



3Com Network Access Manager

User Guide

Version 1.2

<http://www.3com.com/>

Part No. DUA1550-0AAA03
Published July 2007



3Com Corporation
350 Campus Drive
Marlborough, MA USA
01752-3064

Copyright © 2005-2007, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo and SuperStack are registered trademarks of 3Com Corporation.

Microsoft, and Windows are registered trademarks of Microsoft Corporation.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

CONTENTS

ABOUT THIS GUIDE

Naming Conventions	9
Screen Shots	9
Conventions	10
Related Documentation	10

1 INTRODUCTION

3Com Network Access Manager Overview	11
3Com Network Access Manager User Interfaces	13
Users of 3Com Network Access Manager	13
Network Administrators	13
Network Operators	14
3Com EFW Policy Support	15
Backing up 3Com Network Access Manager Data	16
Concepts and Terminology	16
Active Directory	16
Users/Groups/Computers	16
Internet Authentication Service (IAS)	16
Remote Access Policy	17
NAM Rules	17
NAM Rule Priority	18
Network Access Setting	18
RADIUS Authorization	19
MAC-address based Authentication	19
IEEE 802.1X Authentication	19
Authorization	20
Devices Supported	20
Configuring Edge Port Security	21

2 INSTALLING 3COM NETWORK ACCESS MANAGER

System Requirements	23
---------------------	----

Before Installation	25
Installing 3Com Network Access Manager	26
Overview	26
New Installation	26
Upgrading an Existing Installation	33
Modifying and Repairing An Installation	37
Uninstalling 3Com Network Access Manager	39
Activating 3Com Network Access Manager	42

3 GETTING STARTED

Using The Network Administrator User Interface	45
User Interface	45
Setting Up 3Com Network Access Manager	47
NAM VLANs View	47
Creating A New NAM VLAN	48
Deleting An Existing NAM VLAN	49
Renaming A NAM VLAN And Changing The VLAN ID	49
Displaying Rules Associated With A NAM VLAN	50
NAM Policies View	50
Creating A New NAM Policy	51
Deleting An Existing NAM Policy	52
Renaming A NAM Policy And Changing The Policy ID	52
Displaying Rules Associated With A NAM Policy	53
EFW Policies View	53
Creating A New EFW Policy	54
Deleting An Existing EFW Policy	55
Renaming An EFW Policy	56
Displaying Rules Associated With An EFW Policy	56
NAM Rules View	56
Creating A New NAM Rule	57
Deleting An Existing NAM Rule	61
Controlling Permission To Apply A NAM Rule	62
Changing NAM Rule Priorities	62
Changing NAM Rule Properties	63
Displaying Members Of A NAM Rule	63
Changing Members Of A NAM Rule	63
Users View	64

Associating Rules With A User	65
Displaying And Changing Rules Associated With A User	67
Creating A New User	67
Groups View	68
Associating Rules With A Group	68
Displaying And Changing Rules Associated With A Group	69
Creating A New Group	70
Computers View	70
Entering MAC Addresses For A Computer	71
Associating Rules With A Computer	72
Displaying And Changing The Rules And MAC Address Associated With A Computer	74
Creating A New Computer	75
Selecting Appropriate Permissions For An Operator	75
Using the MAC Address Tool	75
Using The Operator User Interface	78
Operator Tasks	78
Displaying And Changing Rules Associated With A User	78
Displaying And Changing Rules Associated With A Group	80
Displaying And Changing The Rule Associated With A Computer	81
Using the Find Feature	83
Find Computer by MAC Address	83
Network Administrator Tasks	84
What Happens	84
Find a NAM Rule/VLAN/NAM Policy	84
Network Administrator Tasks	85
What Happens	85
Using The Online Help	85

4 USING 3COM NETWORK ACCESS MANAGER WITHIN A NETWORK

Case Study Assumptions	87
Case Study 1 — Controlling User Access To The Network	88
Network Administrator Tasks	88
Network Operator Tasks	89
What Happens When A User Logs In	90
Case Study 2 — Restricting Network Access To Known Computers	91

Network Administrator Tasks	91
Network Operator Tasks	92
What Happens	93
Case Study 3 — Blocking A Specific PC From The Network	94
Network Administrator Tasks	94
When a PC needs to be blacklisted:	95
Network Operator Tasks	95
What Happens	96
Case Study 4 — Hot Desking	96
Network Administrator Tasks	96
Network Operator Tasks	97
What Happens When A User Logs In	98
Case Study 5 — Removing Infected Devices From The Network	99
Network Administrator Tasks	99
When a PC needs to be isolated for the first time:	100
Network Operator Tasks	100
What Happens	101
Case Study 6 — Combining Hot Desking With Host Filtering	101
Network Administrator Tasks	101
When a PC needs to be isolated for the first time:	102
Network Operator Tasks	102
What Happens When A User Logs In	103
Case Study 7 — Controlling Guest Access to the Network	103
Network Administrator Tasks	103
What Happens When A Guest User Logs In	104
Case Study 8 — Configure Third-party Device Support with 3Com Network Access Manager	105
Network Administrator Tasks	105
What Happens	106
Case Study 9 — Configure Third-party Health checking system with 3Com Network Access Manager	106
Network Administrator Tasks	107
What Happens	108

5 PROBLEM SOLVING

Checking the Event Viewer	109
Identifying Where The Problem Lies	111
Problems Related to Setting Up	112

Problems Related to Using the MAC Address Tool 118

6 CUSTOMIZING 3COM NETWORK ACCESS MANAGER

- 3Com Network Access Manager Plug-in Processing 120
 - Check RADIUS Request is Valid for 3Com Network Access Manager 120
 - Select the Highest Priority Rule 121
- Customizing the Configuration Files 121
 - 3ComNAMIAS-Configuration.ini File 121
 - 3ComNAMIAS-NASIdent.ini File 122
- Customizing IAS Access Policy 123

A CREATING A REMOTE ACCESS POLICY

- Introduction to IAS Remote Access Policies 125
- Using Microsoft Windows Server 2003 Operating System 126
 - Creating a New Remote Access Policy 127

B USING MICROSOFT WINDOWS SERVER 2008 OPERATING SYSTEM

- Configuring NPS for Health Checking with a 3Com Network Access Manager Response 146
 - NPS Configuration 146
 - Install the NPS Server Role 146
 - Configure the NPS to be a NAP Health Policy Server 146
 - Configure Connection Request Policy 148
 - Configure System Health Validators 151
 - Configure Health Policies 152
 - Configure Network Policies 154
- Configuring NPS for Network Access with a 3Com Network Access Manager Response 163
 - NPS Configuration 164
 - Install the NPS Server Role 164
 - Configure the NPS for Network Access 164
 - Configure Connection Request Policy 165
 - Configure Network Policies 169
- Case Study — Microsoft NAP Health Checking with 3Com Network Access Manager response 173

Network Administrator Tasks 173

C FORMAT OF 3COM NETWORK ACCESS MANAGER RADIUS VENDOR SPECIFIC ATTRIBUTES

3Com Authorization Type VSA 175

3Com Authorization Rule Name VSA 175

D CONFIGURING USE OF THE MAC ADDRESS TOOL

Configuring the Windows Firewall to Allow Access by the MAC Address
Tool 180

Using Windows Vista or Windows Server 2008 or Later 180

Using Windows XP SP2 or Windows Server 2003 SP1 182

Configuring Security Settings for the MAC Address Tool 183

E OBTAINING SUPPORT FOR YOUR 3COM PRODUCTS

Register Your Product to Gain Service Benefits 185

Solve Problems Online 185

Purchase Extended Warranty and Professional Services 186

Access Software Downloads 186

Contact Us 186

Telephone Technical Support and Repair 187

INDEX

3COM END USER SOFTWARE LICENSE AGREEMENT

ABOUT THIS GUIDE

This guide describes how to install and configure the 3Com Network Access Manager.

This guide is intended for use by network administrators who are responsible for installing and setting up network equipment, and who are already familiar with configuring Microsoft's Active Directory and IAS RADIUS servers. Certain sections of the guide may also be useful to non-IT staff responsible for the day-to-day routine of administering network access.



If a release note is shipped with the 3Com Network Access Manager and contains information that differs from the information in this guide, follow the information in the release note.

Most 3Com user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

<http://www.3com.com>

Naming Conventions

This guide refers to Microsoft Active Directory domain controllers as Active Directory servers.

Prior to 3Com Network Access Manager Version 1.2, 'NAM Policies' were referred to as 'QoS Profiles'.

Screen Shots

Screen shots in this User Guide are for Windows Server 2003, unless stated otherwise.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons




Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

Table 2 Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Words in <i>italics</i>	<p>Italics are used to:</p> <ul style="list-style-type: none"> ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the <i>Help</i> menu, select <i>Contents</i>. Click <i>OK</i>.
User entry	This typeface represents information that you must enter
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."

Related Documentation

In addition to this guide, each 3Com Network Access Manager provides on-line help which can be accessed through the application. This guide contains the instructions you need to install and configure your 3Com Network Access Manager.

1

INTRODUCTION

This chapter provides:

- an overview of how 3Com Network Access Manager integrates with Microsoft's IAS and Active Directory
- an explanation of NAM Rules, Rule Priority and RADIUS response
- an explanation of 3Com Network Access Manager's role in authorization
- a list of 3Com devices supported by 3Com Network Access Manager
- advice on configuring edge port security.

3Com Network Access Manager Overview

3Com Network Access Manager is designed for network administrators responsible for networks using Microsoft Active Directory and Microsoft's Internet Authentication Service (IAS). 3Com Network Access Manager simplifies the task of controlling who connects to the network using either IEEE 802.1X (also known as Network Login) or MAC-address based authentication (for example RADA). Today this task can be very complex to install and configure, particularly if using some of the more advanced security features.

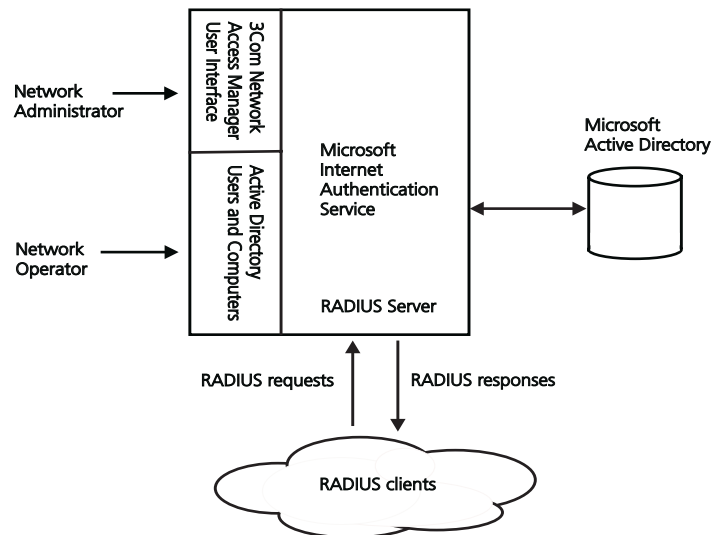
In summary, 3Com Network Access Manager simplifies the administration of:

- Network access for users via IEEE 802.1X.
- Network access for computers via MAC-address based authentication.
- Automatic VLAN assignment when a user or computer connects.
- Automatic QoS configuration when a user or computer connects.
- Automatic EFW policy configuration when an EFW user connects.
- Preventing specific users or computers from connecting to the network.

- Moving specific users or computers (e.g. a PC infected with a virus) into an isolated network.
- Multi-vendor RADIUS clients.

[Figure 1](#) illustrates the integration of 3Com Network Access Manager with Microsoft's Internet Authentication Service (IAS) and Microsoft's Active Directory.

Figure 1 3Com Network Access Manager Integrated with IAS and Active Directory



3Com Network Access Manager is not a standalone RADIUS server.

3Com Network Access Manager is a rule based application that extends the RADIUS response from the IAS RADIUS server to include the VLAN and NAM Policy (which selects the QoS profile to be applied on the switch) associated with the rule. Network administrators create rules through the 3Com Network Access Manager Network Administration interface, and apply them to the users, groups and computers configured within the domain. Network operators, if assigned permission by the network administrator, can apply rules to users, groups and computers, see [“Selecting Appropriate Permissions For An Operator”](#) in [Chapter 3](#).

3Com Network Access Manager can be used to extend the security on a network by setting up a self-protecting network. Creating a “Restricted

Access” user group and corresponding “Isolation” VLAN and QoS settings will enable the network administrator to separate authorized computers or users that represent a security threat to the network from those that do not represent a security threat. For example, a PC infected with a virus or a worm, or a user launching a DoS attack on the network. Further examples of how 3Com Network Access Manager can be used to improve the security on a network are given in [Chapter 4](#).

In addition, 3Com Network Access Manager provides facilities for the configuration of Active Directory based information for use by a 3Com EFW Policy Server, see [“3Com EFW Policy Support”](#).

3Com Network Access Manager User Interfaces

3Com Network Access Manager provides two interfaces: an Administration interface and an Operator interface, see [Figure 1](#).

The Administration interface is a Microsoft Management Console (MMC) snap-in that enables the user to quickly configure Active Directory/IAS to provide user and device authentication, with VLAN and QoS configuration. It is an extension of the existing Active Directory database so the list of users, groups and computers already set up in Active Directory are used to authenticate users. The administrator can also configure a safe network, to isolate PCs identified as being infected with a virus or worm.

The Operator interface is a simple extension to the current Active Directory Users and Computers interface, through the addition of an extra tab added to the Properties pages for users and computers. This allows non IT staff, granted with appropriate permissions, to apply rules that have already been setup by the network administrator.

Users of 3Com Network Access Manager

The 3Com Network Access Manager interfaces enables two different types of users to control and apply rules on a network: Network Administrators and Network Operators. This enables network administrators to delegate much of the day-to-day routine of administering network access to non technical staff.

Network Administrators

3Com Network Access Manager assumes network administrators are responsible for:

- setting up the RADIUS server and edge-port security, including the VLAN, QoS profiles and EFW Policies across the network,

- creating the user group structure within Active Directory, and are familiar with MAC addresses and IEEE 802.1X authentication.

Typical tasks for a network administrator using 3Com Network Access Manager include:

- adding computer MAC addresses,
- setting up appropriate rules to control access to the network, to ensure an appropriate level of security and protection for the network,
- setting appropriate administration privileges for network operators.

Network Operators

Network operators are allocated some limited administration privileges by network administrators, the extent of the privileges being specific to the individual and their role. For example, one operator may be limited to blocking access for specific users, whereas another operator may be allowed to move users between arbitrary groups.

Typical tasks for a network operator include specifying:

- if a user is allowed access to the network,
- if a computer (defined by the MAC address) is allowed access to the network,
- if allowed access, which VLAN should the user or computer connect to, and using which QoS configuration,
- if a computer should be isolated from the main network,
- if a user should be isolated from the main network,
- the EFW Policy for each user when they log into a PC with an EFW NIC installed.

Network operators using 3Com Network Access Manager, do not need to understand the complexities of the network or the technicalities of VLANs, QoS, EFW or RADIUS.

3Com EFW Policy Support

3Com Network Access Manager provides support for 3Com EFW Policy Server v2.5, which adds the concept of user-based Embedded Firewall (EFW) Policies rather than just NIC-based EFW Policies. For example, the policy which is downloaded to the EFW can be specific to the user logged into the PC and not just the PC itself. 3Com Network Access Manager enables the network administrator to define an EFW Policy for each user in Active Directory. The EFW Policy Server then queries Active Directory to determine the profile for each user and replies to the EFW with the relevant configuration.

Through 3Com Network Access Manager, the network administrator can change an EFW Policy at the same time as the port security settings, speeding up the configuration of the network. The EFW Policy is not returned in any RADIUS response.

