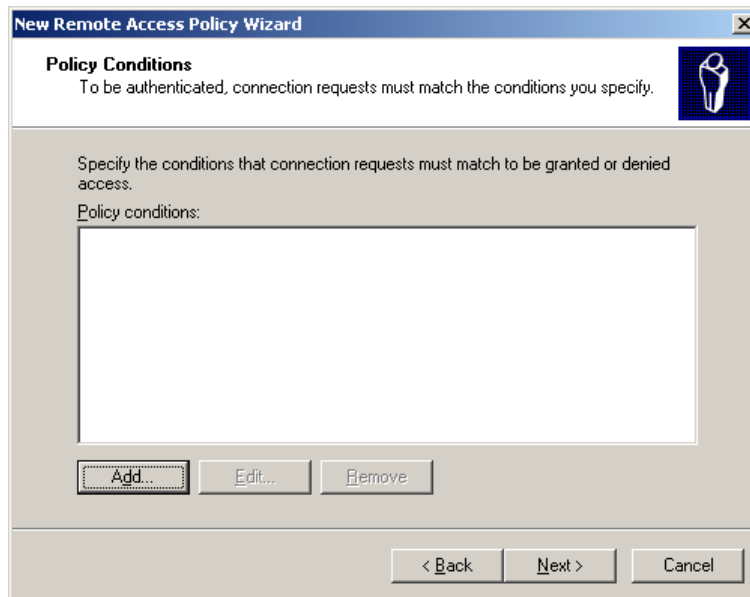
Figure 5: Policy Configuration Method



4. 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).

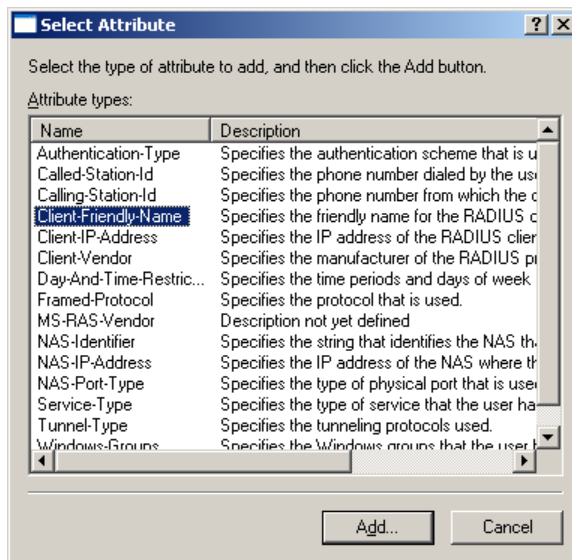
Figure 6: Policy Conditions



5. Under the Policy Conditions field, click **Add**.

The Select Attribute screen appears (Figure 7).

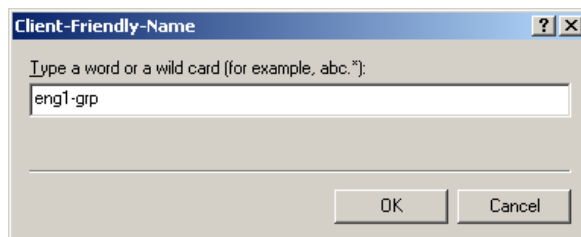
Figure 7: Select Attribute



6. Select **Client-Friendly-Name** and click **Add**.

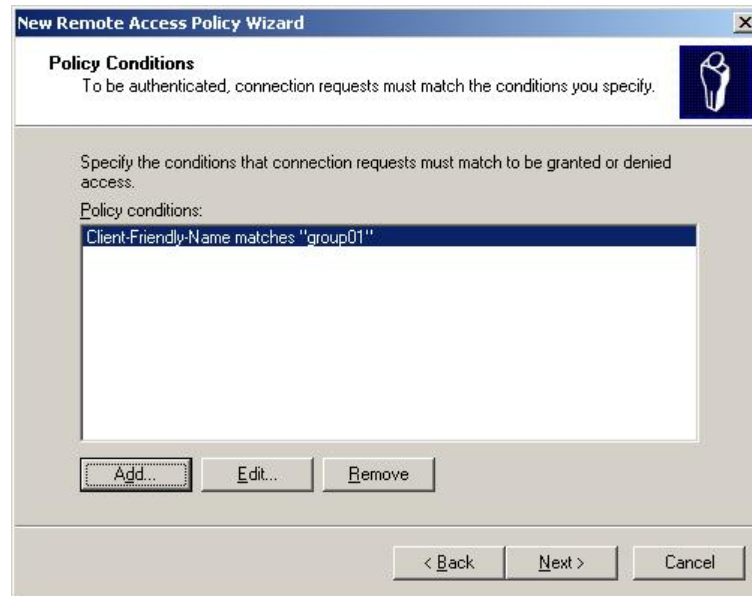
The Client-Friendly Name screen appears (Figure 8).

Figure 8: Client-Friendly Name



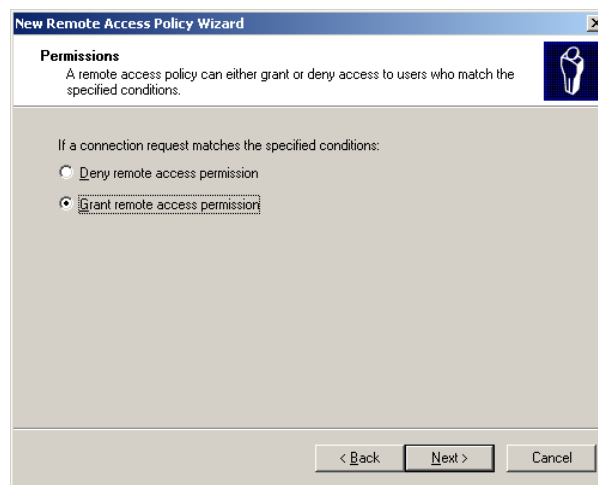
7. Enter the PS Series group name you specified in Overview of Steps
8. Verify the information is correct in the Policy conditions list (Figure 9), then click **Next**.

Figure 9: Policy Conditions (Completed)



The Permissions screen appears (Figure 10).

