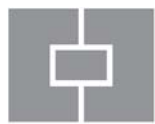


SOPHOS



sophos **nac**

ADVANCED

Configuring Steel-Belted RADIUS Proxy to Send
Group Attributes



Copyright © 2010 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in retrieval system, or transmitted, in any form or by any means electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names are trademarks or registered trademarks of their respective owners.

Document version 3.2
Published December 2010

Table of Contents

About this Document	4
Configuring the Steel-Belted RADIUS Proxy	5
Using the Sophos Compliance Agent.....	17

About this Document

The purpose of this document is to configure Steel-Belted RADIUS to pull group information from a remote directory server and forward that information to Sophos NAC Advanced. This ensures that the group can be given a Sophos compliance policy without the Sophos Compliance Application Server having a direct connection to Active Directory or LDAP. When Sophos NAC Advanced as a RADIUS proxy is used for the group mapping functionality, the RADIUS Enforcer is no longer responsible for looking up the group in Active Directory (via its GroupMapper component). Instead, the remote RADIUS server returns the Sophos VSA #20 (EF-GroupResponse) to let the Compliance Application Server know which group to apply to the user's request.

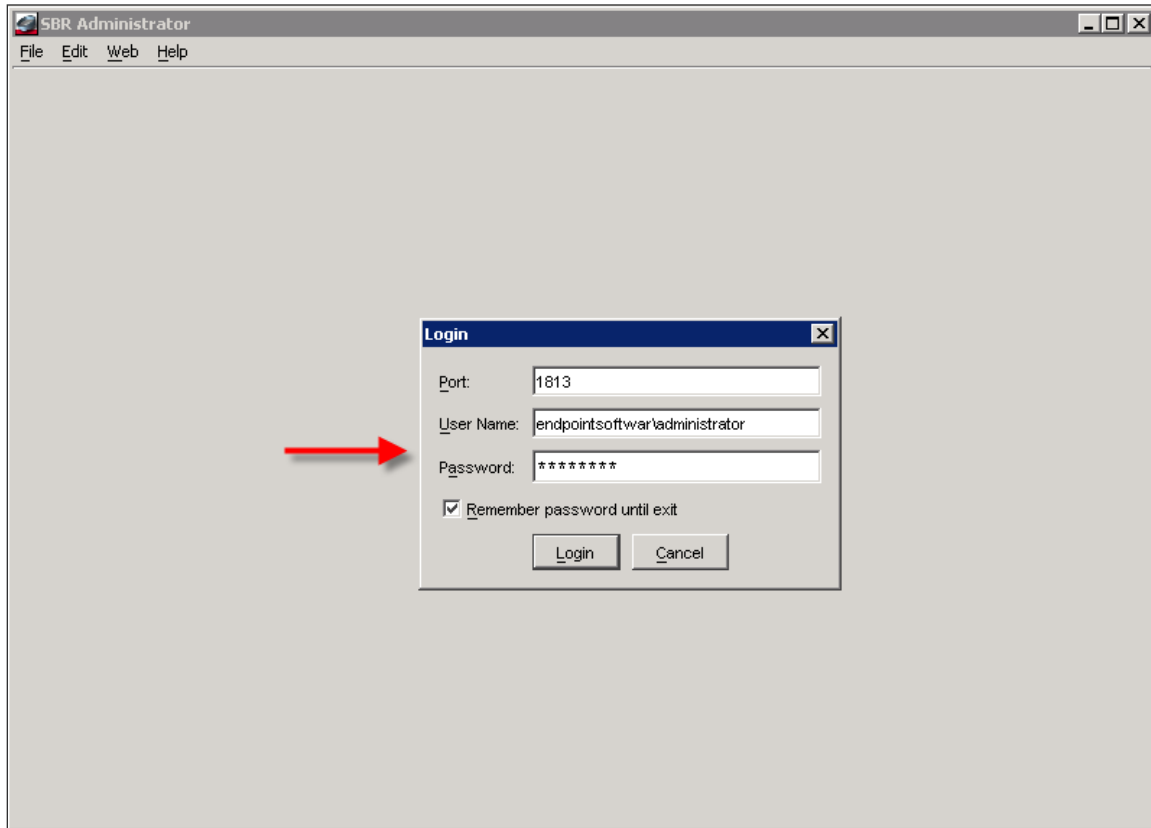
This document requires you to have already configured Internet Authentication Service (IAS) or Network Policy Server to use Sophos NAC Advanced as a RADIUS proxy, as described in the Post-Installation Requirements in the *Sophos NAC Advanced Installation Guide*. This document also assumes that Steel-Belted RADIUS is already set up and installed on the server and is running on ports 1812, 1813, 1645 and 1646 (default ports for Steel-Belted RADIUS). If it is not set up or running on these ports, you must modify these instructions to accommodate the changes.