To ensure that 3Com Network Access Manager and the 3Com EFW Policy Server operate together, the following steps must be followed using 3Com Network Access Manager:

- Define each EFW policy in 3Com Network Access Manager, see [“Creating A New EFW Policy”](#) in [Chapter 3](#). 3Com Network Access Manager creates the EFW Policy as an Active Directory object.
- Associate the EFW Policy with rules created in 3Com Network Access Manager. This can be done during the creation of a new rule, or after a rule has been created, see [“Creating A New NAM Rule”](#) and [“Changing NAM Rule Properties”](#) in [Chapter 3](#).
- Make sure that appropriate users and groups have been associated with each rule associated with the EFW Policy, see [“Displaying Members Of A NAM Rule”](#) in [Chapter 3](#).



Any changes to EFW Policy associations must be made through the 3Com Network Access Manager user interface. 3Com Network Access Manager will not recognize any externally made changes.

After making any change that might affect the EFW Policy of a user, the EFW group associations must be recalculated for the user, this is done by clicking the *Recalculate EFW membership* button on the Tool bar at the top of the Administration Interface window, see [Figure 19](#) in [Chapter 3](#). Examples of changes that might affect the EFW policy of a user are:

- if a user's properties are changed, the correct rule association has to be re-established. Clicking on the *Recalculate EFW membership* button will cause 3Com Network Access Manager to find the highest

priority rule associated with the user, the EFW Policy from that rule is then associated with the user, all other associations are removed.

- if a rule priority or group is changed, the correct associations have to be re-established. Clicking on the *Recalculate EFW membership* button will cause 3Com Network Access Manager to find all users that are members of that rule or group, and then finding the authorization rules applied for each. In a large network this can take a considerable time.

Backing up 3Com Network Access Manager Data

Data from 3Com Network Access Manager is stored in Active Directory, via an LDAP interface. Your normal methods for backing up/restoring of data from Active Directory will also cover 3Com Network Access Manager data. No special backup/restore is required for 3Com Network Access Manager data.

Concepts and Terminology

This section provides descriptions of concepts and terminology that you will need to be familiar with in order to use 3Com Network Access Manager.

Active Directory

Active Directory is the distributed directory service included with the Microsoft Windows Server 2003 operating system. Active Directory enables centralized, secure management of an entire network, which might span a building, a city, or multiple locations throughout the world. Active Directory stores information about objects on the computer network and makes this information easy to find, view and manage. With Active Directory, users can access resources anywhere in the network with a single logon, and administrators have a single point of administration for all objects in the network. When interfaced to IAS, Active Directory provides secure single login for users, and administrators.

Users/Groups/Computers

Users, groups and computers are standard Active Directory objects, membership of a group is managed using normal Active Directory management tools.

Internet Authentication Service (IAS)

IAS is Microsoft's implementation of a RADIUS server, providing authentication and authorization of users. IAS is included with the Microsoft Windows Server 2003 operating system. As a RADIUS server, IAS performs centralized connection authentication, authorization, and

accounting for network access servers (desktop switches and wireless access points acting as RADIUS clients), see [Figure 2](#).

Remote Access Policy

For 3Com Network Access Manager to authenticate users and computers accessing the network, an IAS Remote Access Policy must be created. [Appendix A](#) provides step by step instructions on how to create a Remote Access Policy.

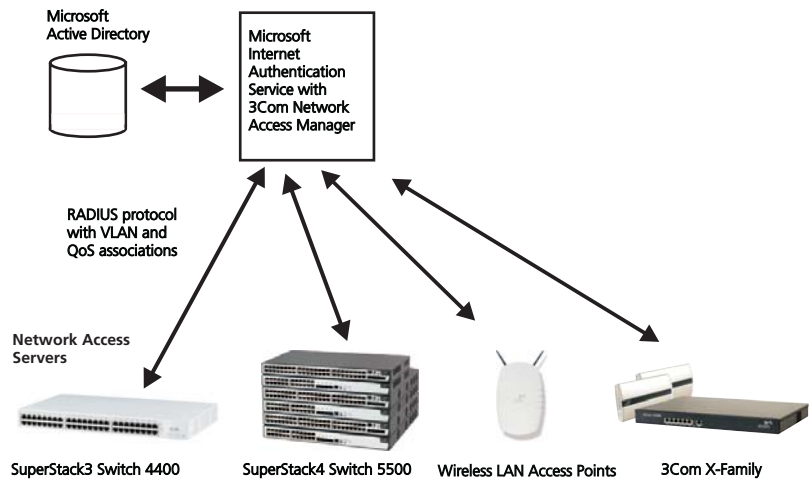


In a mixed-vendor network where only 3Com switches are used for authentication through 3Com Network Access Manager, the Remote Access Policy needs to be adjusted to only match 3Com devices.



In a mixed-Switch (3Com wired, 3Com wireless, 3Com X-Family, and multi-vendor) network where different formats of RADIUS response is needed, the Remote Access Policy needs to be adjusted to identify the correct response type to 3Com Network Access Manager. The 3Com Network Access Manager configuration file may also need adjustment. See ["Customizing the Configuration Files"](#) on [page 121](#).

Figure 2 Network Access Servers within a Domain



NAM Rules

3Com Network Access Manager provides its functionality through a set of NAM Rules implemented in Active Directory. Each rule comprises a priority, a Network Access setting (allow/deny), an optional authorization response (VLAN and Policy), and an optional EFW policy name.

Users, groups and computers (through the MAC address of the PC) are associated with rules. When multiple rules are associated with a user, group or computer then the rule with the highest priority takes precedence.

Only one pre-defined rule, the Default Rule, is supplied as standard. The Default Rule is used whenever an authentication finds that a user, group or computer is not a member of any other rule. Further rules are added by the Network Administrator to implement the required network security policies, see [“Creating A New NAM Rule”](#) in [Chapter 3](#).



CAUTION: *It is important that the default rule is never deleted.*

NAM Rule Priority

Each NAM Rule has a priority associated with it. The rule with priority 1 has the highest priority, and will take precedence over all other rules. Whenever a RADIUS request is authenticated, all associated rules will be found, but only the rule with the highest priority will be used. No two rules can have the same priority.

The Default Rule always has the lowest priority.

Network Access Setting

A rule defines the Network Access as either:

- Allow — the authorization is valid, or
- Deny — the authorization is refused

If the Network Access for a rule is set to *Allow*, and the rule is selected, then the RADIUS response will be *Accept* and will contain the VLAN and Policy associated with the rule. If the Network Access for a rule is set to *Deny*, and the rule is selected, then the RADIUS response will be *Reject*.

To understand the effect that the Network Access setting has in a network, the Network Administrator needs to be aware of how the edge port security has been set up. In some port modes, the setting may appear counter-intuitive, for example *Allow* can be used to implement a blacklist. For more information on edge port security modes, see [“Configuring Edge Port Security”](#).

RADIUS Authorization

The 3Com Network Access Manager Authorization Plug-in for IAS is provided as part of the 3Com Network Access Manager installation. The 3Com Network Access Manager Authorization Plug-in for IAS is responsible for extended verification of the access request and sending the RADIUS response for a user or computer that is recognized by 3Com Network Access Manager.

The two forms of RADIUS authentication supported by 3Com Network Access Manager are:

- MAC-address based authentication, for example RADA (RADIUS Authenticated Device Access).
- IEEE 802.1X authentication, also known as dot1X, 802.1X and Network Login.

MAC-address based Authentication

3Com Network Access Manager relies on the RADIUS server to perform MAC-address based authentication through a single authentication user name (as opposed to the MAC address as a user name).

When 3Com Network Access Manager receives an authentication request it authenticates the MAC authentication user name and MAC address of the computer against the 3Com Network Access Manager rules to determine the authentication outcome, as follows:

- 1 Look up the MAC authentication user name against all users configured, to find all associated rules.
- 2 Look up the MAC address against all Computers configured, to find all associated rules.
- 3 If rules are found, select the highest priority rule.
- 4 If no rules are found, select the Default Rule.
- 5 Return the authentication result from the selected rule.

IEEE 802.1X Authentication

When a switch performs IEEE 802.1X authentication, the process is identical to the MAC-address based authentication, as follows:

- 1 Look up the IEEE 802.1X username against all Users configured, to find all associated rules.
- 2 Look up the MAC address against all Computers configured, to find all associated rules.

- 3 If rules are found, select the highest priority rule.
- 4 If no rules are found, select the Default Rule.
- 5 Return the authentication result from the selected rule.

Checking the MAC address ensures that network policies such as blocked hosts can be maintained, regardless of edge port security mode.

Authorization

Once a user has successfully authenticated, the authorization process determines which VLANs and QoS to return to the switch, as follows:

- 1 From the authentication rule selected, if any VLAN has been specified, return the VLAN ID in the RADIUS response.
- 2 From the authentication rule selected, if a Policy has been specified, return the Policy as QoS Profile ID in the RADIUS response.



Policy can be returned as any or multiple attributes in the RADIUS response. See [“Customizing the Configuration Files”](#) on [page 121](#).

Devices Supported

The following 3Com devices are supported by 3Com Network Access Manager v1.2.

Table 3 3Com Devices Supported By 3Com Network Access Manager

Device Type	Agent Version	Authorization Type	Unit / Port Security Mode
4200 (4226T/4250T)	3.00	1	802.1X RADA
4200G	3.1	1	802.1X RADA
4210	3.1	1	802.1X RADA
4400	6.13	1	802.1X RADA
4500	3.01.00p01	1	802.1X RADA
5500	3.2.3	1	802.1X RADA

Table 3 3Com Devices Supported By 3Com Network Access Manager

Device Type	Agent Version	Authorization Type	Unit / Port Security Mode
5500G	3.2.4	1	802.1X RADA
7700	3.01.51	1	802.1X RADA
7757	3.2.0	1	802.1X RADA
8800	3.01.31e	1	802.1X
Wireless AP 7250/8250/8750	3.31	1	802.1X
Wireless AP 7760	3.31	1	802.1X
Wireless AP 8760	3.31	1	802.1X
Wireless Switch WXR100	6.0.3	1 and 3*	802.1X
Wireless Switch WX1200	6.0.3	1 and 3*	802.1X
Wireless Switch WX2200	6.0.3	1 and 3*	802.1X
Wireless Switch WX4400	6.0.3	1 and 3*	802.1X
Unified Gigabit Wireless Switch	1.1.15	1	802.1X
X5	2.5.1	1	Web Portal

* Advised if roaming required.



Ensure that the configurations of the devices on your network are consistent with the security policy to be set up using 3Com Network Access Manager.

Configuring Edge Port Security

If VLANs are to be configured in 3Com Network Access Manager then edge ports on switches across the network need to be set to a security mode that supports auto-VLANS. If VLANs are not to be set up in 3Com Network Access Manager, then the devices do not need to support auto-VLANS.

In addition, the edge ports on switches must be set to consistent modes, otherwise the same RADIUS response will yield different actions on different ports. For example, *RADA And Network Login* only allows user login if the RADIUS server returns *Accept*. *RADA-Else-Network Login* only allows user login if the RADIUS server returns *Reject* for RADA request.

[Table 4](#) lists suitable edge port security modes and their typical use within a network. The case studies in Chapter 4 explain how these port security modes operate to control network access.

Table 4 Edge Port Security Modes Compatible With 3Com Network Access Manager

Port Security Mode	Typical Use
RADA-Else-Network Login	<p>Primarily used for isolating unwanted hosts, as the RADA authorization overrides the ability for the user to log-in.</p> <p>This is the recommended edge port security mode, if the devices on your network support it. All users have to be authorized before being allowed access. Any computer or device can access the network as long as that they have not been identified as infected. This allows a network administrator to easily add host filtering to an existing IEEE 802.1X network.</p>
RADA And Network Login	<p>Both the computer and the user need to be authorized to gain access to the network.</p> <p>It is primarily used for “White-list” style of security, where all known computers have to be first configured before a user can log-in from one of these computers.</p>
RADA Or Network Login	<p>Access to the network is granted if either the computer or the user is authorized. This mode is flexible for environments where not every device has a IEEE 802.1X client</p>
RADA (MAC-address based Authentication)	<p>Use to control computer access to the network.</p>
Network Login (IEEE 802.1X)	<p>Use to control user access and manage QoS and VLAN configuration.</p>

2

INSTALLING 3COM NETWORK ACCESS MANAGER

This chapter covers:

- the operating systems and required PC configurations that are compatible with the 3Com Network Access Manager components,
- the tasks that need to be performed before installing and running 3Com Network Access Manager,
- how to install 3Com Network Access Manager,
- how to modify and repair an existing 3Com Network Access Manager installation,
- how to uninstall 3Com Network Access Manager.

System Requirements

[Table 5](#) lists the Microsoft Windows operating systems compatible with installing and running the 3Com Network Access Manager components.

Table 5 Microsoft Windows Operating Systems Supported By 3Com Network Access Manager

3Com Network Access Manager Component	Windows Server 2003 SP1 & SP2 (32 bit/64 bit)	Windows 2000 Professional SP1	Windows XP Professional SP1	Vista
IAS component	yes	no	no	no
Active Directory component	yes	no	no	no
Network Administrator User Interface	yes	yes	yes	yes
Network Operator User Interface	yes	yes	yes	yes
User Guide	yes	yes	yes	yes

[Table 6](#) lists the configuration requirements of PCs that will have 3Com Network Access Manager components installed.

Table 6 PC Configuration Requirements

3Com Network Access Manager Component	For each PC that will have 3Com Network Access Manager component installed:
IAS component	Ensure IAS is installed on PC. Ensure the PC is a member of the required domain.
Active Directory component	Only install on one domain controller. This must become the schema master (schema FSMO) to perform the install. You will need to have Schema Administrator privileges to install the Active Directory component.
Network Administrator User Interface	Ensure the PC is a member of the required domain. Install Active Directory Users and Computers, if not already installed.
Network Operator User Interface	Ensure the PC is a member of the required domain. Install Active Directory Users and Computers, if not already installed.
User Guide	Adobe Acrobat Reader is required on each PC used to view the 3Com Network Access Manager user guide (this guide). Obtain a free download of Adobe Acrobat Reader from http://www.adobe.com/

Before Installation

You must perform the following tasks on your network before installing and setting up 3Com Network Access Manager:

- 1 Install and configure Microsoft Internet Authentication Service (IAS),
 - a Install IAS on one or more Windows 2003 servers in the network. IAS is included as part of the operating system. For information on setting up IAS, refer to the Microsoft documentation supplied with IAS.
 - b Ensure all 3Com devices in the network that will use IAS are configured in IAS as RADIUS clients with client-vendor set to '3Com'.
 - c Setup an IAS Remote Access Policy that 3Com Network Access Manager will be required to use to authenticate users and computers. Refer to [Appendix A](#) for details on how to create an IAS Remote Access Policy.



3Com recommends that you avoid including the same attributes in the IAS access policy.

- 2 Ensure all Users, Groups and Computers have been added to Microsoft Active Directory for your network domain, refer to the user documentation supplied with Active Directory for details.
- 3 Configure the 3Com switches and wireless access points on your network
 - a Configure the 3Com switches with consistent VLAN and QoS settings throughout the network.
 - b Configure all edge ports on 3Com switches with a suitable and consistent edge port security mode and Intrusion Action setting. For information on edge port security modes suitable for use with 3Com Network Access Manager, see "[Configuring Edge Port Security](#)" in [Chapter 1](#).



CAUTION: *Using different security modes on switch edge ports on your network, will result in different meanings for RADIUS responses across the network.*



Use 3Com Network Director or 3Com Enterprise Management Suite to make the VLAN, QoS and port security mode settings, or else configure each switch through its web or command line interface. Refer to the user documentation accompanying the management application or switch for details.

Installing 3Com Network Access Manager

Follow the instructions in this section to install 3Com Network Access Manager.

Overview

3Com Network Access Manager comprises five components:

- Internet Authentication Server component consisting of the 3Com Network Access Manager Authorization Plug-in for IAS
- Active Directory Server component, this component will extend your Active Directory schema configuration which cannot be deleted from Active Directory
- Network Administrator User Interface
- Network Operator User Interface
- this user guide

Each component is installed through the 3Com Network Access Manager installer.

To install any of the components requires that you have administration privileges on the local computer. When installing the IAS plug-in you must use a domain account, that is, you can not install the IAS plug-in using the local administrator account.



You will need to have Schema Administrator privileges to install the Active Directory component.