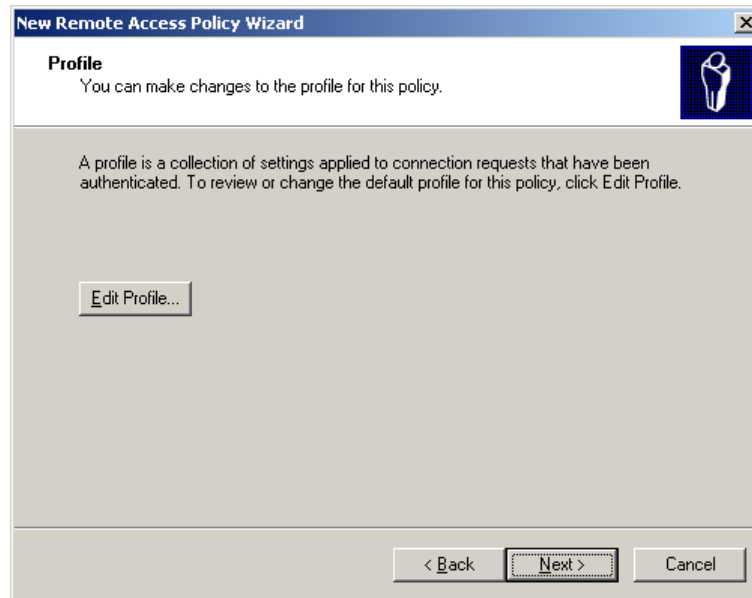
Figure 10: Permissions



9. Select **Grant remote access permission**, and click **Next**.

The Profile screen appears (Figure 11).

Figure 11: Profile

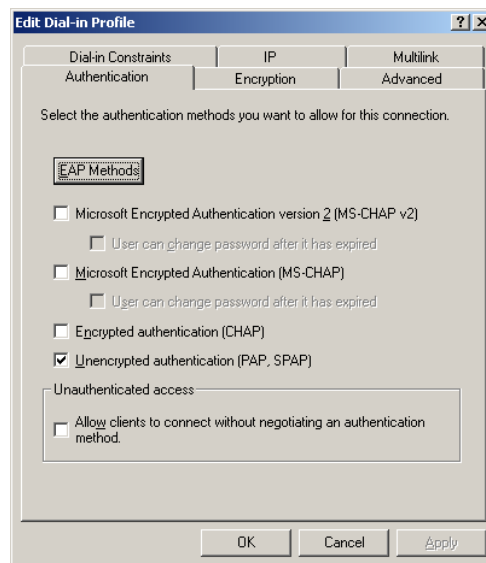


10. Click **Edit Profile**, and do the following:

- On the Authentication tab (Figure 12), select **Unencrypted authentication** and deselect everything else.

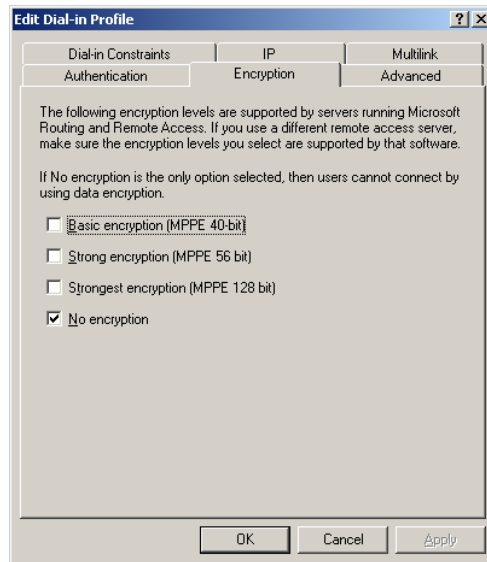
Note: By default all passwords are encrypted by the RADIUS protocol. Choosing the unencrypted authentication here is simply for tunneling into the IAS server.

Figure 12: Edit Profile: Authentication



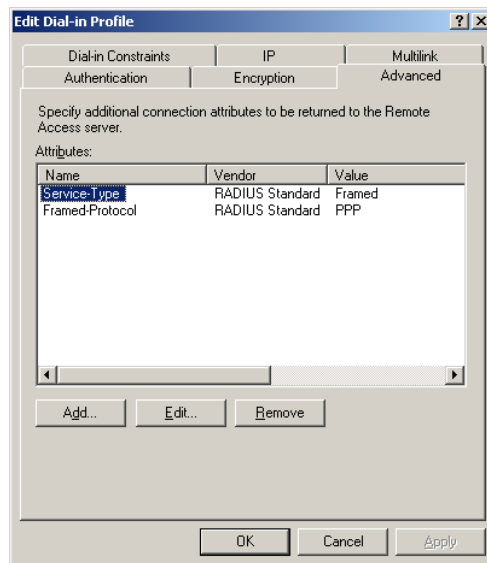
- On the Encryption tab (Figure 13), select **No encryption** and deselect everything else.

Figure 13: Edit Profile: Encryption



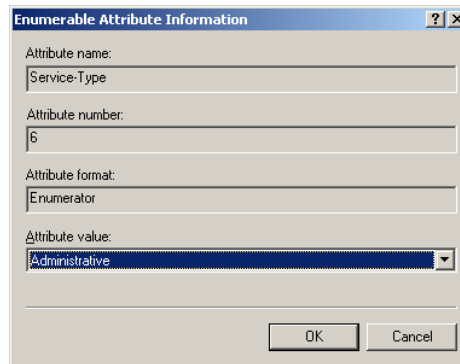
- On the Advanced tab (Figure 14), select **Framed-Protocol** and click **Remove**.
- Then select **Service-Type** and click **Edit** (Figure 14).

Figure 14: Edit Profile: Advanced



The Enumerable Attribute Information screen appears (Figure 15).

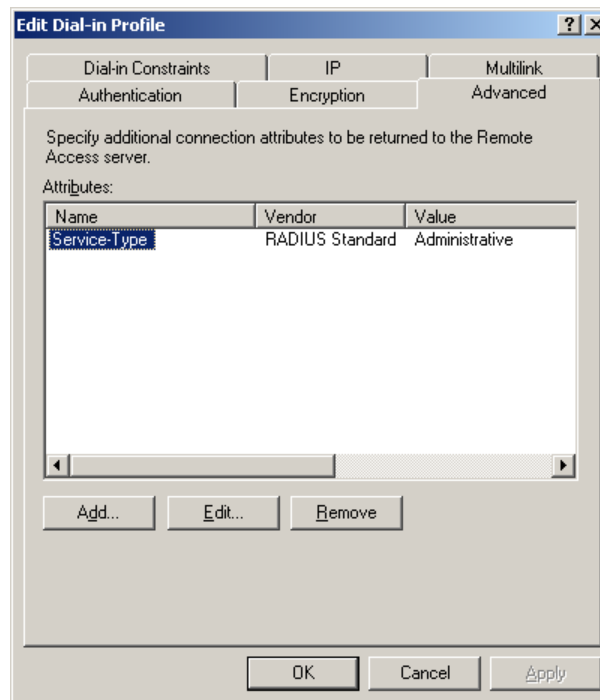
Figure 15: Enumerable Attribute Information



11. 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, which should now look like Figure 16.