If you plan on using Steel-Belted RADIUS to connect to an Active Directory Domain Controller to pull user/group information, make sure the Steel-Belted RADIUS server is on the domain or is in a trusted domain for the account/group information it will be pulling from. Also, ensure you use an account that is a member of the Domain Users Group so that you will have access to pull user/group information from Active Directory.

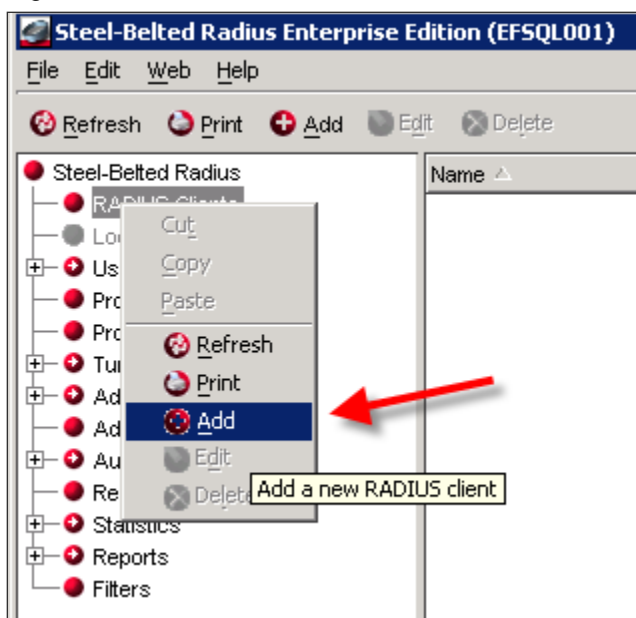
Configuring the Steel-Belted RADIUS Proxy

1. Go to <http://localhost:1812>, and click the **Launch** link to start Steel-Belted RADIUS.

2. Log in to Steel-Belted RADIUS.



3. Right-click **RADIUS Clients**, and click **Add**.



4. Type the appropriate information in the following fields:
 - Name (1)
 - Description (2)
 - IP address for the remote RADIUS client (3) (IP address of the Sophos Compliance Application Server)
 - Shared secret (4) (This must be the same password that was used in IAS or Network Policy Server when setting up Sophos NAC Advanced as the RADIUS proxy.)

The screenshot shows the 'Edit RADIUS Client' dialog box with the following fields and annotations:

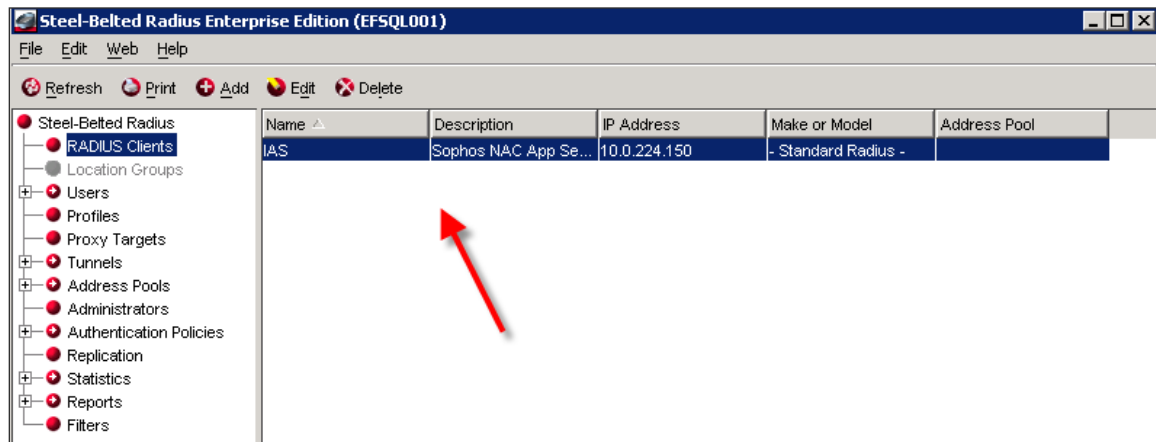
- Name:** IAS (Arrow 1)
- Description:** Sophos NAC App Server (Arrow 2)
- IP Address:** 10.0.224.150 (Arrow 3)
- Range:** 1 (Arrow 4)
- Shared Secret:** ***** (Arrow 4) with a **Validate** button and an **Unmask** checkbox.
- Make or model:** - Standard Radius - (Arrow 5)
- Address pool:** (Arrow 5) with a **View** button.
- Location Group:** (Arrow 5) with a **View** button.
- Profiles:**
 - Use Profile:** (Arrow 5) with a **View** button.
 - Attribute Combination:**
 - Merge**
 - Override**
 - Merge Precedence:**
 - User**
 - RADIUS Client**
- Advanced:**
 - Use different shared secret for Accounting** with an **Edit...** button.
 - Assume down if no keepalive packets after** [] **seconds**.

At the bottom, the **OK** button is highlighted with a red arrow and the number 6.