New Installation

The Internet Authentication Server component needs to be installed on each IAS in the network. However, the Active Directory Server component should only be installed on one Active Directory server (also known as a domain controller) which should be the schema master on your network. The changes that the Active Directory Server component makes to the Active Directory server will be replicated across all of the Active Directory servers on your network.



The extensions that the Active Directory Server component makes to the Active Directory schema configuration cannot be deleted. The 3Com Network Access Manager uninstaller will not affect or remove these Active Directory extensions.

Install the Network Administrator User Interface and Network Operator User Interface on the PCs that will be used by the network administrators and operators using 3Com Network Access Manager. Before installing, check that the operating system and configuration of the PC complies with [Table 5](#) and [Table 6](#).

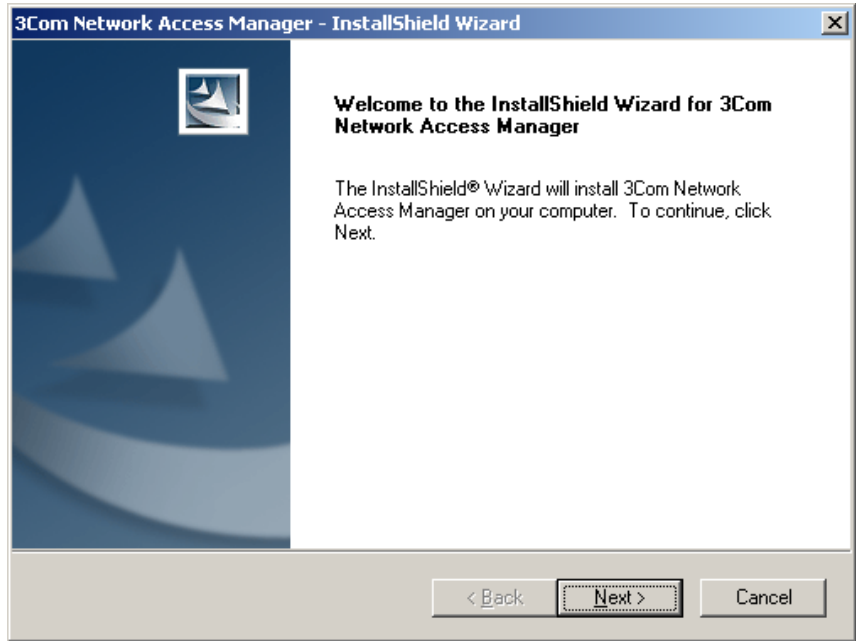
Follow these steps to install the 3Com Network Access Manager components:

- 1** Insert the 3Com Network Access Manager CD in the PC's CDROM drive. If Autorun is enabled on the PC, the installation starts automatically and you can skip steps 2 and 3.
- 2** From the *Start* menu, select *Run*.
- 3** Type `D:\setup` (substitute the appropriate letter of your CD-ROM drive for D), and click *OK*.
- 4** A splash screen will display and the installer will check that:
 - the user has administrator privileges on the local machine
 - a supported version of Windows is installed on the PC, as shown in [Table 5](#),
 - the PC is a member of a domain,

if any of the checks fail, an error message will display indicating the problem and the installer will abort. You need to correct the problem before restarting the installer.

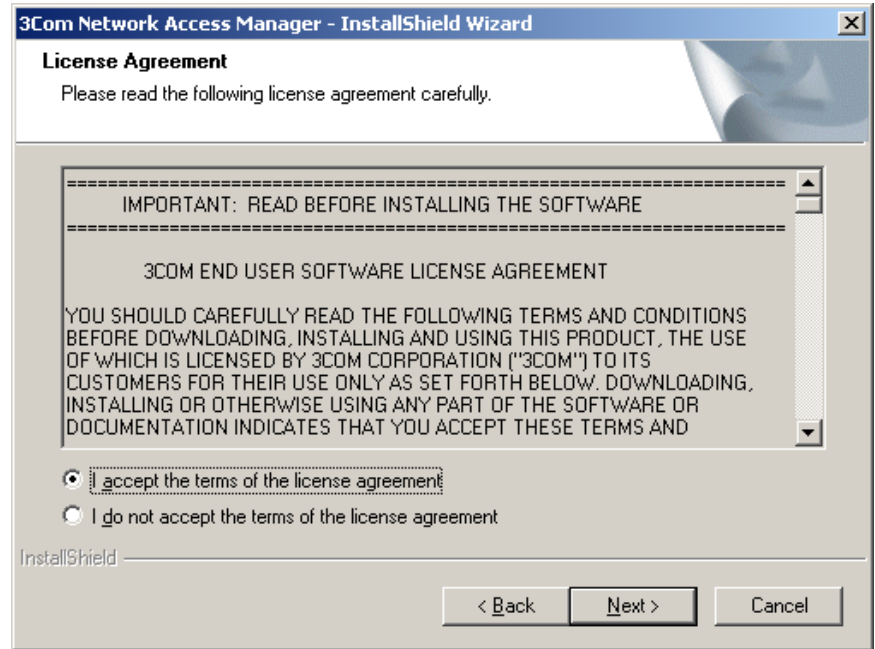
If the checks are successful, the *Welcome* dialog is displayed, [Figure 3](#).

Figure 3 InstallShield Wizard



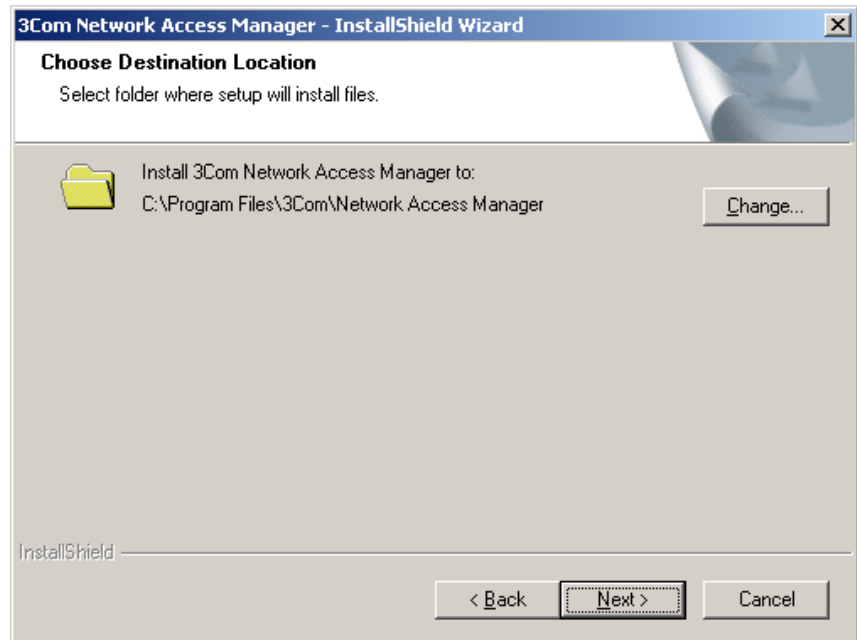
- 5 Select *Next*, the *End User License Agreement* will display, [Figure 4](#).

Figure 4 End User Licence Agreement dialog



To continue the installation select *I accept the terms of the license agreement*, and press the *Next* button. Otherwise, select *Back* to move to the previous dialog or *Cancel* to end the installation.

- 6 On the next dialog, [Figure 5](#), either select the destination location for the 3Com Network Access Manager files using the *Change* button or else use the default location *Program Files\3Com\Network Access Manager*. Press *Next*.

Figure 5 Choose Destination Location

- 7 On the next dialog, [Figure 6](#), select the 3Com Network Access Manager features to install on the PC. Ticked features will be installed. Un-ticked features will not be installed. The *Next* button will be grayed out until a component has been ticked.



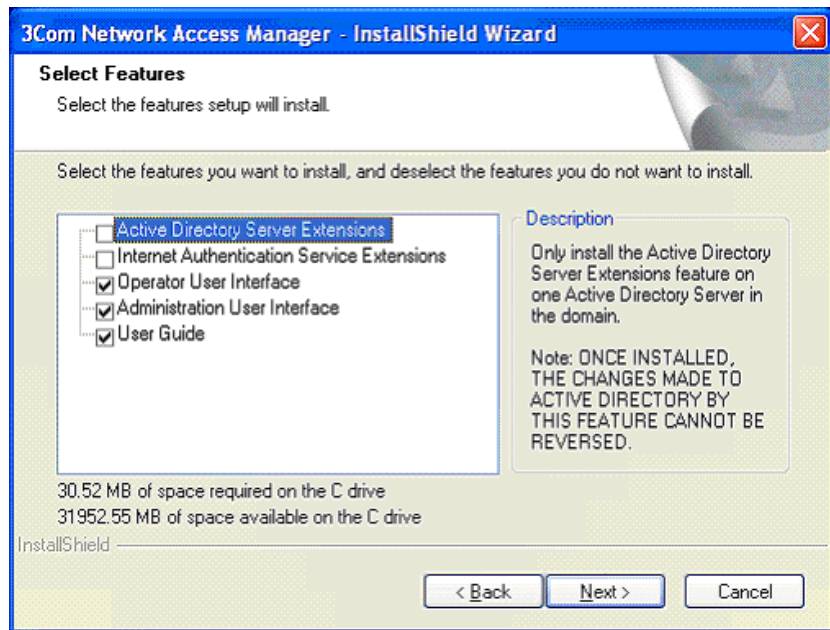
Any combination of features is permitted on a PC providing they are supported by the PC's operating system, see [Table 5](#).



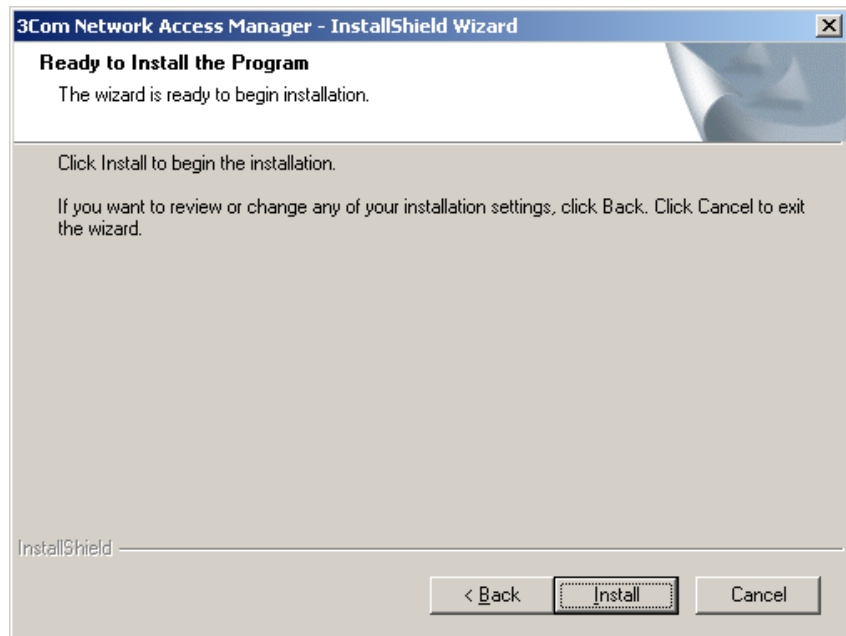
CAUTION: *The changes that the Active Directory Server component makes to the Active Directory schema configuration cannot be deleted.*



You will need to have Schema Administrator privileges to install the Active Directory component.

Figure 6 Feature Selection

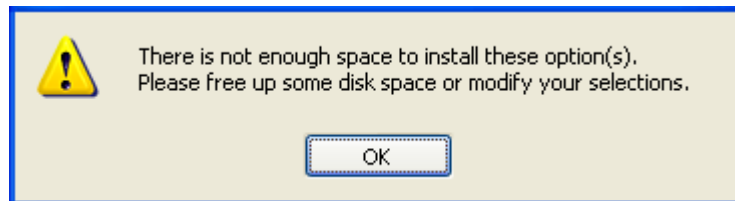
- 8 On the next dialog, [Figure 7](#), select *Install* to start the installation, or *Back* to return to the previous dialog.

Figure 7 Confirmation of Installation

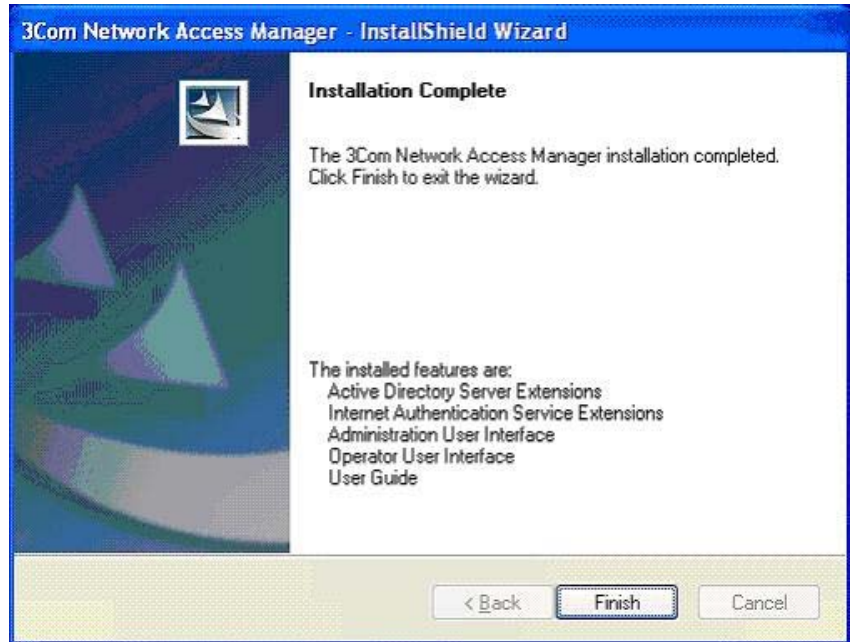
- 9 The Installer will check the hard disk space available on the PC. If sufficient disk space is available, the installer will install the components selected.



If insufficient disk space is available, an error message is displayed, see [Figure 8](#), the installation will stop until sufficient space is made available.

Figure 8 Insufficient Disk Space Error Message

- 10 Once each of the selected components have been successfully installed, the Installer displays a *Installation Complete* dialog, see [Figure 9](#). If the Internet Authentication Server component was installed, then the IAS server will need to be restarted.

Figure 9 Installation Complete

Any problems encountered during installation will result in an error message being displayed and the installation aborted. You will need to manually fix the problem before restarting the installation.

If during the installation of the Active Directory Server Extensions feature the Network Access Manager schema extensions are found to already be configured in the domain then this will be reported on the Installation Complete dialog which will also include a reference to the AD-Information.txt file which will contain details of the schema changes.

- 11** Repeat steps 1 to 8 for any other PC being used for RADIUS, Administrator or Operator users.

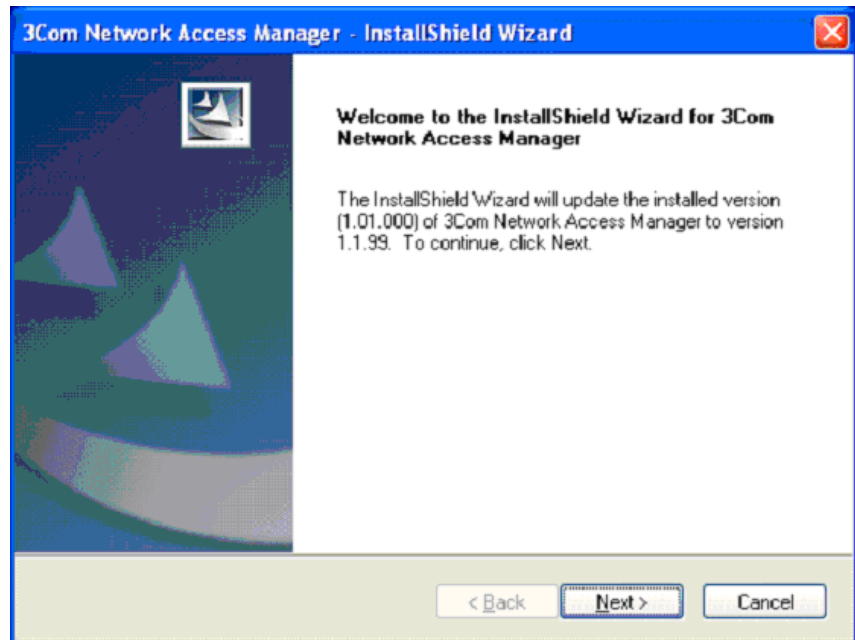
Upgrading an Existing Installation

This section describes the how the installer behaves when an upgrade is carried on a system which has a previous version of 3Com Network Access Manager installed. In this case a different set of options are presented as described below.