Figure 16: Edit Profile: Advanced (Modified)



12. Leaving this screen visible, continue with Adding the EqualLogic Vendor-Specific Attributes.

Adding the EqualLogic Vendor-Specific Attributes

Vendor-specific attributes tailor the remote access policy to the vendor. For EqualLogic, 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

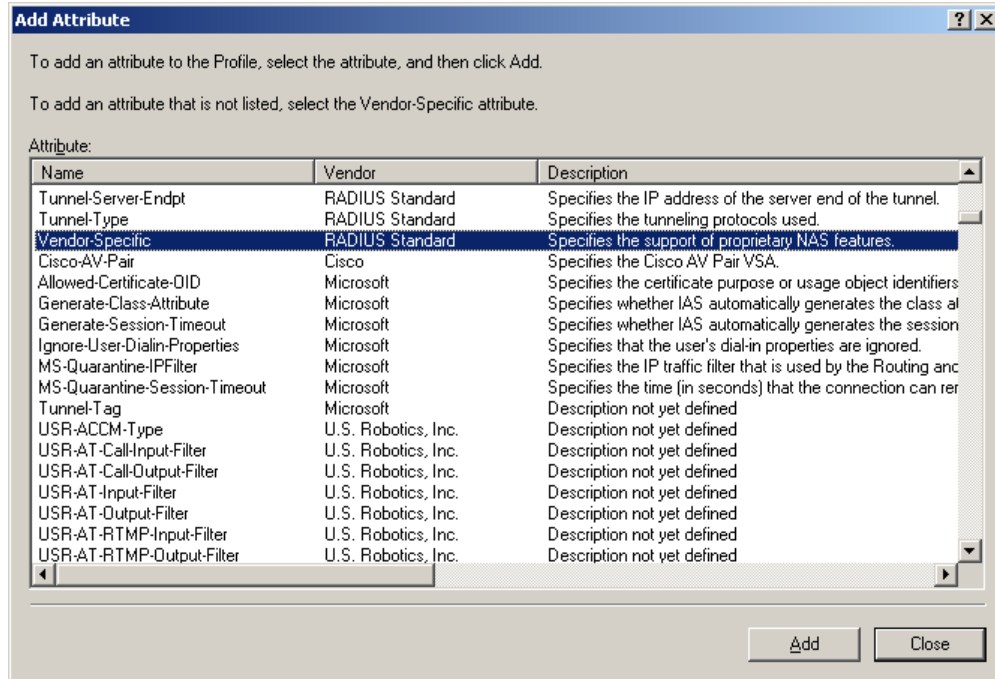
GUI for each contact. Every time a user logs in, their information will be updated if it has changed since the last login.

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

To add vendor-specific attributes for EqualLogic:

1. On the Edit Dial-In Profile – Advanced tab, click **Add**.
2. In the Add Attribute dialog box (Figure 17), select **Vendor-Specific** and click **Add**.

Figure 17: Add Attribute



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

Figure 18: Multivalued Attribute Information

Multivalued Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value
--------	-------

Move Up
Move Down
Add
Remove
Edit

OK Cancel

4. 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 Information

Vendor-Specific Attribute Information

Attribute name:
Vendor-Specific

Specify network access server vendor.

Select from list: RADIUS Standard

Enter Vendor Code: 12740

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

Yes. It conforms.

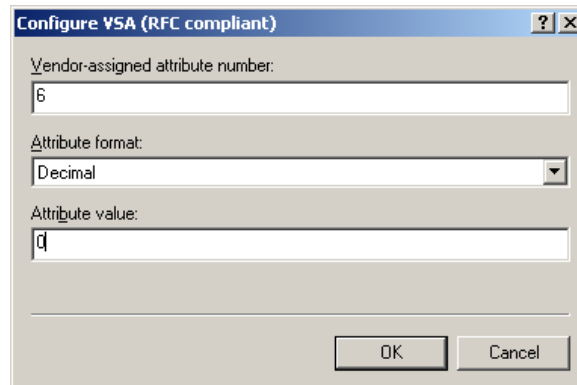
No. It does not conform.

Configure Attribute...

OK Cancel

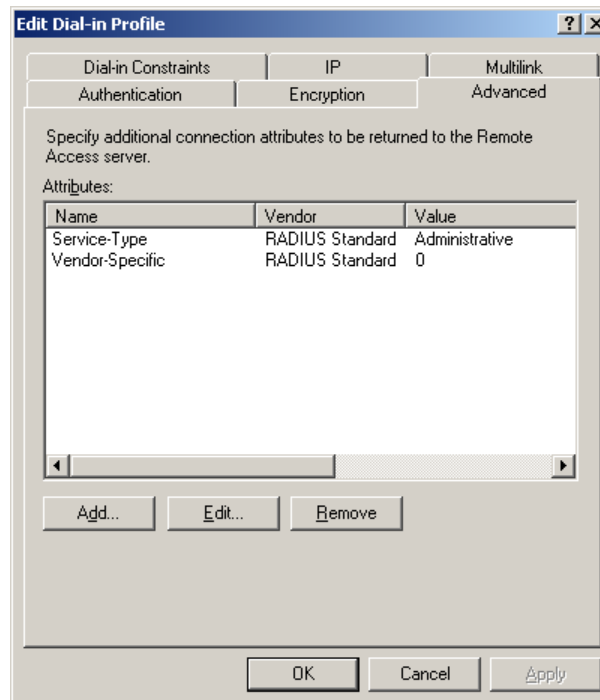
The Configure VSA dialog box is displayed (Figure 20).