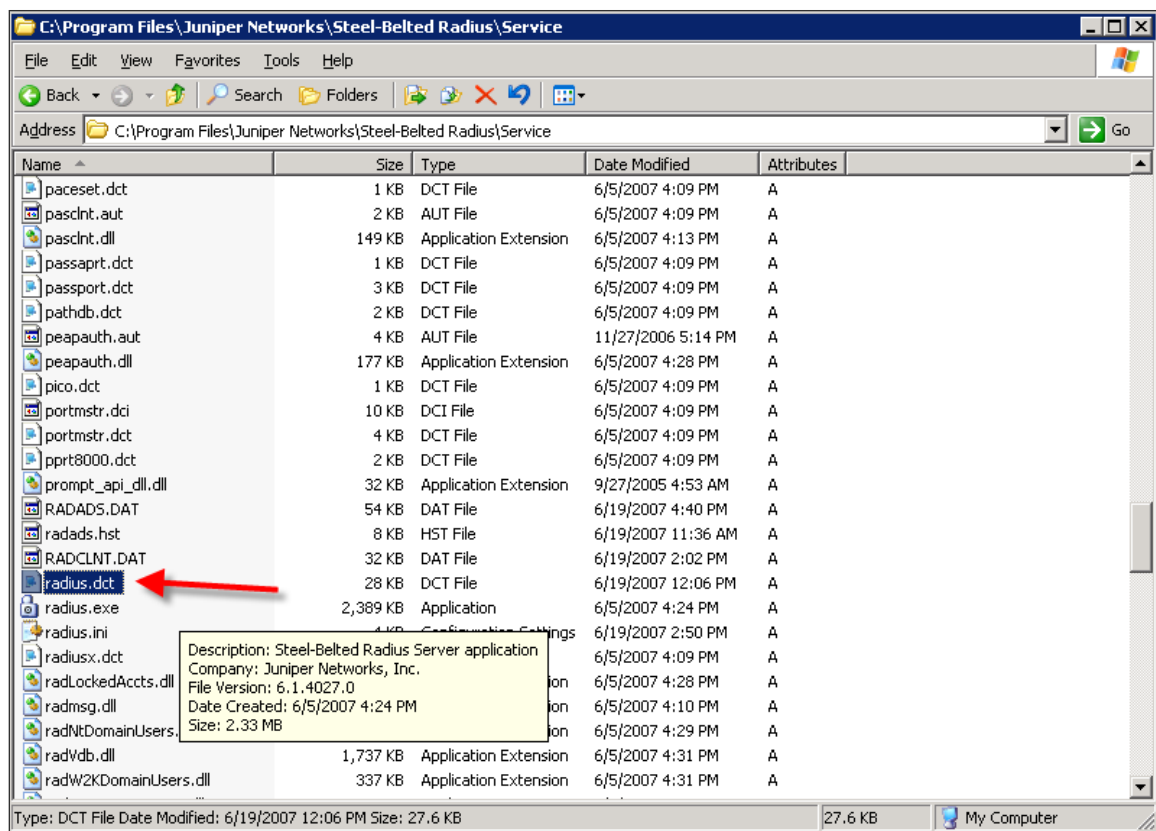
5. From the **Make or model** (5) list box, select **Standard RADIUS**.
6. Click **OK** (6) to save your changes.