To upgrade an existing installation:

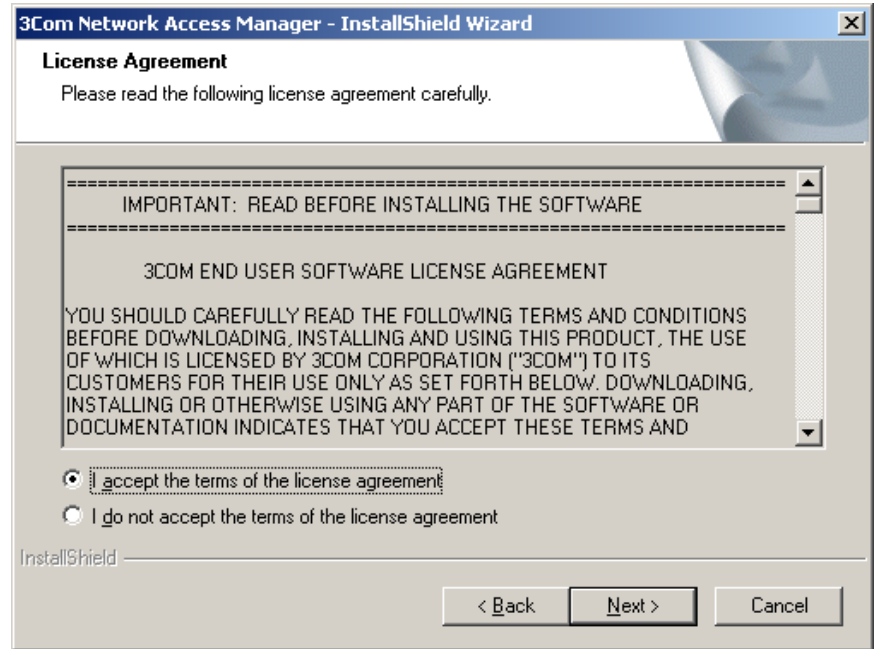
- 1 Carry out steps 1 to 3 as described in [“New Installation”](#).
- 2 After the initial splash screen and the background dialog has displayed and the initial installation checks have all passed, the Welcome dialog displays indicating the old and new version numbers as shown in [Figure 10](#).

Figure 10 InstallShield Wizard Upgrade Welcome Dialog



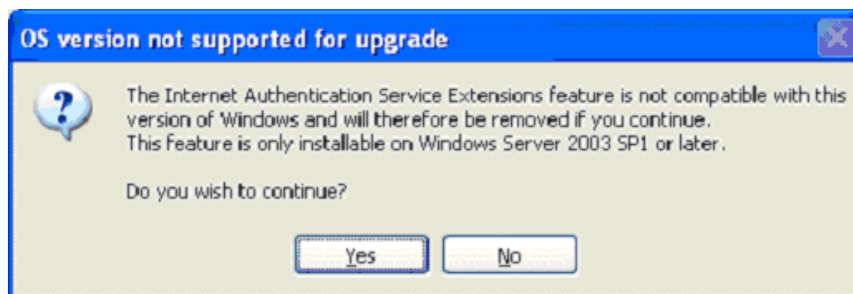
- 3 Select *Next*, the *End User License Agreement* will display, [Figure 11](#).

Figure 11 End User Licence Agreement dialog



To continue the installation select *I accept the terms of the license agreement*, and press the *Next* button. Otherwise, select *Back* to move to the previous dialog or *Cancel* to end the installation.

- 4 On the next dialog select the features to be installed on the PC. Any unticked features will be removed if already installed on the PC. Select *Next* to continue with the installation.
- 5 If the Internet Authentication Service Extension is installed a check is made that the target Operating System version is supported. If the target OS is not supported then the dialog is displayed as shown in [Figure 12](#).

Figure 12 OS Version not supported for Upgrade Message

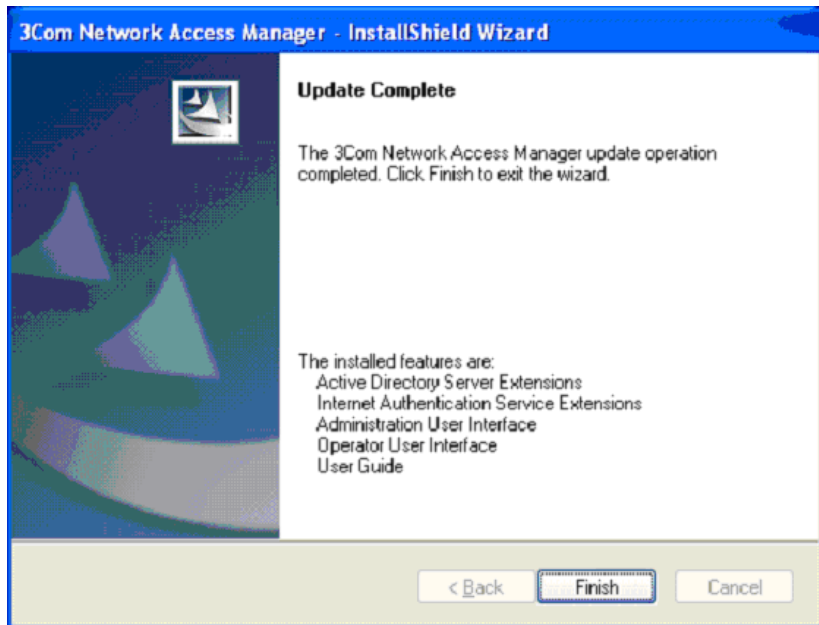
If you select **Yes** the Internet Authentication Service Extensions feature will be removed during the installation operation, otherwise the installation will be aborted.

- 6 If the Internet Authentication Service Extensions feature is being installed then the following additional actions apply:
 - If the authorization plug-in configuration files already exist in the destination location then you are prompted to select whether these files should be retained or replaced with the default files.



If you chose to replace the existing configuration files they will be renamed so that that can still be recovered if you later wish to revert to using them.

- If the IAS service is running then you will be asked if the IAS service should be restarted during the upgrade.
- 7 The Installer will check the hard disk space available on the PC. If sufficient disk space is available, the installer will install the selected features. After the installation is complete, the Upgrade Complete Dialog displays as shown in [Figure 13](#).

Figure 13 Upgrade Complete Dialog

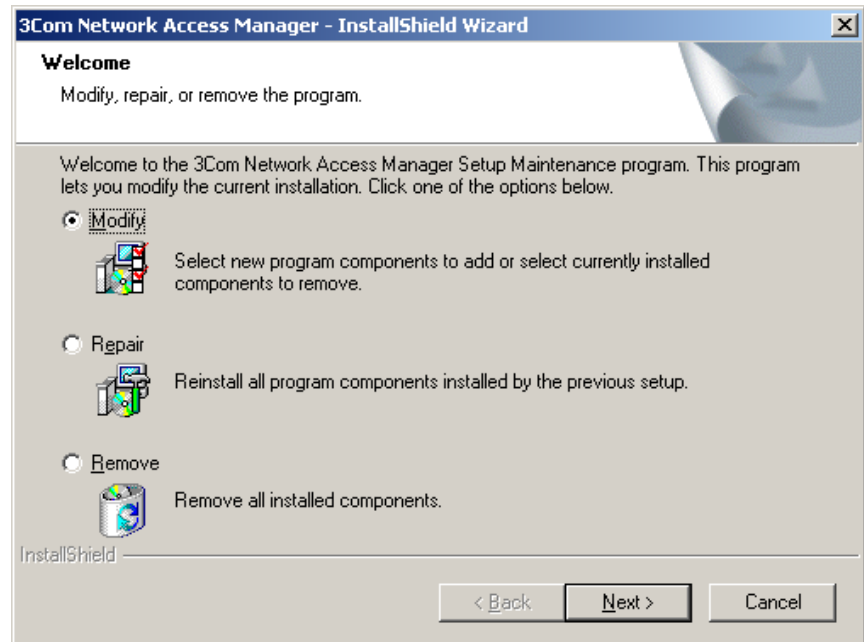
Modifying and Repairing An Installation



To change the 3Com Network Access Manager components installed on a PC or repair an existing installation, follow the steps below.

All computers with 3Com Network Access Manager installed in a domain should be updated to the same version of 3Com Network Access Manager.

- 1** Insert the 3Com Network Access Manager CD in the PC's CDROM drive. If Autorun is enabled on the PC, the installation starts automatically and you can skip steps 2 and 3.
- 2** From the *Start* menu, select *Run*.
- 3** Type `D:\setup` (substitute the appropriate letter of your CD-ROM drive for D), and click *OK*.
- 4** The splash screen will display followed by the *Maintenance* dialog, see [Figure 14](#).

Figure 14 Maintenance dialog

- 5 Click on the *Modify* button to change the components installed on the PC.

- a The *Select Components* dialog will display.
- b Tick the components to be installed.
- c Any unticked components will be removed if already installed on the PC.
- d Click *Next*. The Installer will check the hard disk space available on the PC. If sufficient disk space is available, the installer will install the components selected.



If insufficient disk space is available, an error message is displayed, and the installation will stop until sufficient space is made available.

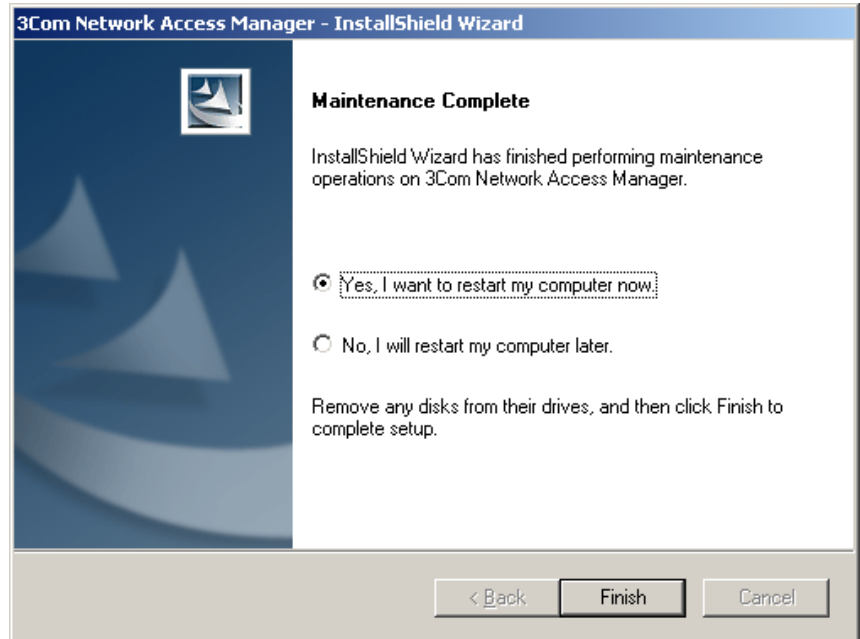
- 6 Click on the *Repair* button to repair an existing 3Com Network Access Manager installation on a PC. All of the currently installed 3Com Network Access Manager components will be reinstalled on the PC.



If the original installation included the Active Directory Server component, then repairing the installation will give a warning message on the Maintenance Complete dialog that the Active Directory

components are already present in Active Directory. This will not affect Active Directory.

Figure 15 Maintenance Complete dialog

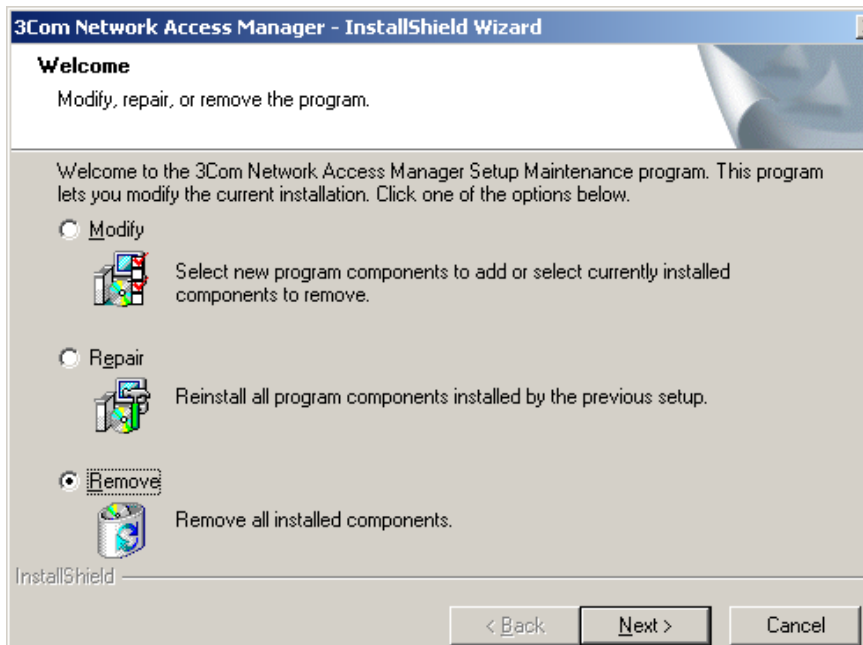


- 7 Click *Finish* to exit the Maintenance program. If the Internet Authentication Server component was installed, then the IAS server will need to be restarted.

Uninstalling 3Com Network Access Manager

To uninstall the 3Com Network Access Manager components from a PC, follow these steps:

- 1 Insert the 3Com Network Access Manager CD in the PC's CDROM drive. If Autorun is enabled on the PC, the installation starts automatically and you can skip steps 2 and 3.
- 2 From the *Start* menu, select *Run*.
- 3 Type `D:\setup` (substitute the appropriate letter of your CD-ROM drive for D), and click *OK*.
- 4 The splash screen will display followed by the *Maintenance* dialog, see [Figure 16](#).

Figure 16 Maintenance dialog

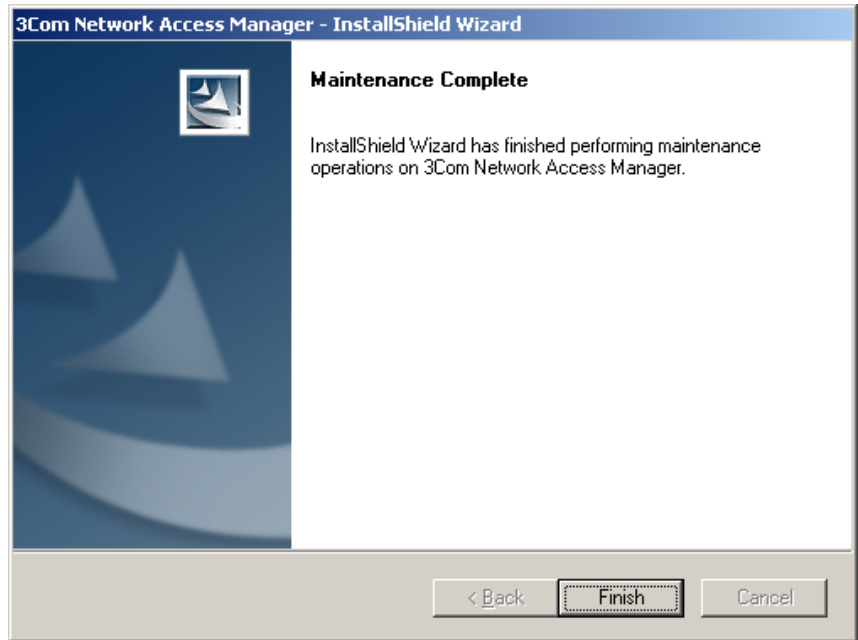
- 5 Click on the *Remove* button. On the next dialog, click *Yes* to remove the 3Com Network Access Manager components installed on the PC, click *No* to stop the uninstall and return to the *Maintenance* dialog.