Figure 20: Configure VSA



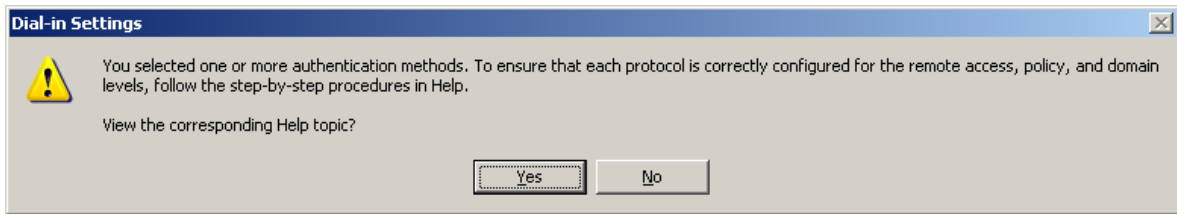
5. Enter the following information for the EQL-Admin attribute:
 - In the Vendor-assigned attribute number field, enter **6**.
 - In the Attribute format drop-down list, select **Decimal**.
 - In the Attribute value field, enter **0** (for a group administrator).
6. Click **OK**.
7. Continue to close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

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



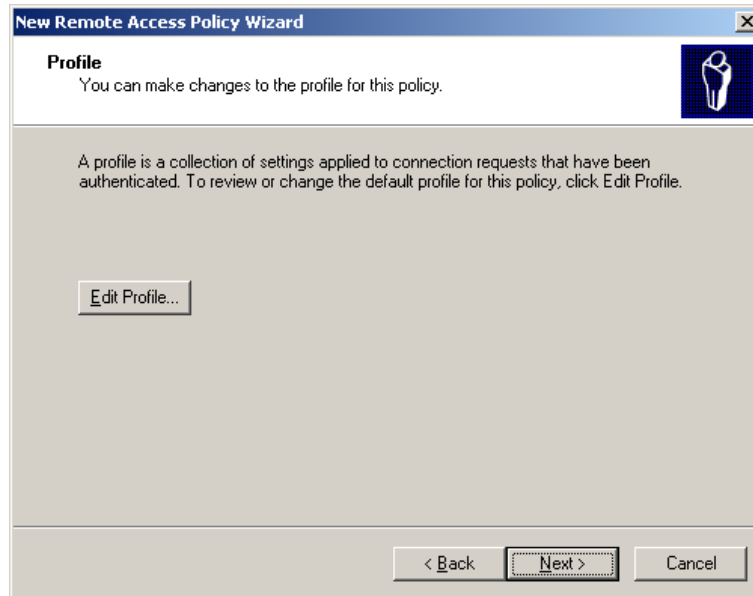
9. The Dial-in Settings confirmation box is displayed (Figure 22), asking if you want to view online help about protocol configuration. Click **No**.

Figure 22: Dial-In Settings



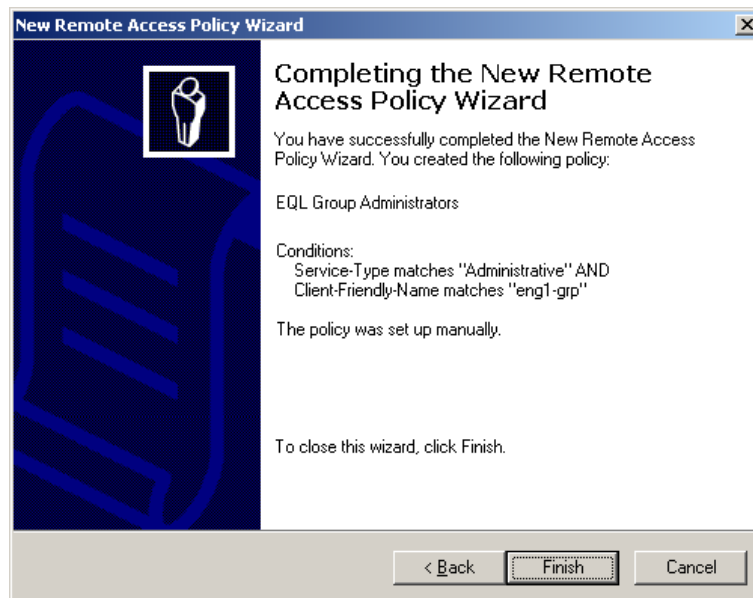
10. On the Profile screen (Figure 23), click **Next**.

Figure 23: Profile



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

Figure 24: Completing the Wizard

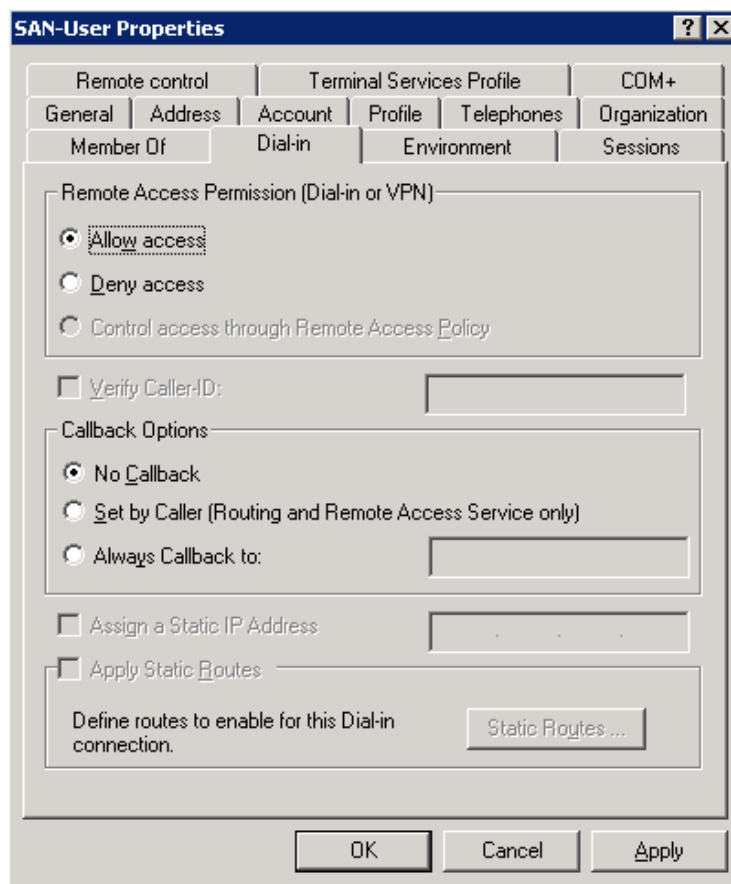


MANAGING SAN ADMINISTRATORS WITH ACTIVE DIRECTORY GROUPS

Once you have configured your IAS server, you can give users permissions to access the PS Series SAN. It is recommended that you create a new Active Directory group 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.