Configuring Steel-Belted RADIUS Proxy to Send Group Attributes

7. Click **RADIUS Clients** to verify the new entry.



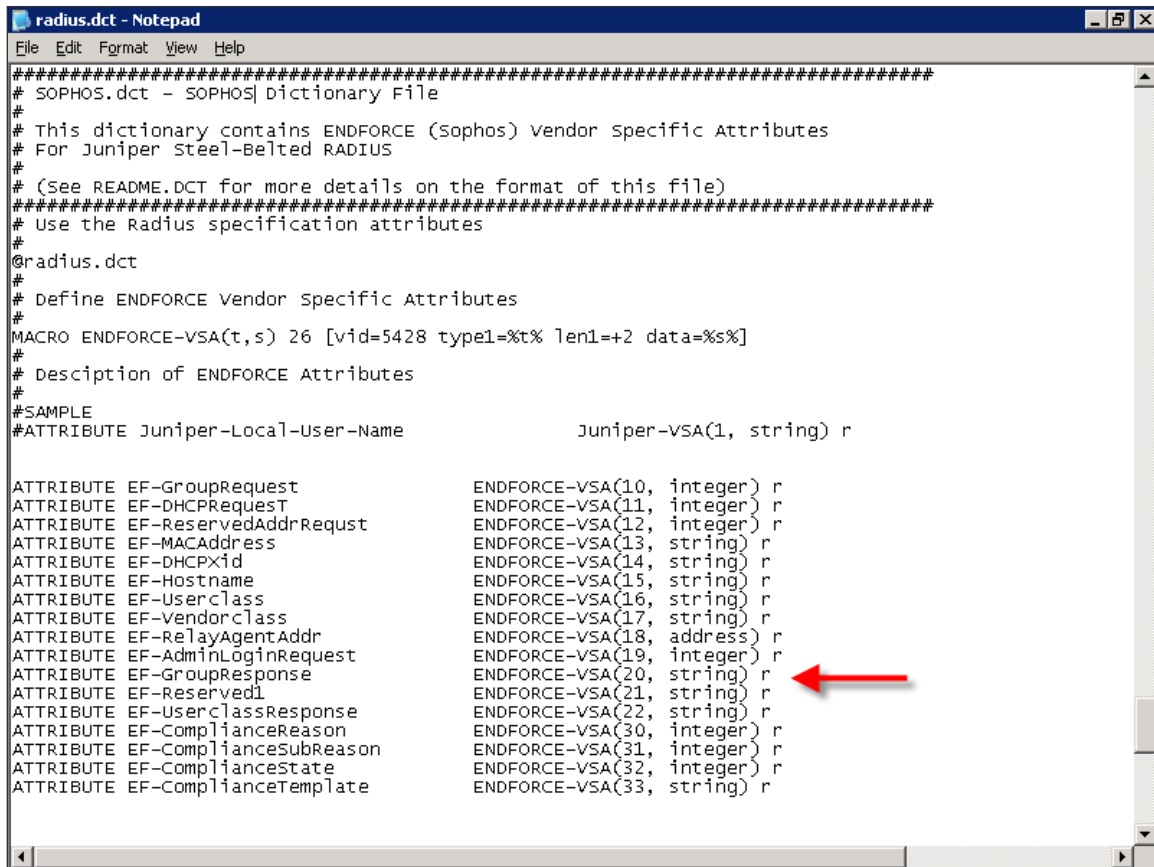
8. Open c:\program files\Juniper Networks\Steel-Belted RADIUS\Service. This is the default location for radius.dct file.
9. Open the radius.dct file.



10. In the radius.dct file, add the following lines for the following Sophos Dictionary attributes.

```
#####  
# SOPHOS.dct – SOPHOS Dictionary File  
@radius.dct  
MACRO ENDFORCE-VSA(t,s) 26 [vid=5428 type1=%t% len1=+2 data=%s%]  
ATTRIBUTE EF-GroupResponse ENDFORCE-VSA(20, string) r  
#####
```

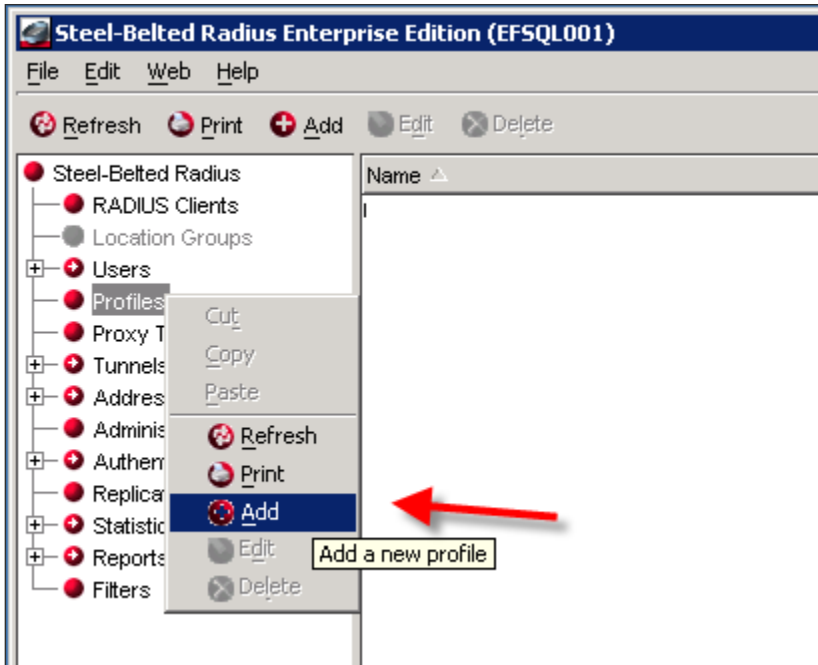
You can add all of the vendor-specific attributes, as shown below, but the one that Sophos requires for configuration is indicated below.