The extensions made to Active Directory by the Active Directory Server component cannot be removed.

- 6 After the 3Com Network Access Manager components have been removed from the PC, the *Maintenance Complete* dialog will display, see [Figure 17](#). Click on the *Finish* button.

Figure 17 Maintenance Complete dialog



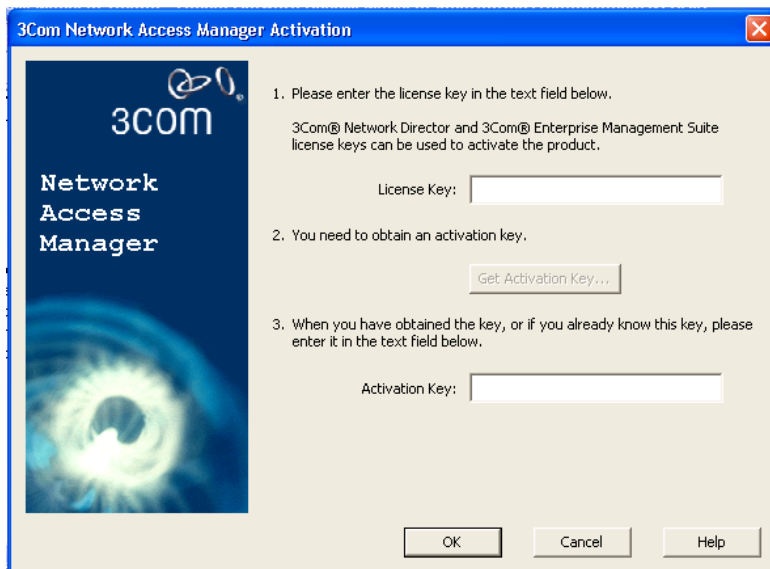
Activating 3Com Network Access Manager

To license 3Com Network Access Manager you have to 'activate' the product.

To activate 3Com Network Access Manager:

- 1 Select *About > Activate Now* to display the 3Com Network Access Manager Activation dialog as shown in [Figure 18](#).

Figure 18 3Com Network Access Manager Activation Dialog



- 2 Enter either the License Key for 3Com Network Director or 3Com Enterprise Management Suite to activate 3Com Network Access Manager.
- 3 If you need to obtain a key, click *Get Activation Key....*

When the *Get Activation Key* is clicked the web browser is launched and you must then enter the Product Number (3C number), the Serial Number and the Licence key (another dialog is also launched containing the information which can then be cut and paste into the web page).

The web page can also be manually launched (this is useful if you do not have direct web access from the domain on which 3Com Network Access Manager is being installed).

- 4 Enter the activation key in the Activation Key field and click *OK*.

- 5 After activating 3Com Network Access Manager it is recommended that any IAS Servers with the 3Com Network Access Manager Authorization plug-in installed are restarted so that they become activated immediately.

The *About > 3Com Network Access...* dialog will display the license status of 3Com Network Access Manager. If the 3Com Network Access Manager is operating in the evaluation mode the MMC status bar will display a message that indicates how many days the 3Com Network Access Manager is into the evaluation period when any of the items in the Tree or the Details pane are selected. If an item in the tree or details pane is selected and no message is displayed then the 3Com Network Access Manager is fully activated.

3

GETTING STARTED

This chapter describes:

- how to configure 3Com Network Access Manager after installation, using the Network Administrator User Interface,
- how to configure the User Interface for Network Operators.



Before configuring 3Com Network Access Manager, make sure you have created a Remote Access Policy in IAS that uses 3Com Network Access Manager to authorize users and computers accessing the network, see [Appendix A](#).

Using The Network Administrator User Interface

As a Network Administrator on a network that already employs Microsoft's Active Directory and Internet Authentication Service (IAS) you will be familiar with managing Users, Groups and Computers through the Active Directory MMC console. 3Com Network Access Manager extends these capabilities by providing facilities to:

- set up rules on how NAM VLANs, NAM Policies and EFW Policies are applied,
- edit security profiles for users, groups and computers to include NAM VLAN, NAM Policy and EFW policy information.

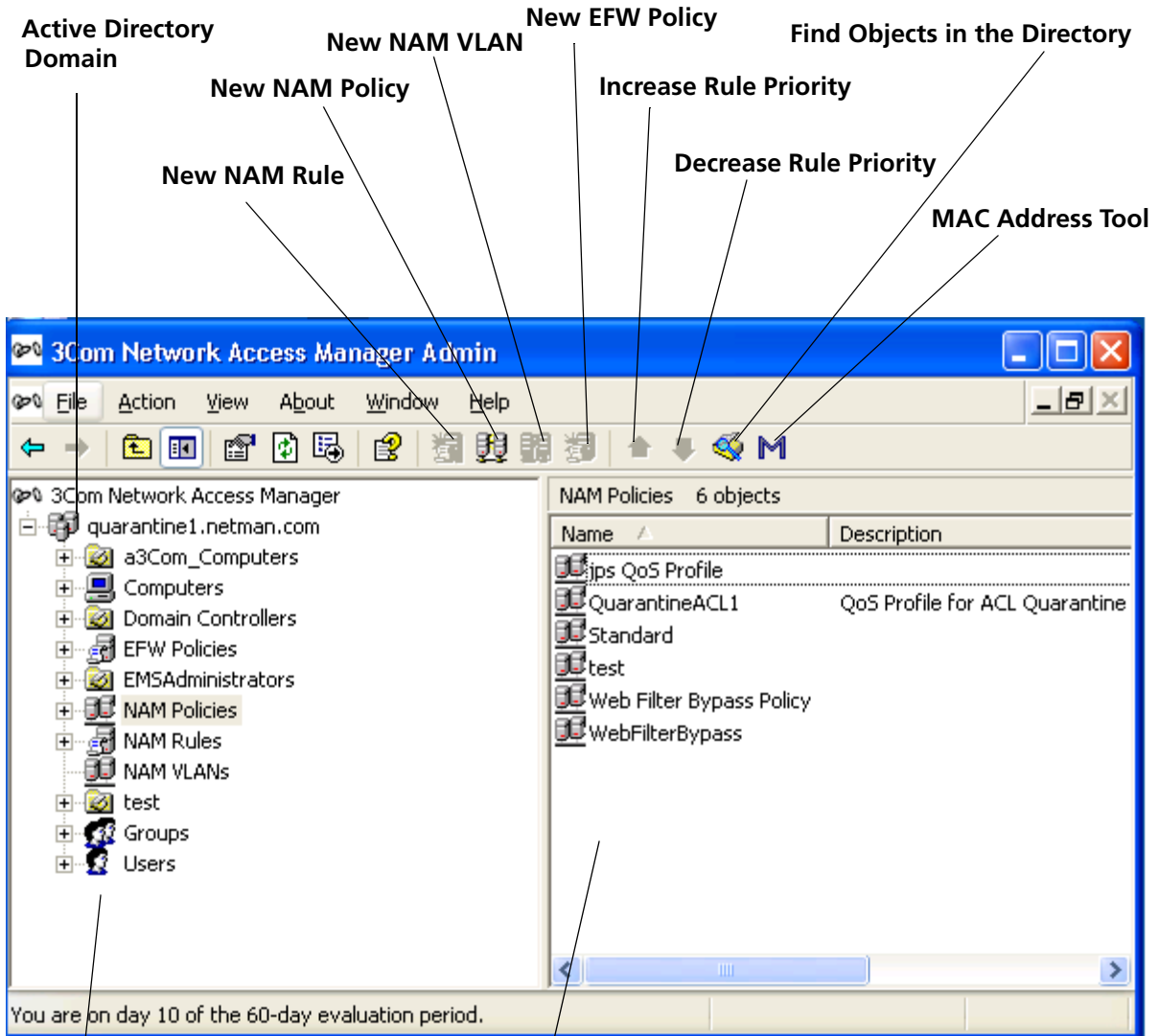
User Interface

To display the Network Administrator's User Interface, select *Start>Control Panel> Administrative Tools >3Com Network Access Manager Admin*

The User Interface is a Microsoft Management Console (MMC) console consisting of a window divided into two panes, see [Figure 19](#). The left pane, called the Tree pane in this guide, displays the console tree and the items that can be configured within the console. The right pane, called

the Details pane, shows information about the item selected in the Tree pane.

Figure 19 Network Administrator User Interface



The Tree pane.
Click on an object in the tree to display a list of items known to the system in the Details pane

The Details pane.
Lists the items known to the system for the object selected in the Tree pane

Setting Up 3Com Network Access Manager

To configure 3Com Network Access Manager after installation, follow these steps:

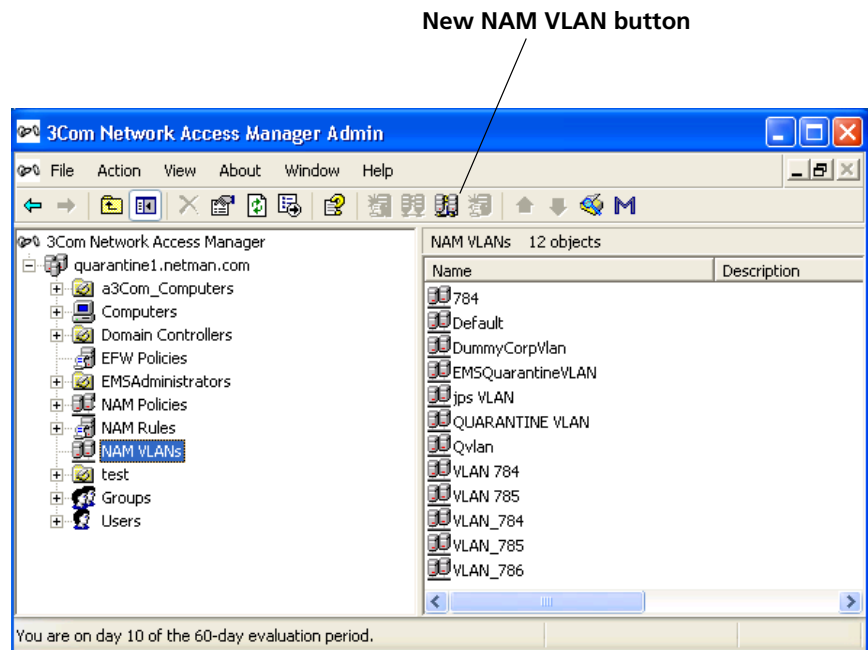


Before adding entries for VLANs, Policies and EFW policies in 3Com Network Access Manager make sure that the network is configured correctly, including VLANs, QoS profiles and EFW policies. These settings must be consistent throughout the entire network.

- 1 Create VLANs, see [“Creating A New NAM VLAN”](#).
- 2 Create Policies, see [“Creating A New NAM Policy”](#).
- 3 Create EFW policies, see [“Creating A New EFW Policy”](#).
- 4 Specify the MAC address(es) for the computers in the domain, see [“Using the MAC Address Tool”](#) or [“Entering MAC Addresses For A Computer”](#).
- 5 Create rules and assign attributes to the rules, see [“Creating A New NAM Rule”](#).
- 6 Ensure the appropriate permissions for each network operator who will use 3Com Network Access Manager have been set, see [“Selecting Appropriate Permissions For An Operator”](#).
- 7 Associate the rules with the users, groups, and computers in the network domain.

NAM VLANs View

Clicking on NAM VLANs in the Tree pane displays in the Detail pane a list of VLANs already entered into 3Com Network Access Manager. Initially the Detail pane will be empty, until one or more VLAN entries have been created, see [“Creating A New NAM VLAN”](#). After a VLAN entry has been created in 3Com Network Access Manager, the Detail pane will show the VLAN Name and ID, see [Figure 20](#).

Figure 20 NAM VLANs View Detail Pane.

Creating A New NAM VLAN

To create a new NAM VLAN entry in 3Com Network Access Manager, follow these steps:

- 1 Either click *NAM VLANs* in the Tree pane and click the *New VLAN* button on the Tool bar, or right-click *VLANs* in the Tree pane and select *New> VLAN*
- 2 In the dialog box enter the name of the new VLAN and the VLAN ID.



The VLAN ID should be a string of characters that match the ID assigned to the VLAN in the network access device (switch or wireless access point). For maximum compatibility with supported devices use numeric IDs.

- 3 Click *OK* to create the VLAN.

The VLAN name will be checked to ensure it is valid and unique, and the new VLAN name and ID will be added to the list of VLANs shown in the Detail pane of the VLAN view.

This completes creating a new VLAN entry in 3Com Network Access Manager.



The configuration file determines when to return VLAN Name and when to return VLAN ID in the RADIUS response. See [“Customizing the Configuration Files”](#).

You can now associate rules with this VLAN if the rules have already been created, see [“Changing NAM Rule Properties”](#).

Deleting An Existing NAM VLAN

To delete an existing NAM VLAN entry in 3Com Network Access Manager, follow these steps:

- 1 Click on *NAM VLANs* in the Tree pane. The Details pane on the right will list all of the VLANs in 3Com Network Access Manager.
- 2 Select the VLAN to delete and right-click. Select *Delete*.
- 3 Click Yes to confirm deleting the VLAN from 3Com Network Access Manager.



You can select multiple NAM VLANs for the delete operation.



If you delete a VLAN which is associated with one or more rules, then the rules are updated to have a VLAN assignment of 'Unspecified'.

Renaming A NAM VLAN And Changing The VLAN ID

To rename an existing NAM VLAN entry in 3Com Network Access Manager, follow these steps:

- 1 Click on *NAM VLANs* in the Tree pane. The Details pane on the right will list all of the VLANs in 3Com Network Access Manager.
- 2 Select the VLAN to rename and right-click. Select *Rename*.
- 3 Enter the new name for the VLAN and press Return.

This completes renaming the VLAN entry in 3Com Network Access Manager.

To change the NAM VLAN ID of an existing VLAN entry in 3Com Network Access Manager, follow these steps:

- 1 Click on *NAM VLANs* in the Tree pane. The Details pane on the right will list all of the VLANs in 3Com Network Access Manager.
- 2 Select the VLAN to change and right-click. Select *Properties*.

The Properties dialog window will appear.

- 3 Select the *VLAN* tab and change the ID for the VLAN.



The ID should be a string of characters, for example a number, that matches the ID assigned to the VLAN during configuration of the network access device (switch or wireless access point).

- 4 Click *OK*

This completes changing the ID for an existing VLAN entry in 3Com Network Access Manager.

Displaying Rules Associated With A NAM VLAN

To display the rules associated with a NAM VLAN, follow these steps:

- 1 Click on *NAM VLANs* in the Tree pane. The Details pane on the right will list all of the VLANs in 3Com Network Access Manager.
- 2 Select the VLAN to view and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Members* tab, a list of rules associated with the VLAN will be displayed in the window.
- 4 Click *OK* or *Cancel*.

This completes displaying the rules associated with a VLAN.