Note: This section assumes your domain is or has been raised to Windows Server 2003 functional level. If you are currently running in mixed mode you will have to **allow** each user Remote Access Permission (Figure 25).

Figure 25: Adding Remote Access Permissions (Mixed mode domain)

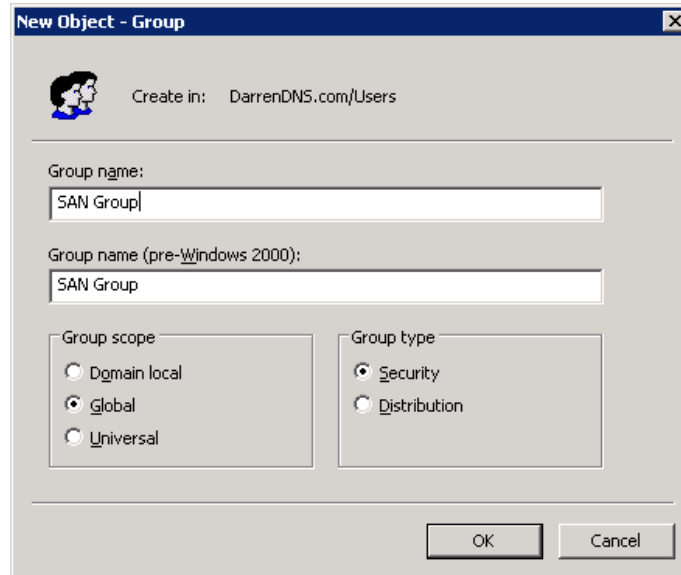


Creating a New Active Directory Group for PS SAN Administrators

To add a new group and add users to that group:

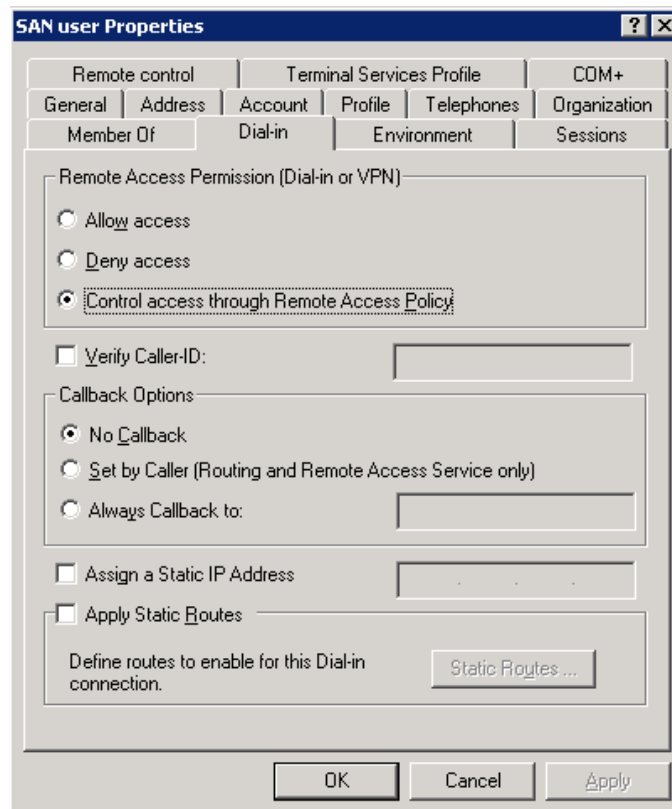
- 1) Open the Using Active Directory Users and Computers panel and create a new group to manage SAN Administrators (Figure 26).

Figure 26: New Group



- 2) 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 Remote Access Policy** (Figure 27).

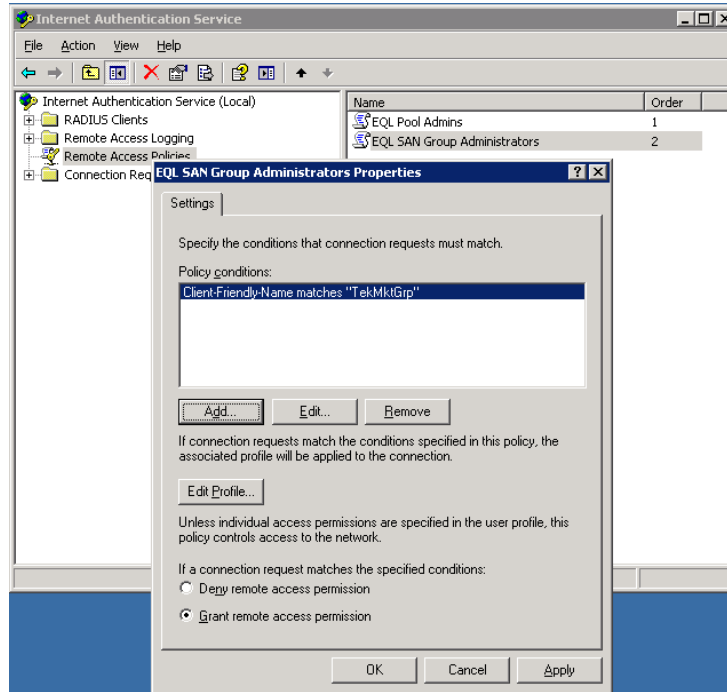
Figure 27: Remote Dial-in Properties



Adding the Active Directory Group to the Remote Access Policy

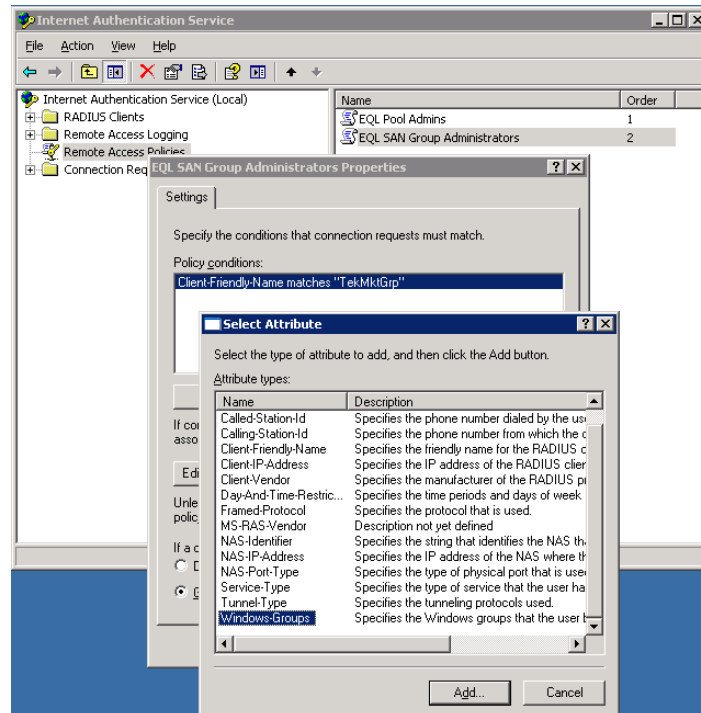
- 3) Add the Active Directory group to the Remote Access Policy settings by opening the properties of the policy within IAS and clicking the **Add** button (Figure 28).