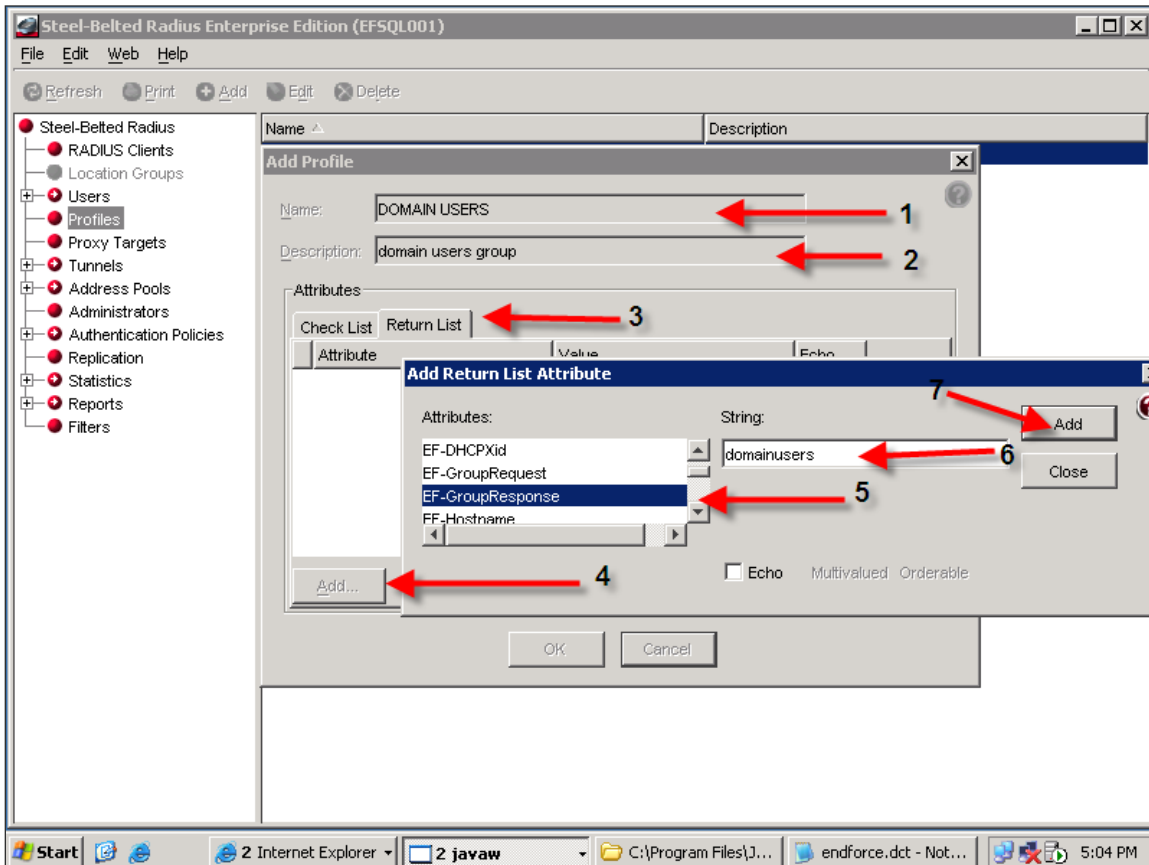
11. Save the radius.dct file.

12. Restart the Steel-Belted RADIUS Service for the changes to take effect.

13. Log in to the Steel-Belted RADIUS Administrator application.
14. Right-click **Profiles**, and click **Add**.



15. Type a name (1) and description (2) for the profile in the appropriate fields.



16. Click the **Return List** tab (3).

Note: This step ensure that RADIUS sends back the group attribute to the Sophos Compliance Application Server.

17. Click **Add** (4).

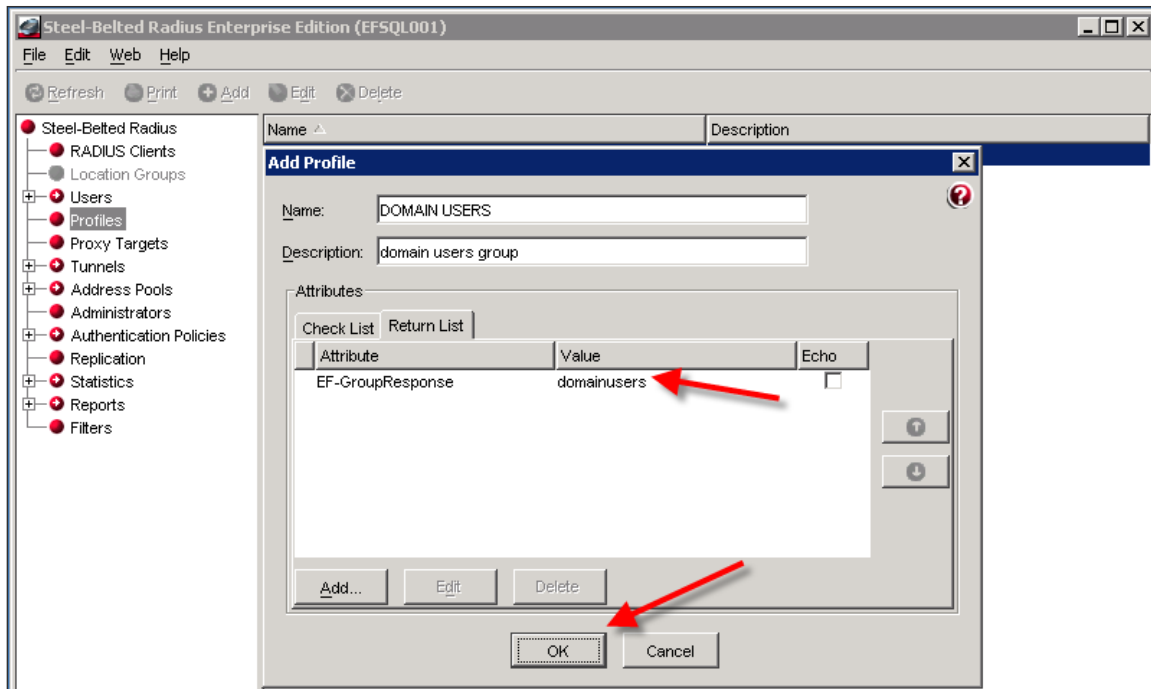
18. In the Attributes list, locate and select **EF-Group Response** (5).