NAM Policies View

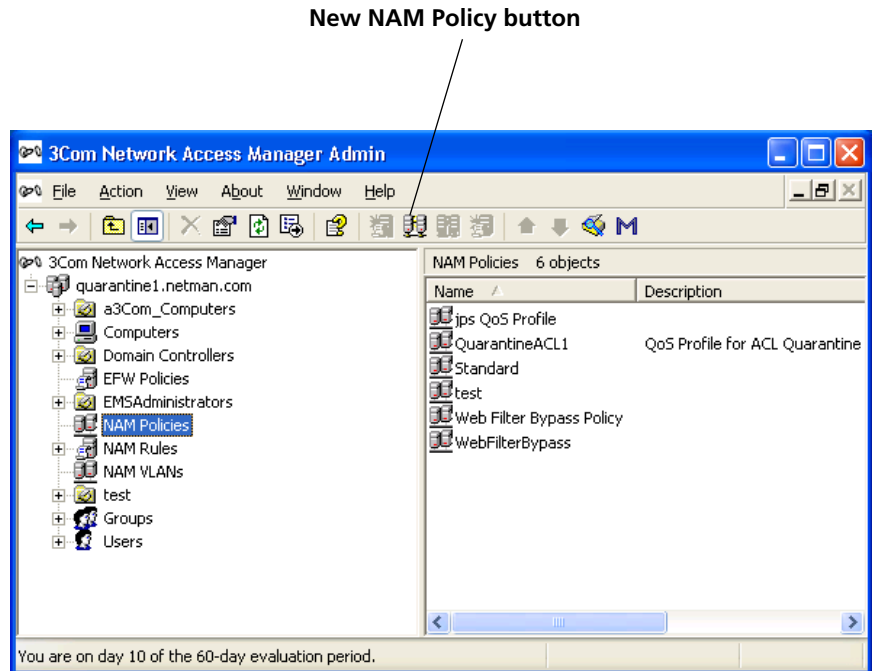
Clicking on NAM Policies in the Tree pane displays in the Detail pane a list of Policies already entered into 3Com Network Access Manager. Initially the Detail pane will be empty, until one or more Policy entries have been created, see [“Creating A New NAM Policy”](#). After a Policy entry has been created in 3Com Network Access Manager, the Detail pane will show the Policy Name and Policy ID, see [Figure 21](#).



Prior to 3Com Network Access Manager Version 1.2, 'NAM Policies' were referred to as 'QoS Profiles'.

Policy provides a powerful means to configure edge ports used to authenticate access to the network. The Policy name and/or ID can be changed on a per RADIUS Client (Switch) basis. The default configuration is to use Policy ID as the NAM Policy setting for the RADIUS Client. See [“Customizing the Configuration Files”](#) on [page 121](#).

Figure 21 NAM Policy View Detail Pane



Creating A New NAM Policy

To create a new NAM Policy entry in 3Com Network Access Manager, follow these steps:

- 1 Either click *NAM Policies* in the Tree pane and click the *New Policy* button on the Tool bar, or right-click *NAM Policies* in the Tree pane and select *New > Policy*
- 2 In the dialog box enter the name of the new Policy and the Policy ID.



The Policy ID should be a string of characters (with no spaces) that match the ID assigned to the NAM Policy in the network access device (switch or wireless access point), otherwise the device may not accept the RADIUS response.

- 3 Click *OK* to create the NAM Policy. The new NAM Policy name and ID will be added to the list of NAM Policies displayed in the Detail pane of the Policies View.

This completes creating a new NAM Policy entry in 3Com Network Access Manager.

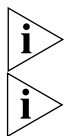
You can now:

- associate rules with this Policy if the rules have already been created, see [“Changing NAM Rule Properties”](#).

Deleting An Existing NAM Policy

To delete an existing NAM Policy in 3Com Network Access Manager, follow these steps:

- 1 Click on *NAM Policies* in the Tree pane. The Details pane on the right will list all of the NAM Policies in 3Com Network Access Manager.
- 2 Select the NAM Policy to delete and right-click. Select *Delete*.
- 3 Click *Yes* to confirm deleting the NAM Policy from 3Com Network Access Manager.



You can select multiple NAM Policies for the delete operation.

If you delete a NAM Policy which is associated with one or more rules, then the rules are updated to have a Policy assignment of 'Unspecified'.

Renaming A NAM Policy And Changing The Policy ID

To rename an existing NAM Policy entry in 3Com Network Access Manager, follow these steps:

- 1 Click on *NAM Policies* in the Tree pane. The Details pane on the right will list all of the NAM Policies in 3Com Network Access Manager.
- 2 Select the NAM Policy to rename and right-click. Select *Rename*.
- 3 Enter the new name for the NAM Policy and press Return.

This completes renaming the NAM Policy entry in 3Com Network Access Manager.

To change the ID of an existing NAM Policy entry in 3Com Network Access Manager, follow these steps:

- 1 Click on *NAM Policies* in the Tree pane. The Details pane on the right will list all of the NAM Policies in 3Com Network Access Manager.
- 2 Select the NAM Policy to change and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Policy* tab and change the ID for the NAM Policy.



The ID should be a string of characters that match the ID assigned to the NAM Policy in the network access device (switch or wireless access point).

- 4 Click *OK* or *Cancel*.

This completes changing the ID for an existing NAM Policy entry in 3Com Network Access Manager.

Displaying Rules Associated With A NAM Policy

To display the rules associated with a NAM Policy, follow these steps:

- 1 Click on *NAM Policies* in the Tree pane. The Details pane on the right will list all of the NAM Policies in 3Com Network Access Manager.
- 2 Select the NAM Policies to view and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Members* tab, a list of rules associated with the Policy will be displayed in the window.
- 4 Click *OK* or *Cancel*.

This completes displaying the rules associated with a Policy.

EFW Policies View

You can enable EFW Support from *View > EFW Support*. By default this option is disabled. The following items are only visible when EFW support is enabled:

- *Recalculate EFW membership* toolbar button.
- *New EFW Policy* toolbar button and menu command.
- EFW Policy column in the Rules detail view.
- EFW Policies container.
- Warning dialog regarding manually updating the EFW Policy membership.

Clicking on EFW Policies in the Tree pane displays in the Detail pane a list of EFW policies already entered into 3Com Network Access Manager. Initially the Detail pane will be empty, until one or more EFW policy entries have been created, see [“Creating A New EFW Policy”](#). After an EFW policy entry has been created in 3Com Network Access Manager, the Detail pane will show the EFW policy name, see [Figure 22](#).

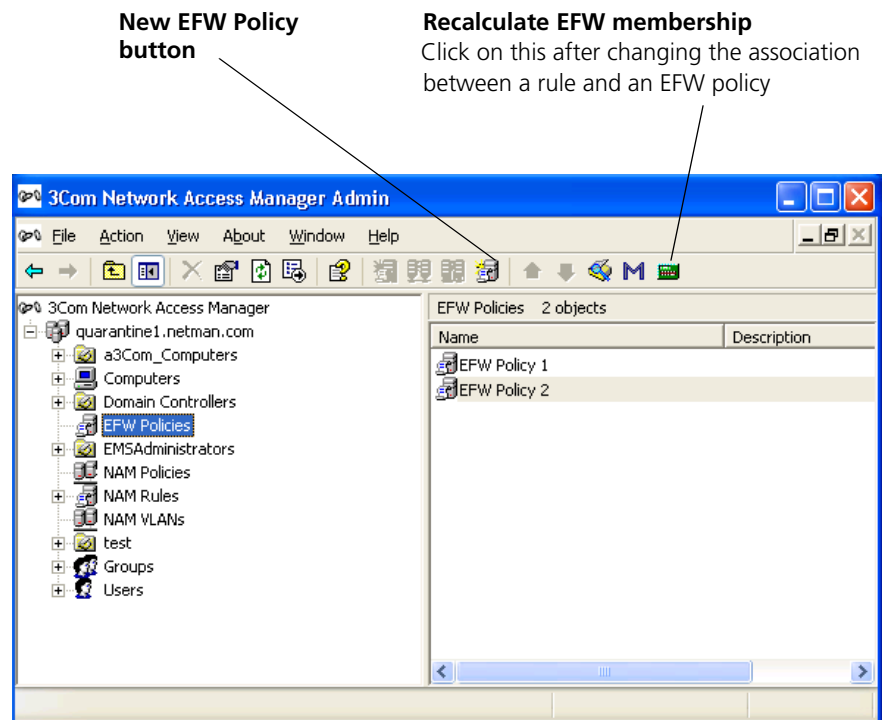
EFW policies are only required if your network includes a 3Com EFW Policy Server.

If an attempt to disable EFW Policy Support is made when EFW Policies exist it will be rejected.

The "EFW Policy" item on the Rule property sheet "Action" pane is only visible if EFW Policies have been defined.

The Find dialog is available from the *Action* menu and from the *Context* menu.

Figure 22 EFW Policies View Detail Pane



Creating A New EFW Policy

Before creating an EFW policy in 3Com Network Access Manager make sure that the EFW policy has already been created in the EFW Policy Server.

To create a new EFW policy entry in 3Com Network Access Manager, follow these steps:

- 1 Either click EFW Policies in the Tree pane and click the *New EFW Policy* button on the Tool bar, or right-click EFW Policies in the Tree pane and select *New> EFW Policy*.
- 2 In the dialog box enter the name of the new EFW policy. The name must be the same as the name assigned to the policy in the EFW Policy Server.



The name must not be the same as the name of a user or group. (An error message is displayed when attempting to create an EFW Policy with a name that matches the name of an existing EFW Policy, user or group.)

- 3 Click *OK* to create the EFW policy. The new EFW policy name will be added to the list of EFW policies shown in the Detail pane of the EFW Policy view.

This completes creating a new EFW policy entry in 3Com Network Access Manager.

You can now:

- associate rules with this EFW policy if the rules have already been created, see [“Changing NAM Rule Properties”](#).

Deleting An Existing EFW Policy

To delete an existing EFW policy in 3Com Network Access Manager, follow these steps:

- 1 Click on EFW Policies in the Tree pane. The Details pane on the right will list all of the EFW policies in 3Com Network Access Manager.
- 2 Select the EFW policy to delete and right-click. Select *Delete*.
- 3 Click on *Yes* to confirm deleting the EFW policy from 3Com Network Access Manager.



You can select multiple EFW Policies for the delete operation.



If you delete an EFW policy which is associated with one or more rules, then the rules are updated to have an EFW policy assignment of 'Unspecified'.

Renaming An EFW Policy

To rename an existing EFW policy entry in 3Com Network Access Manager, follow these steps:

- 1 Click on EFW Policies in the Tree pane. The Details pane on the right will list all of the EFW policies in 3Com Network Access Manager.
- 2 Select the EFW policy to rename and right-click. Select *Rename*.
- 3 Enter the new name for the EFW policy and press Return.

This completes renaming the EFW policy entry in 3Com Network Access Manager.

Displaying Rules Associated With An EFW Policy

To display the rules associated with an EFW policy, follow these steps:

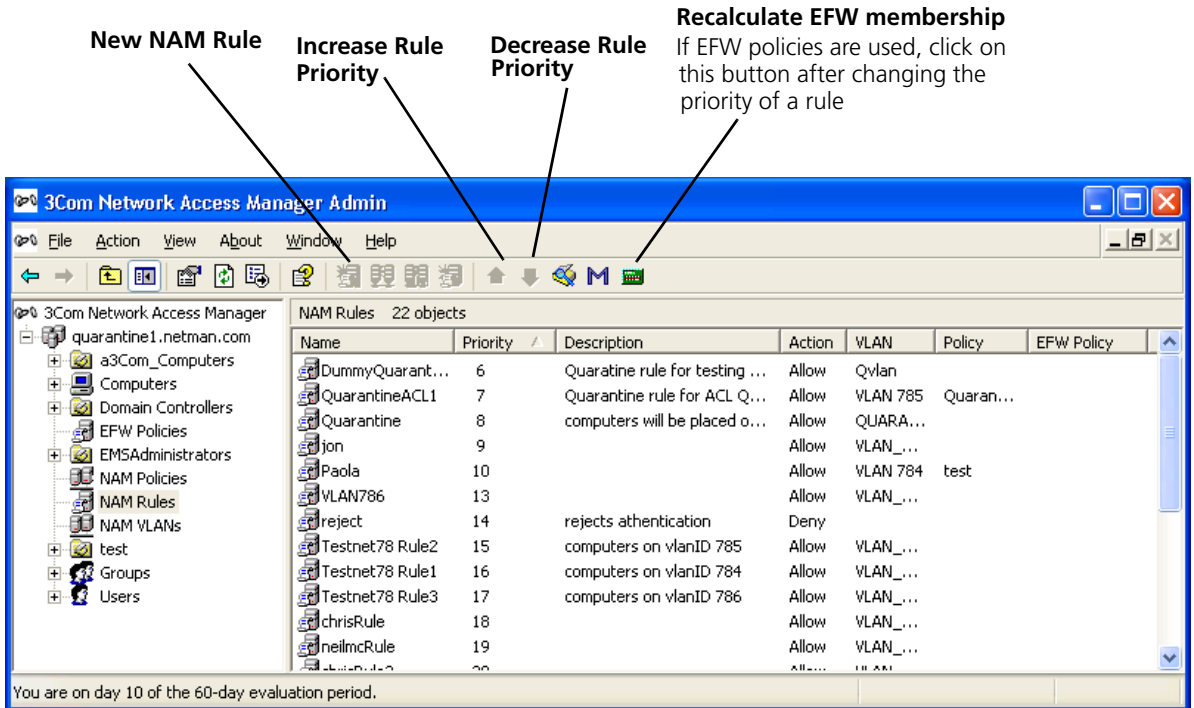
- 1 Click on EFW Policies in the Tree pane. The Details pane on the right will list all of the EFW policies in 3Com Network Access Manager.
- 2 Select the EFW policy to view and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Members* tab, a list of rules associated with the EFW policy will be displayed in the window.
- 4 Click *OK* or *Cancel*.

This completes displaying the rules associated with an EFW policy.

NAM Rules View

Clicking on NAM Rules in the Tree pane displays in the Detail pane a list of rules already entered into 3Com Network Access Manager. Initially the Detail pane will be empty, until one or more rules have been created, see [“Creating A New NAM Rule”](#). After a rule has been created in 3Com Network Access Manager, the Detail pane will show the Priority of the rule, the Rule Name and Description, its Action and the VLANs, Policy and EFW Policy applied to the rule, see [Figure 23](#).

Figure 23 NAM Rules View Detail Pane.



Creating A New NAM Rule

To create a new NAM Rule, assign a priority and network access response to the rule, follow these steps:

- 1 Either click *NAM Rules* in the Tree pane and click the *New Rule* button on the Tool bar, or right-click *NAM Rules* in the Tree pane and select *New>Rule*
- 2 In the dialog box enter the name of the new rule.
- 3 Click *OK* to create the rule.

You now need to set the priority for the rule, which must be unique. The priority determines the order in which rules are examined when a RADIUS request is received. The rule with priority 1 has the highest priority, and will take precedence over all other rules. The new rule will have been assigned the current lowest priority, for example if the lowest priority was 10 before creating the rule, then the new rule will have priority 11.

- 4 Click *NAM Rules* in the Tree pane. The Details pane on the right will list all of the rules.
- 5 Select the newly created rule and use the ↓↑ buttons on the Tool bar to increase or decrease the priority of the rule to match your network security requirements.

Now set the other attributes for the rule.

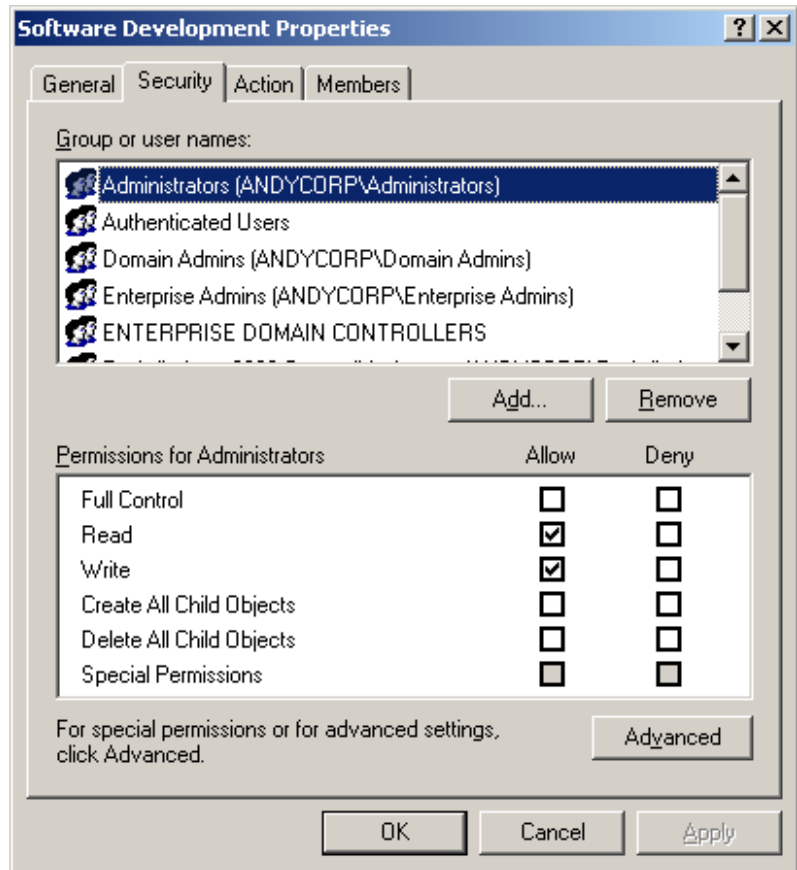
- 6 Select the new rule from the list of rules shown in the Detail pane, and right-click, select *Properties*.