Figure 28: Policy Properties



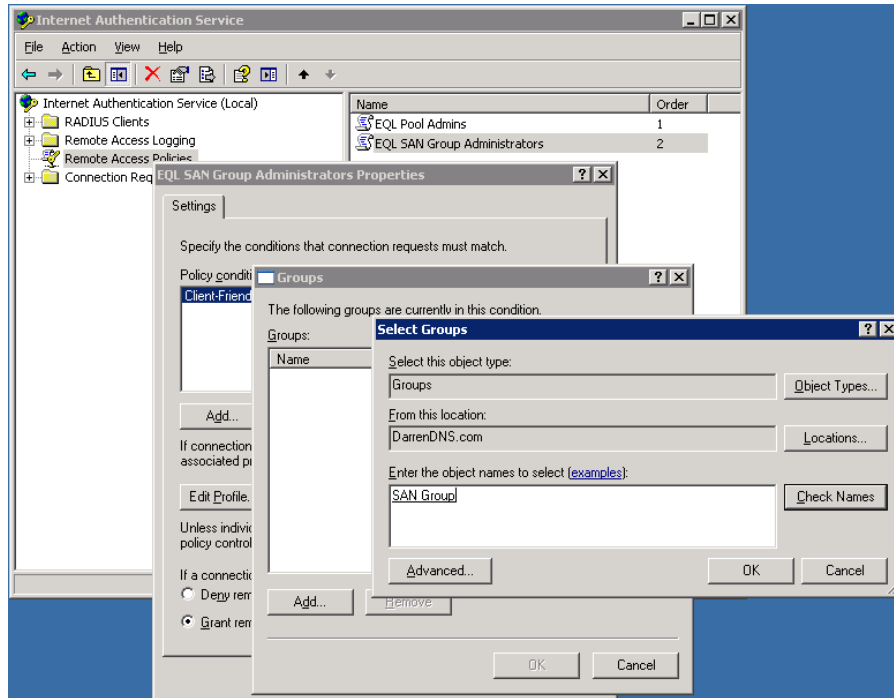
- 4) Add a policy condition for **Windows-Groups** and click **Add** (Figure 29).

Figure 29: Adding Windows Group to the Remote Access Policy



- In the Groups window click the **Add** button and add the group to the Select Groups window (Figure 30).

Figure 30: Groups Dialog Window



- Click **OK** to confirm the selection and complete the Remote Access Policy change.

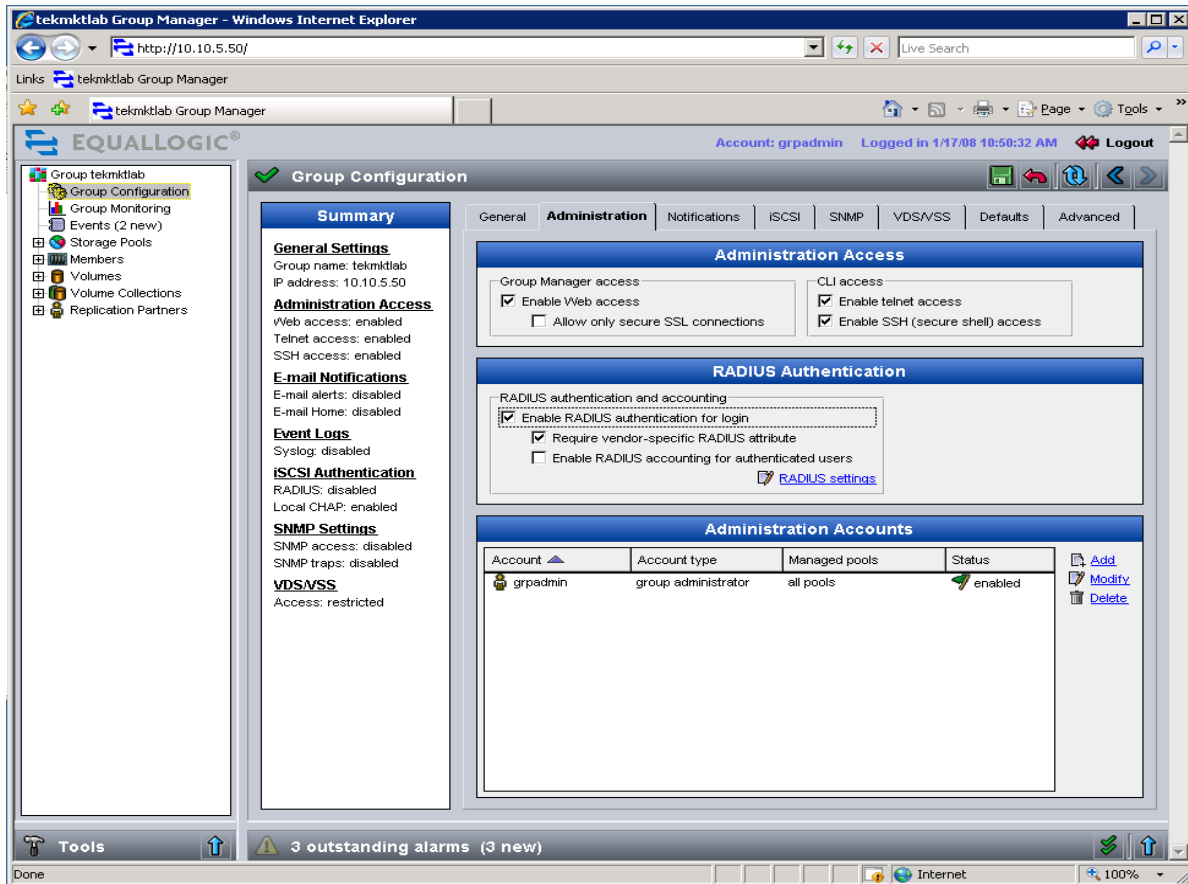
CONFIGURING THE PS SERIES GROUP

After you finish creating the Remote Access Policy to allow your administrators to connect to the PS Series SAN (or SANs), you must configure the PS Series groups to recognize and allow login attempts from the RADIUS authentication server. You can use either the Group Manager GUI or the CLI to configure the group. Both procedures are provided.