19. In the **String:** field, type the group name that you want to pull for this profile (6), and click **Add** to add the Return List Attribute.

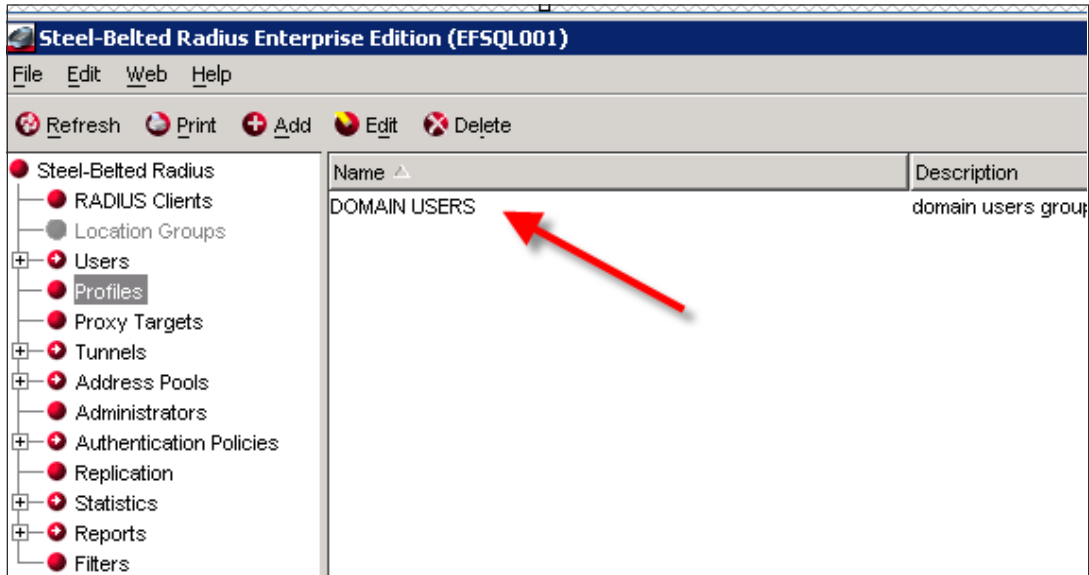
20. Click **Close**.

Note: The attribute is not a multi-valued attribute. Sophos NAC Advanced only supports single-valued attributes.

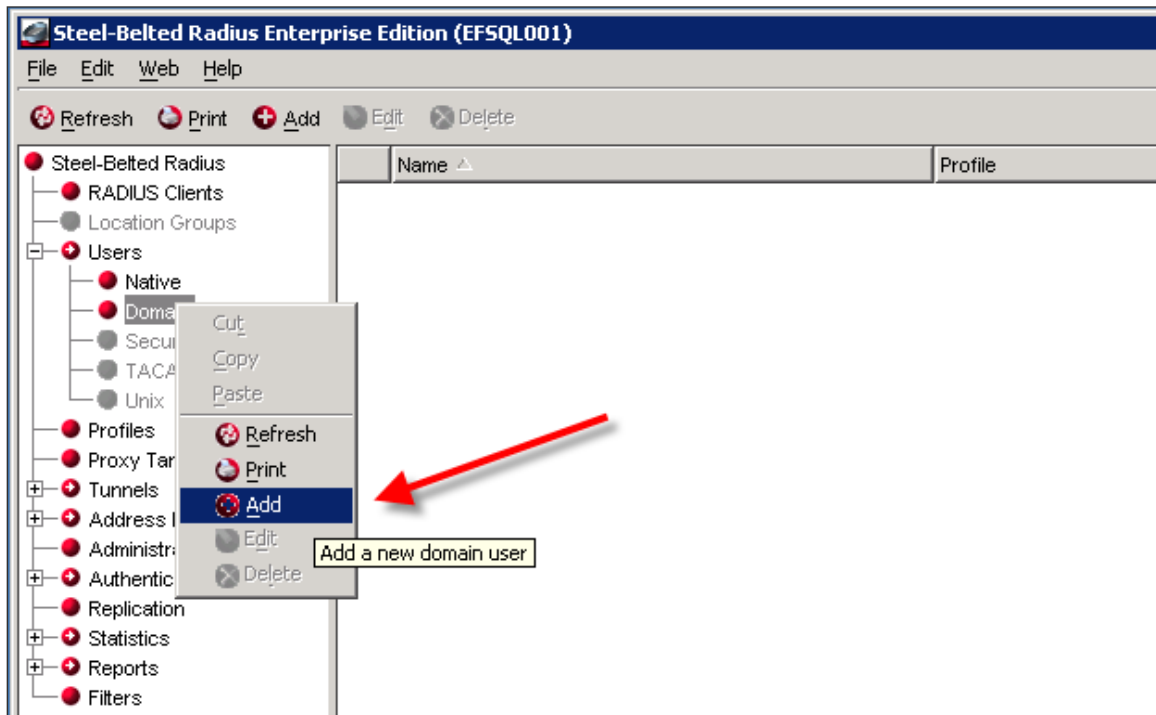
21. Verify that the new Return List Attribute displays, and click **OK**.