The Properties dialog window will appear.

- 7 Select the *Security* tab to assign security permissions to network administrators and operators who are permitted to apply the rule to users, groups and computers, see [Figure 24](#).
 - a Select a group or user from the list of names in the window and click *Add*.
 - b Select the appropriate security permission to match the role of the group or user, see [Table 7](#).



All Network Administrators must have Read permission for ALL rules to ensure that they can see how rules have been applied, and enable them to troubleshoot access difficulties in the network.

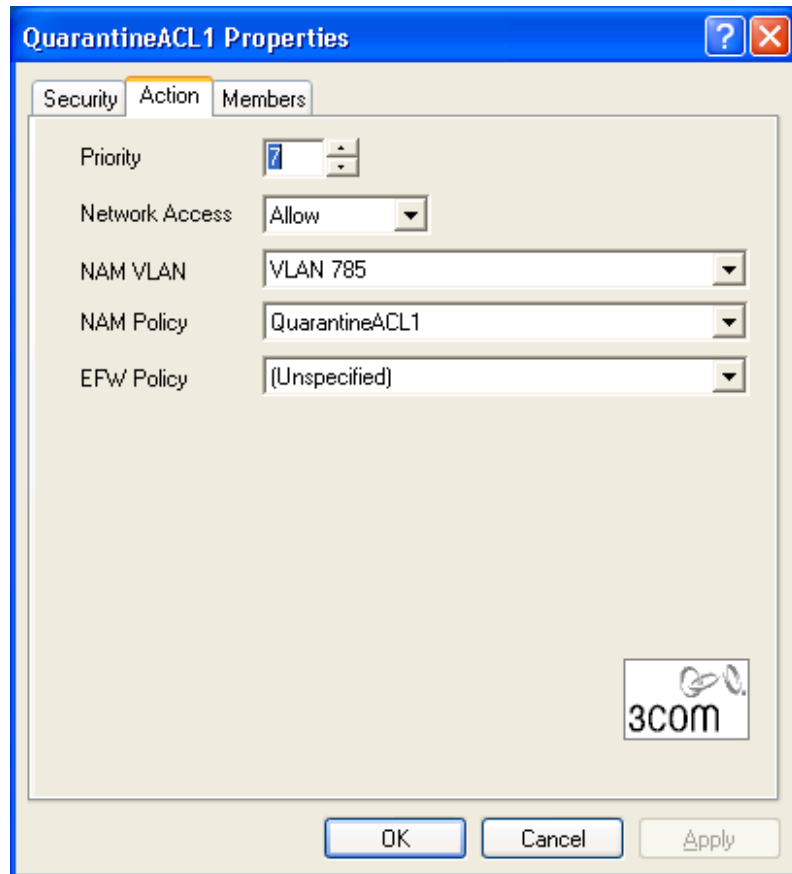
Figure 24 Security Tab For A Rule**Table 7** Selecting Appropriate Rule Permissions

Role	Rule Permissions
Network Administrator(s) or Network Operator(s) allowed to associate the rule with a user, group, or computer	Tick Allow for Read and Write permissions.
Network Administrator(s) not allowed to associate the rule with a user, group, or computer	Tick Allow for Read permission.
Network Operator not allowed to associate the rule with a user, group, or computer	Do not tick any boxes.

- c Repeat steps 7a and 7b for each group and user permitted to assign the rule.

- 8 Select the *Action* tab and configure the action attributes for the rule, [Figure 25](#).

Figure 25 Action Tab For A Rule



- a You changed the Priority setting for the rule in step 5. There is no need to change it again unless you need to assign a different unique priority.
- b Select the Network Access setting that the RADIUS server will return in the RADIUS response, on the rule being obeyed. *Allow* indicates authentication is valid. *Deny* indicates authentication is refused. If you select *Deny* all attributes below Network Access will be grayed out, go to [step 9](#).



To understand the effect of this action, you need to be aware of how the edge port security is set up on the network. In some port modes, the

response may appear illogical, for instance, Allow can be used to implement a blacklist.

- c If Network Access is set to Allow, select the VLAN from the drop down list, this VLAN will be included in the RADIUS response if the rule is obeyed. Select the (Unspecified) option to prevent a VLAN from being included in the RADIUS response.



The network access device may interpret the VLAN as a tagged or untagged VLAN depending upon the switch or wireless access point type and configuration.

- d Select the Policy (if any) associated with the rule. The Policy will be included in the RADIUS response if the rule is obeyed. If you do not wish to associate a Policy with the rule, select the (Unspecified) setting.
- e Select the EFW policy (if any) associated with the rule. If you do not wish to associate an EFW policy with the rule, select the (Unspecified) setting.



EFW policy information is NOT returned in a RADIUS response

- 9 Select the Members tab to display a list of members (users, groups or computers) associated with the rule. At this stage the list will be empty.
- 10 Click OK

This completes creating a new rule in 3Com Network Access Manager, you now need to associate users, groups and computers with the rule. Follow the steps in ["Associating Rules With A User"](#), ["Associating Rules With A Group"](#), ["Associating Rules With A Computer"](#) as appropriate.

Deleting An Existing NAM Rule

To delete an existing NAM Rule in 3Com Network Access Manager, follow these steps:

- 1 Click on NAM Rules in the Tree pane. The Details pane on the right will list all of the rules in 3Com Network Access Manager.
- 2 Select the rule to delete and right-click. Select Delete.
- 3 Click Yes to confirm deleting the rule from 3Com Network Access Manager.



You can select multiple NAM Rules for the delete operation.



CAUTION: Do NOT delete or rename the default rule.

Controlling Permission To Apply A NAM Rule

Selecting who has permission to apply a NAM Rule, is performed when the rule is created. Permissions can be changed after a rule is created, providing the user or group making the change has write permission for the rule.

To change permissions on a rule, follow these steps:

- 1 Click on *NAM Rules* in the Tree pane. The Details pane on the right will list all of the rules in 3Com Network Access Manager.
- 2 Select the rule to change and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the Security tab. Follow the instructions in [step 7](#) of "[Creating A New NAM Rule](#)" to re-assign permissions for the rule.

Changing NAM Rule Priorities

Setting the priority of a NAM rule, is performed when the rule is created. The rule priority can be changed after a rule is created, providing the user or group making the change has write permission for the rule. Priority 1 is the highest priority, a rule assigned priority 1 will take precedence over all other rules. A rule assigned priority 2 will take precedence over rules assigned a priority of 3, 4...The Default Rule has the lowest priority.

To change the priority of a rule, follow these steps:

Either:

- 1 Click on *NAM Rules* in the Tree pane. The Details pane on the right will list all of the rules in 3Com Network Access Manager.
- 2 Select the rule to change and use the **↕** buttons on the Tool bar to increase or decrease the priority of the rule to match your network security requirements. Ensure the rule has a unique priority.
- 3 If EFW policies are used, click on the Recalculate EFW Membership button in the Tool bar after changing the rule priorities.

Or:

- 1 Click *NAM Rules* in the Tree pane. The Details pane on the right will list all of the rules in 3Com Network Access Manager.
- 2 Select the rule to change and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Action* tab and select the Priority for the rule. .

- 4 Click *OK*.
- 5 If EFW policies are used, click on the Recalculate EFW Membership button in the Tool bar after changing the rule priorities.

Changing NAM Rule Properties

Selecting the properties for a rule is performed when the rule is created. Rule properties can be changed after a rule is created, providing the user or group making the change has write permission for the rule.

To change properties for a rule, follow these steps:

- 1 Click on *NAM Rules* in the Tree pane. The Details pane on the right will list all of the rules in 3Com Network Access Manager.
- 2 Select the rule to change and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Action* tab. Follow the instructions in [step 8 of "Creating A New NAM Rule"](#) to select different properties for the rule.



If EFW policies are used, click on the Recalculate EFW Membership button in the Tool bar after changing the rule properties.

Displaying Members Of A NAM Rule

To display all of the members (users, groups and computers) associated with a rule, follow these steps:

- 1 Click on *NAM Rules* in the Tree pane. The Details pane on the right will list all of the rules in 3Com Network Access Manager.
- 2 Select the rule to view and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Members* tab. The members associated with the rules will be listed in the window.
- 4 Click *OK*

Changing Members Of A NAM Rule

To add or remove users associated with a rule, refer to ["Displaying And Changing Rules Associated With A User"](#).

To add or remove groups associated with a rule, refer to ["Displaying And Changing Rules Associated With A Group"](#).

To add or remove computers associated with a rule, refer to [“Displaying And Changing The Rules And MAC Address Associated With A Computer”](#).

Users View

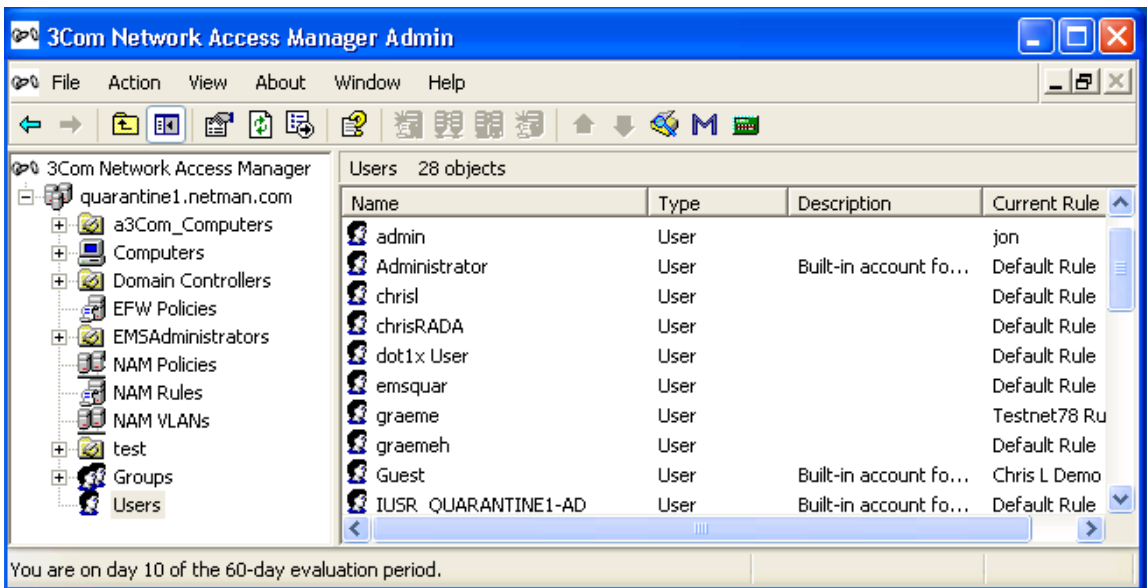
Clicking on Users in the Tree pane displays in the Detail pane a list of Users which already exist in the domain, see [Figure 26](#). Alternatively if you have created Organizational Units to structure your users, click on the organizational units subfolders until you reach the desired unit holding the user.

In the Detail pane, the Current Rule column indicates the rule with the highest priority that is associated with a user, and which is used for authorization of the user. A new user without specific rules applied, will have the Default Rule in the Current Rule column.



The current rule for a user may be overridden by MAC address related settings, for example, if the MAC address of a user's PC was blocked because the PC was infected, it would usually be set to override the user's own allocations.

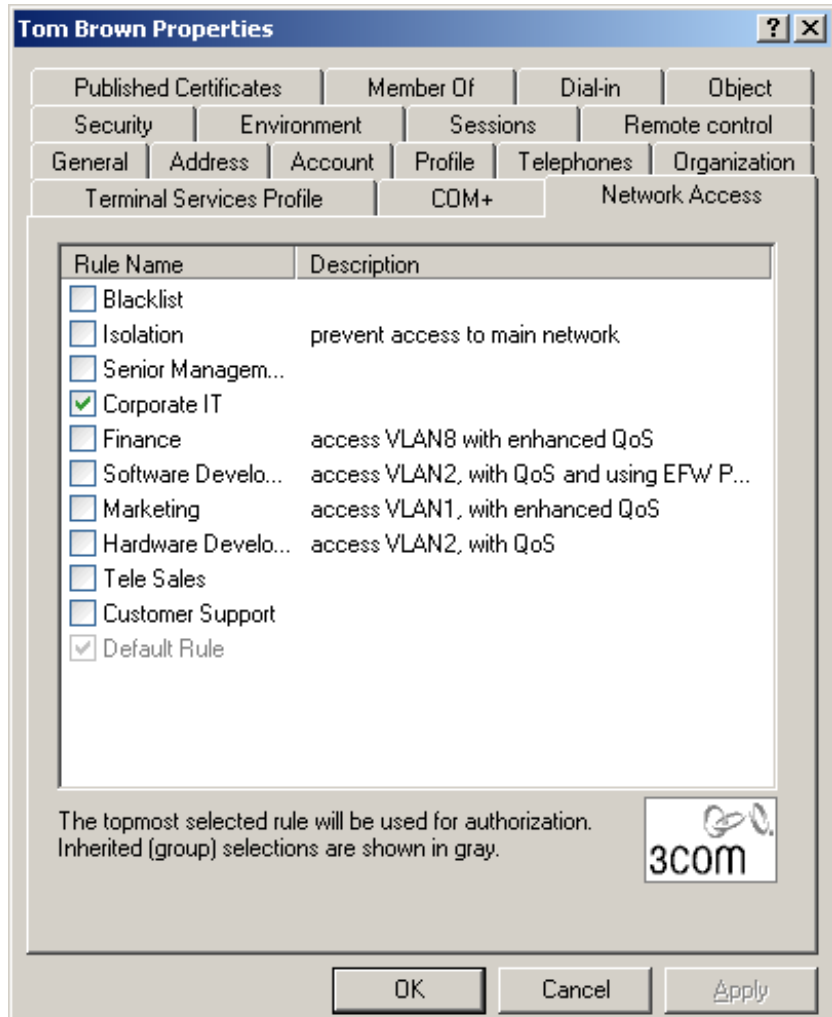
Figure 26 Users View Detail Pane.



Associating Rules With A User

All users in the domain will have the Default Rule applied until they are associated with other rules created with 3Com Network Access Manager. To associate a rule(s) with a user, follow these steps:

- 1** Either click on *Users* in the Tree pane or if you have created Organizational Units to structure your users, click on the organizational units subfolders until you reach the desired unit holding the user.
- 2** Select the user in the Details pane and right-click. Select *Properties*. The Properties dialog window will appear.
- 3** Select the *Network Access* tab, a list of rules created with 3Com Network Access Manager and for which you have read permission will be displayed in the window, see [Figure 27](#).

Figure 27 Network Access Tab

- 4 Tick the box beside each rule that is to be associated with the user. If the rule is grayed out then the user is a member of a group which is already associated with the rule.



A user can be associated with multiple rules, however only the highest priority rule associated with the user will be used for the RADIUS authorization.

- 5 Click OK
This completes associating rules with a user.

Displaying And Changing Rules Associated With A User

To display and change the rules associated with a user, follow these steps:

- 1 Either click on Users in the Tree pane or if you have created Organizational Units to structure your users, click on the organizational units subfolders until you reach the desired unit holding the user.
- 2 Select the user in the Details pane and right-click. Select *Properties*. The Properties dialog window will appear.
- 3 Select the *Network Access* tab, a list of rules created with 3Com Network Access Manager and for which you have read permission will be displayed in the window, see [Figure 27](#). The tick box indicates how the rule is to be applied to the user, see [Table 8](#).