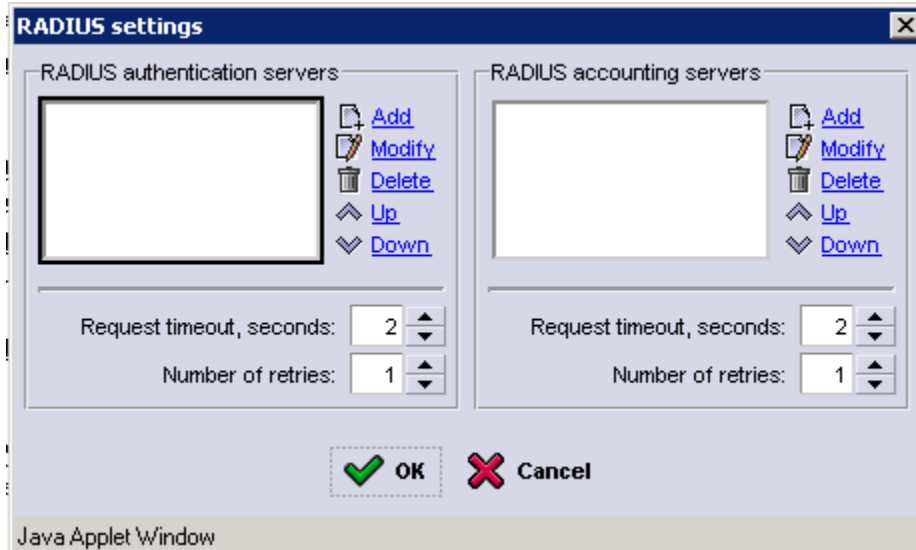
Using the Group Manager GUI

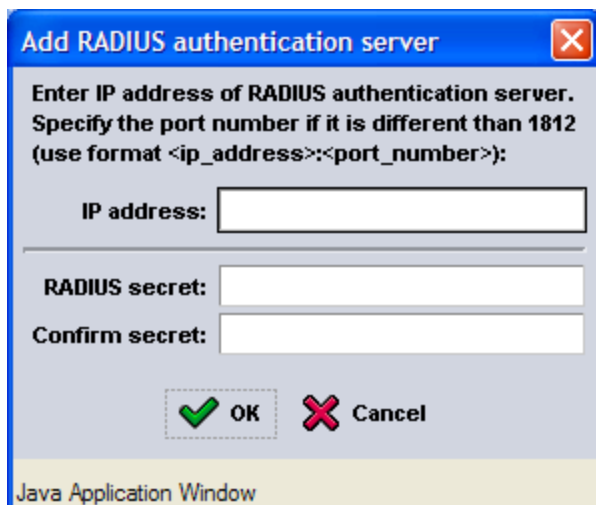
To configure the group using the Group Manager GUI:

- Log in to the Group Manager GUI.
- Click **Group Configuration > Administration** tab.



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





7. Enter the IP address for the RADIUS authentication server, and enter and confirm a secret. Click **OK**.
8. Adjust the Request timeout value and Number of retries value in the RADIUS settings dialog window as desired. Click **OK**.
9. Finally, confirm and save all settings by clicking the floppy disk icon in the group manager interface.

Using the CLI

To configure the PS Series group using the command-line interface:

1. Log in to the Command Line Interface for the group using the group IP address and a group administrator account, such as grpadmin.
2. Enter the following command to enable RADIUS logins:

```
grpparams login-radius-auth enable
```
3. 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
```
4. Enter the following command to add the password (secret) you configured in Overview of Steps

```
grpparams radius-auth-secrets secret
```
5. 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
```
6. 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
```
7. 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
```

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

```
grpparams show
```

```
.  
.   
.
```

```
_____ Radius Information _____  
radius-auth-list:                login-radius-auth: enabled  
radius-auth-retries: 3           radius-auth-timeout: 5secs  
login-radius-acct: disabled      radius-acct-retries: 1  
radius-acct-timeout: 2secs       iscsi-radius-auth: disabled  
iscsi-local-auth: enabled        radius-acct-list:  
login-radius-attr: enabled       radius-auth-secrets:  
radius-acct-secrets:
```

APPENDIX A

This appendix describes how to create remote access policies for pool administrators or read-only monitors.

As of PS Series Firmware Version 3.2, you can create pool administrators. 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 IAS server specific to each type of pool administration account you need.

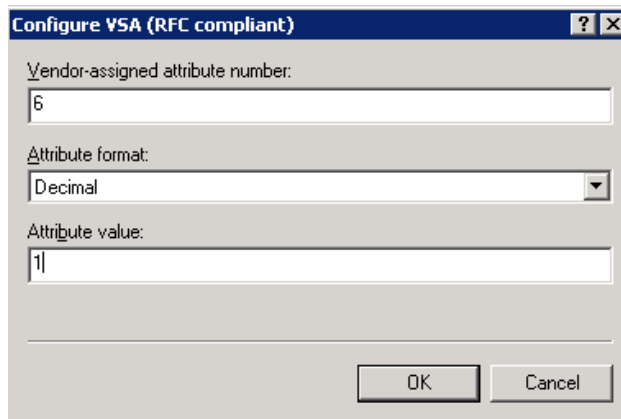
For example, you might have pool administrators for Pools A and B on a PS Series group, and others for Pools C and D. Additionally, you might have pool administrators who also have group-wide read-only privilege. These users can see, but not change, all the other objects in the group.

If you have PS Series groups running different firmware versions, and you create pool administrator accounts for the groups that support them (those running PS Series Firmware Version 3.2 or higher), those administrators will be allowed full group administrator access to PS Series groups running firmware versions earlier than V3.2. To prevent this, configure the RADIUS server to restrict access for those pool administrators to the IP address of the group running PS Series Firmware version 3.2.