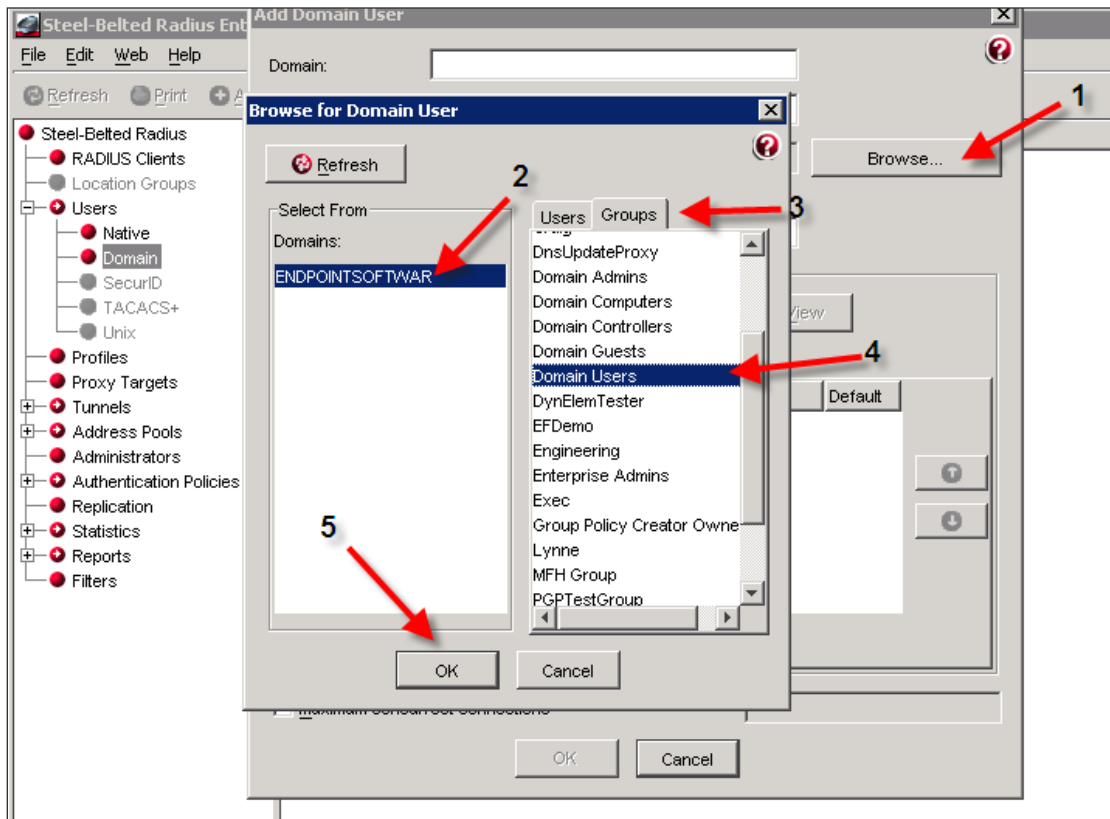
22. Verify that the new profile displays in the **Profiles** section.



23. Map the new profile to the domain group that the users are a part of in Active Directory. To do this, expand the **Users** section, right-click **Domains**, and click **Add**.



24. Click **Browse** to look for the possible users/groups to add (1).



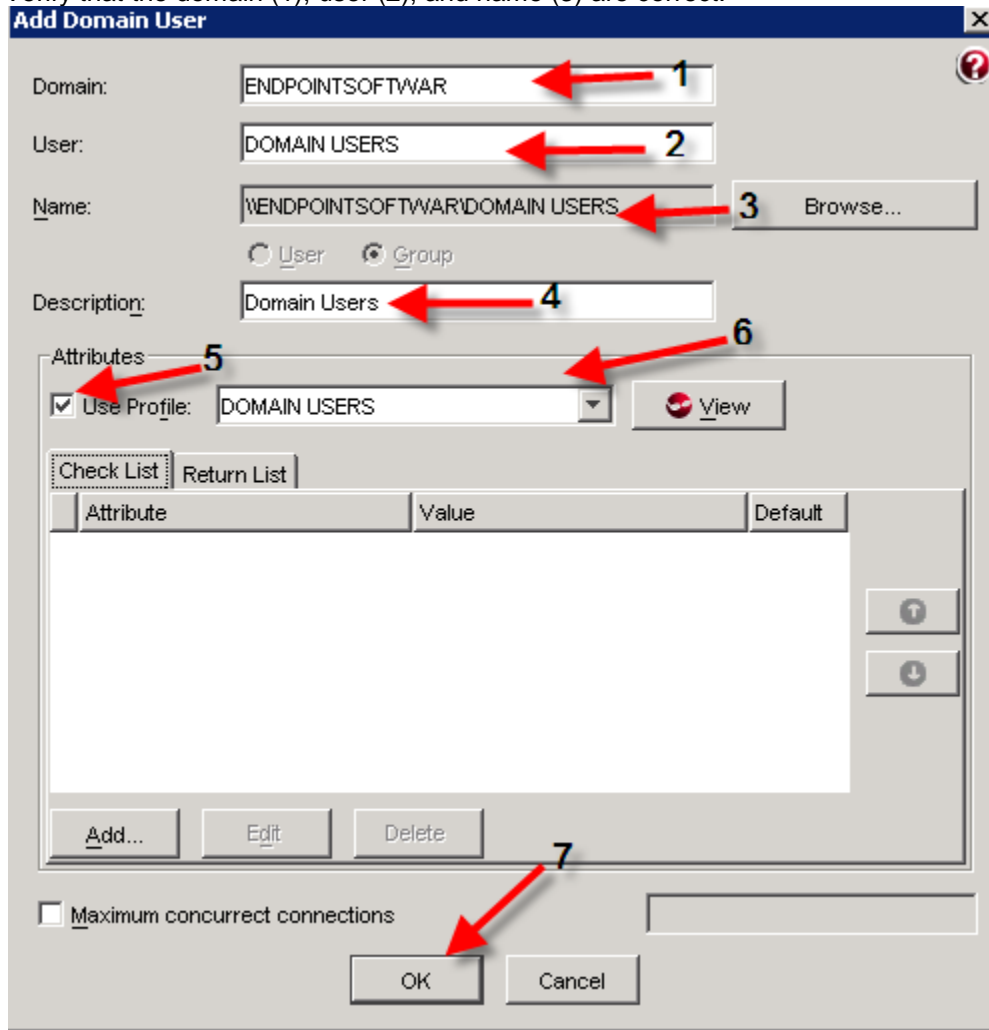
25. Select the domain (2).

26. Click the **Groups** tab (3).

27. Select the appropriate group from the list (4).

28. Click **OK** (5) to add the new group.

29. Verify that the domain (1), user (2), and name (3) are correct.



30. Type a description (4).

31. Select the **Use Profile** check box (5).

32. Select the name of the profile you just created from the list box (6).

33. Click **OK** (7).

Note: You can view the added group and its corresponding profile. By configuring groups/profiles in this manner, you can apply policies to whole groups of users, and then send the group attribute back to the Sophos Compliance Application Server using IAS or Network Policy Server so that a compliance policy can be applied to that group.

Using the Sophos Compliance Agent

When you use the Sophos Compliance Agent with a valid username and password that exists in the domain users group in Active Directory, an entry for this user displays in the Manage > Endpoints area of the Sophos Compliance Manager.

The screenshot shows the Sophos Compliance Manager web interface. At the top, there are navigation tabs: MANAGE, ENFORCE, REPORT, and CONFIGURE SYSTEM. Below these are sub-tabs: POLICIES, PROFILES, GROUPS, APPLICATIONS, PATCHES, and ENDPOINTS. The main heading is "Manage : Endpoints".

Search Criteria section includes input fields for Username, Group, Agent ID, and MAC Address, along with dropdown menus for Status and Expires in (Days). There are "Reset" and "Search" buttons.

Showing 1 - 1 of 1 Results Per Page: 50 Go Previous Go to Page: 1 Go of 1 Next

<input type="checkbox"/>	Username	Group	Agent ID	MAC Address	Status	Date/Time
<input type="checkbox"/>	jmaxwell	domainusers	7a9276a8-5df4-4add-8c3a-5d3a4f056bfe	00-10-A4-98-42-51	Active	6/19/2007 7:30:55 PM

At the bottom, there is a "Configure Agent Registration Settings" link and "Expire" and "Delete" buttons. The footer contains the copyright notice: © 2000-2007 Sophos Group. All rights reserved.