Attributes for Pool Administrators (EQL-Pool-Access VSA):

Follow the steps laid out in [Creating a New Remote Access Policy](#) to add the new policy attributes for pool administrators. When adding the Vendor Specific Attributes for the new Remote Access Policy, follow the steps below.

1. Add a vendor-specific attribute with the following fields:
 - a. Vendor-specific attribute number: enter **6**
 - b. Attribute format drop-down: select **Decimal**
 - c. Attribute value field: enter **1**



The screenshot shows a dialog box titled "Configure VSA (RFC compliant)". It contains three input fields: "Vendor-assigned attribute number" with the value "6", "Attribute format" with a dropdown menu set to "Decimal", and "Attribute value" with the value "1". There are "OK" and "Cancel" buttons at the bottom right.

2. Click **OK** twice to get back to the Multivalued Attribute Information window.
3. **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:
 - a. Vendor-specific attribute number: enter **7**
 - b. Attribute format drop-down: select **String**

- c. Attribute value field: enter the list of pools, separated by commas only (no spaces)

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
7

Attribute format:
String

Attribute value:
Pool1

OK Cancel

The Multivalued Attribute Information window should look as follows:

Multivalued Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

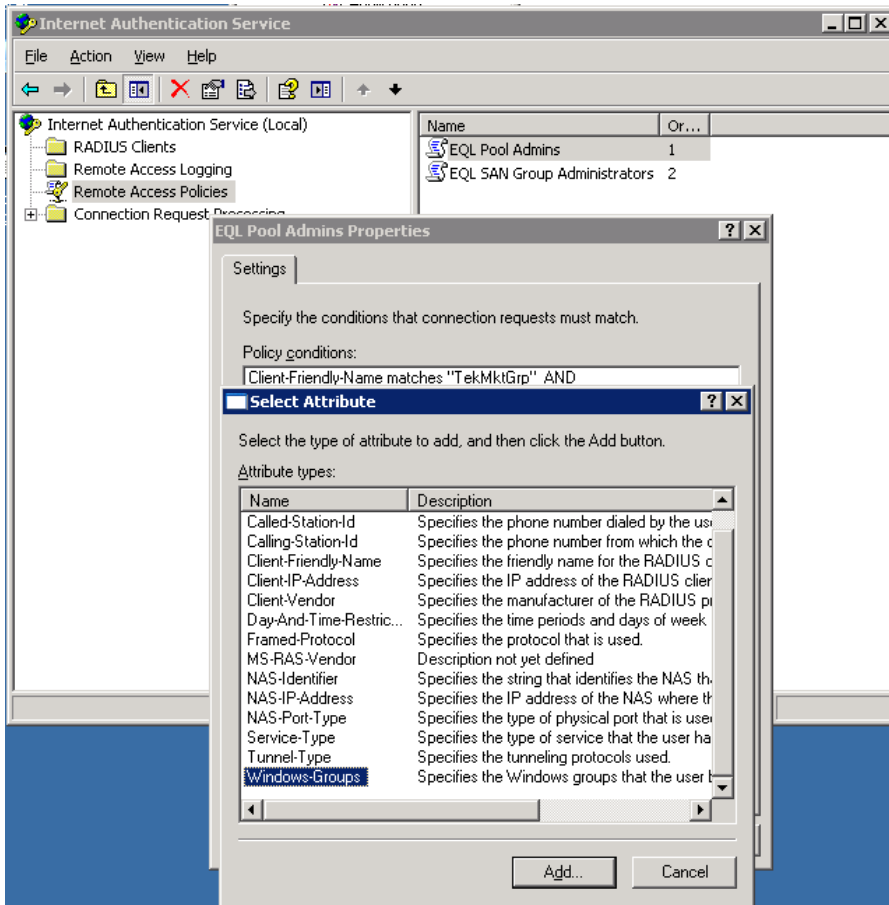
Attribute values:

Vendor	Value
Vendor code: 12740	1
Vendor code: 12740	Pool1

Move Up
Move Down
Add
Remove
Edit

OK Cancel

4. Once you have created the Active Directory Groups for specific pool managers, add the group to the Remote Access Policy settings as in step 3 of [Creating a New Active Directory Group for PS SAN Administrators](#).



To add any of the optional vendor-specific attributes, refer to Table 1 for their values.

Table 1: EqualLogic Optional Vendor-Specific Attributes*

Attribute	Field	Value
EQL-Admin-Full-Name	Attribute Number	1
	Attribute Format (Syntax)	String (Max. length: 247)
	Attribute Value	Name of person assigned to the account
EQL-Admin-Email	Attribute Number	2
	Attribute Format (Syntax)	String (Max. length: 247)
	Attribute Value	Email address of person assigned to the account
EQL-Admin-Phone	Attribute Number	3
	Attribute Format (Syntax)	String (Max. length: 247)
	Attribute Value	Phone number of person assigned to the account
EQL-Admin-Mobile	Attribute Number	4

* Applies to PS Series Firmware V3.0.5 or higher

Attribute	Field	Value
	Attribute Format (Syntax)	String (Max. length: 247)
	Attribute Value	Mobile number of person assigned to the account
EQL-Admin-Poll-Interval	Attribute Number	5
	Attribute Format (Syntax)	Integer
	Attribute Value	Number of seconds until the group configuration data must be repolled by the GUI. Default is 30 seconds.

EQUALLOGIC DOCUMENTATION AND CUSTOMER SUPPORT

Visit the EqualLogic Customer Service website, where you can download the latest documentation and firmware. You can also view FAQs, the Knowledge Base, and Technical Reports and submit a service request.

EqualLogic PS Series storage array documentation includes the following:

- d. *Release Notes*. Provides the latest information about PS Series storage arrays and groups.
- e. *QuickStart*. Describes how to set up the hardware and start using a PS Series storage array.
- f. *Group Administration*. Describes how to use the Group Manager GUI to manage a PS Series group. This manual provides comprehensive information about product concepts and procedures.
- g. *CLI Reference*. Describes how to use the Group Manager command line interface to manage a group and individual arrays.
- h. *Hardware Maintenance*. Provides information on maintaining the PS Series storage array hardware.

To access the Customer Support website, go to <https://www.equallogic.com/support/> and click LOGIN to log in to your support account. If you do not have an account, you can request one on this page.

If the issue is urgent, please call us at 1-877-887-7337 (toll free US & Canada) or 919-767-5729 to speak with a member of the customer support team.

If you have any comments or suggestions related to this technical report, please send them to techreports@equallogic.com