Table 8 Rules Tick Box For A User

Tick Box Setting	Meaning
Black, not ticked	The rule does not apply to this user
Black, ticked	The rule is applied to this user
Grey, ticked	The rule is applied to this user indirectly through the user's membership of one or more groups that have the rule specifically applied

- 4 You can change which of these rules are applied to a user by either ticking or removing the tick from rules that are black. To change a rule that is applied indirectly through a group, see [“Displaying And Changing Rules Associated With A Group”](#).



A user can be associated with multiple rules, however only the highest priority rule associated with the user will be used for the RADIUS authorization.

- 5 Click *OK*
This completes displaying and changing the rules associated with a user.



DO NOT change rule membership using the Members Of tab.

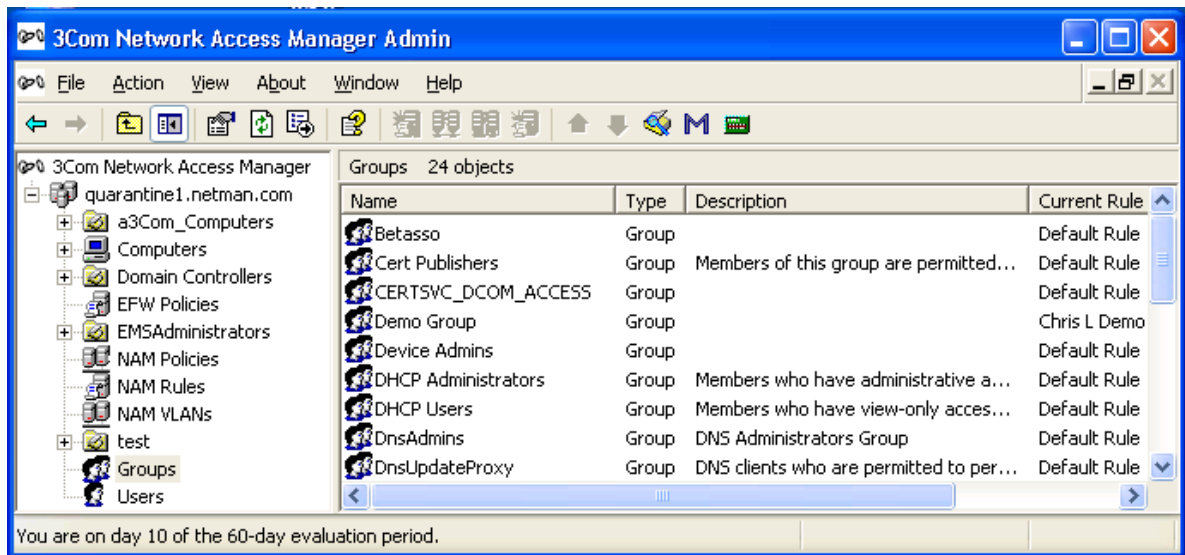
Creating A New User

To create a new user in the system, you will need to use a tool such as the “Active Directory Users and Computers” administration tool. You cannot create users through 3Com Network Access Manager. Follow the instructions given in the user documentation shipped with Microsoft Active Directory.

Groups View Clicking on Groups in the Tree pane displays in the Detail pane a list of Groups which already exist in the domain, see [Figure 28](#). Alternatively if you have created Organizational Units to structure your groups, click on the organizational units subfolders until you reach the desired unit holding the group.

The Current Rule column indicates the rule with the highest priority that is associated with a group, and which is used for authorization of the group. A new group without specific rules applied, will have the Default Rule in the Current Rule column.

Figure 28 Groups View Detail Pane



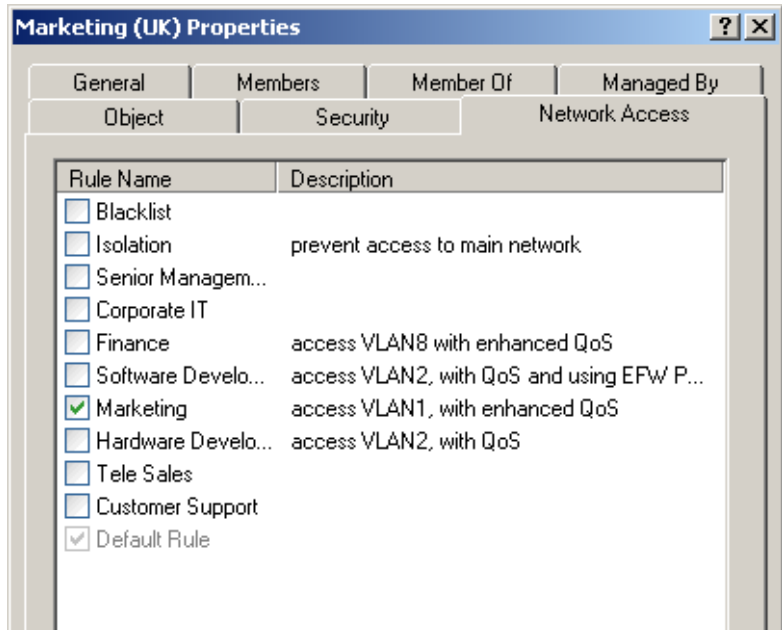
Associating Rules With A Group

All groups in the domain will have the Default Rule applied until they are associated with other rules created with 3Com Network Access Manager. To associate a rule(s) with a group, follow these steps:

- 1 Either click on Groups in the Tree pane or if you have created Organizational Units to structure your groups, click on the organizational units subfolders until you reach the desired unit holding the group.
- 2 Select the group in the Details pane and right-click. Select *Properties*. The Properties dialog window will appear.

- 3 Select the *Network Access* tab, a list of rules created with 3Com Network Access Manager and for which you have read permission will be displayed in the window, see [Figure 29](#).

Figure 29 Network Access Tab



- 4 Tick the box beside each rule that is to be associated with the group. If the rule is grayed out then the group is a member of a group which is already associated with the rule.



A group can be associated with multiple rules, however only the highest priority rule associated with the group will be used for the RADIUS authorization.

- 5 Click OK

This completes associating rules with a group.

Displaying And Changing Rules Associated With A Group

To display and change the rules associated with a group, follow these steps:

- 1 Either click on Groups in the Tree pane or if you have created Organizational Units to structure your groups, click on the organizational units subfolders until you reach the desired unit holding the group.
- 2 Select the group in the Details pane and right-click. Select *Properties*.

The Properties dialog window will appear.

- 3 Select the *Network Access* tab, a list of rules created with 3Com Network Access Manager and for which you have read permission will be displayed in the window, see [Figure 29](#). The tick box indicates how the rule is to be applied to the group, see [Table 9](#).

Table 9 Rules Tick Box for A Group

Tick Box Setting	Meaning
Black, not ticked	The rule does not apply to this group
Black, ticked	The rule is applied to this group
Grey, ticked	The rule is applied to this group indirectly through the group's membership of one or more groups that have the rule specifically applied

- 4 You can change which of these rules are applied to a group by either ticking or removing the tick from rules that are black.



To change the rules applied indirectly through being a member of another group, select the other group from the Detail pane and apply steps 1 to 4 above on the other group.



A group can be associated with multiple rules, however only the highest priority rule associated with the group will be used for the RADIUS authorization.

- 5 Click *OK*
- 6 If EFW policies are used, click on the *Recalculate EFW Membership* button.

This completes displaying and changing the rules associated with a group.



*DO NOT change rule membership using the *Members Of* tab.*

Creating A New Group

To create a new group in the system, you will need to use a tool such as the "Active Directory Users and Computers" administration tool. You cannot create groups through 3Com Network Access Manager. Follow the instructions given in the user documentation shipped with Microsoft Active Directory.

Computers View

Clicking on Computers in the Tree pane displays in the Detail pane a list of Computers known to the domain, see [Figure 30](#). Alternatively if you

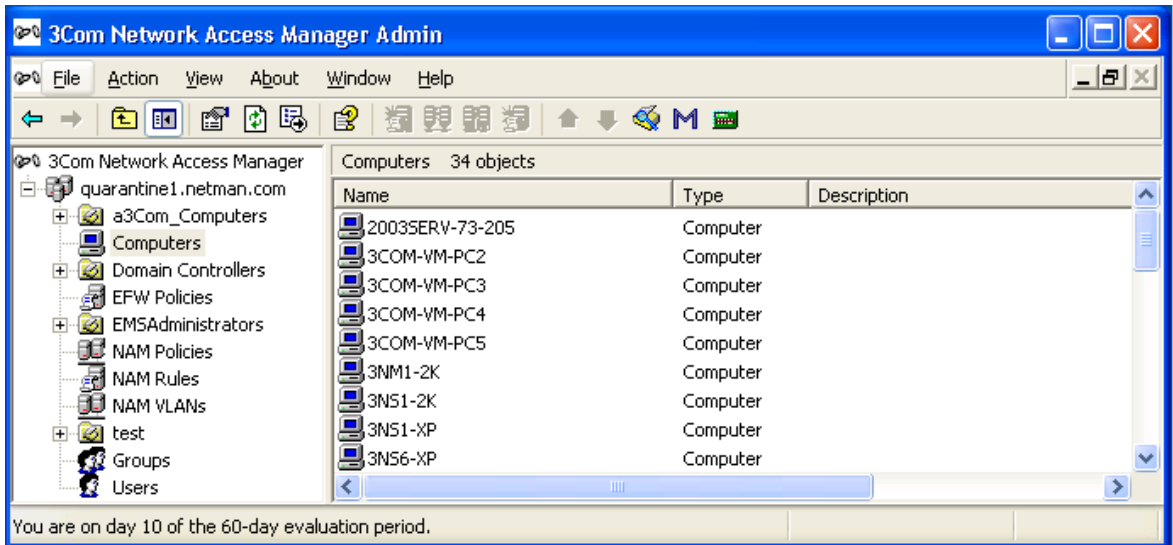
have created Organizational Units to structure your computers, click on the organizational units subfolders until you reach the desired unit holding the computer.

The Current Rule column indicates the rule with the highest priority that is associated with a computer, and which is used for authorization of the computer. A computer without specific rules applied, will have the Default Rule in the Current Rule column.



The current rule for a computer may be overridden by user related settings.

Figure 30 Computers View Detail Pane



Entering MAC Addresses For A Computer

To use MAC-address based authentication, the computers in the domain need to have their MAC addresses entered into 3Com Network Access Manager. To enter the MAC address(es) for a computer follow these steps:

- 1 Either click on *Computers* in the Tree pane or if you have created Organizational Units to structure your computers, click on the organizational units subfolders until you reach the desired unit holding the computer.
- 2 Select the computer in the Details pane and right-click. Select *Properties*.

The Properties dialog window will appear.

- 3 Select the *MAC Address* tab. You can manually enter the MAC Address(es) of the computer in the field provided and click *Add*, or you can retrieve the MAC Addresses live from the device by clicking *Live MAC Addresses*.
- 4 Click *OK*

This completes entering a MAC address for a computer.



3Com Network Access Manager has a MAC Address Tool that can be used to easily update all or a selection of computers MAC Addresses. See [“Using the MAC Address Tool”](#).

Associating Rules With A Computer

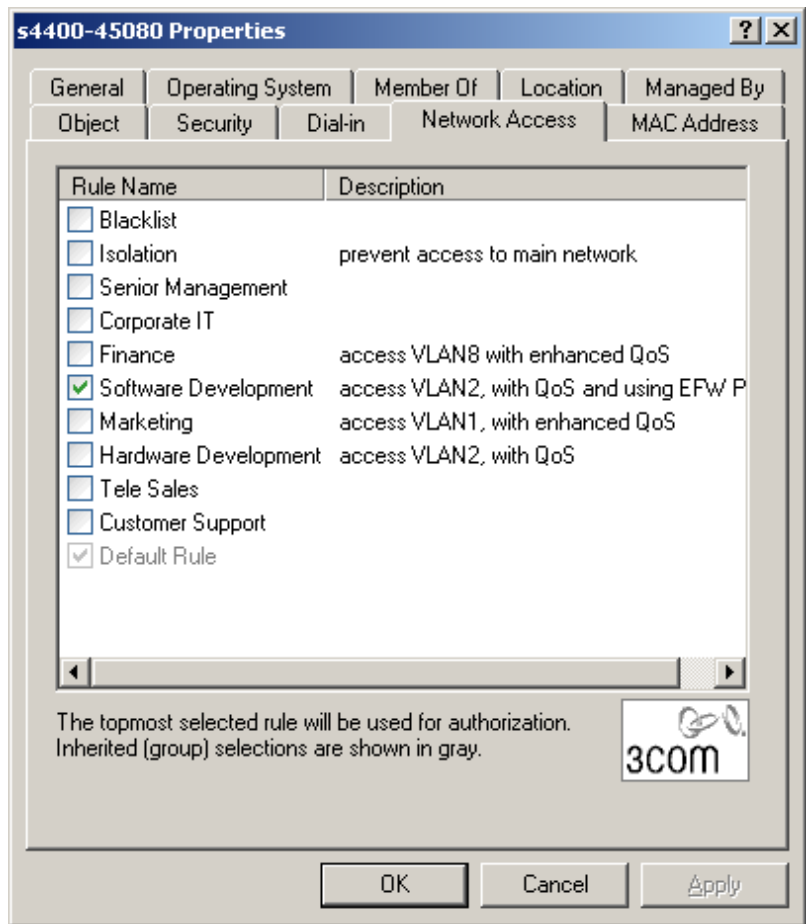


Ensure you have entered the MAC address of the computer in your network, before associating rules with the computer. 3Com Network Access Manager will only apply a rule to the computer if the RADIUS request includes the MAC address as the Calling-Station-Id.

All computers in the domain will have the Default Rule applied until they are associated with other rules created with 3Com Network Access Manager. To associate a rule(s) with a computer, follow these steps:

- 1 Either click on Computers in the Tree pane or if you have created Organizational Units to structure your computers, click on the organizational units subfolders until you reach the desired unit holding the computer.
- 2 Select the computer in the Details pane and right-click. Select *Properties*. The Properties dialog window will appear.
- 3 Select the *Network Access* tab, a list of rules created with 3Com Network Access Manager and for which you have read permission will be displayed in the window, see [Figure 31](#).

Figure 31 Network Access Tab



- 4 Tick the box beside each rule that is to be associated with the computer. If the rule is grayed out then the computer is a member of a group which is already associated with the rule.



A computer can be associated with multiple rules, however only the highest priority rule associated with the computer will be used for the RADIUS authorization.

- 5 Click OK
This completes associating rules with a computer.

Displaying And Changing The Rules And MAC Address Associated With A Computer

To display and change the rules and MAC addresses associated with a computer, follow these steps:

- 1 Either click on Computers in the Tree pane or if you have created Organizational Units to structure your computers, click on the organizational units subfolders until you reach the desired unit holding the computer.
- 2 Select the computer in the Details pane and right-click. Select *Properties*. The Properties dialog window will appear.
- 3 Select the *Network Access* tab, a list of rules created with 3Com Network Access Manager and for which you have read permission will be displayed in the window, see [Figure 31](#). The tick box indicates how the rule is to be applied to the computer, see [Table 10](#).

Table 10 Rules Tick Box for A Computer

Tick Box Setting	Meaning
Black, not ticked	The rule does not apply to this computer
Black, ticked	The rule is applied to this computer
Grey, ticked	The rule is applied to this computer indirectly through the computer's membership of one or more groups that have the rule specifically applied

- 4 You can change which of these rules are applied to a computer by either ticking or removing the tick from rules that are black. To change a rule that is applied indirectly through a group, see [“Displaying And Changing Rules Associated With A Group”](#).



A computer can be associated with multiple rules, however only the highest priority rule associated with the computer will be used for the RADIUS authorization.

- 5 Click *Apply* to apply the changes.
- 6 Select the MAC Address tab. Enter the 12 digit MAC address of the computer in the format XX-XX-XX-XX-XX-XX. You can enter multiple MAC Addresses manually.



You can use the MAC Address button on the Properties tab to find and update computers MAC Addresses.

- 7 Click *OK*.

This completes displaying and changing the rules and MAC addresses associated with a computer.

Creating A New Computer

To add a computer to the system, you will need to use a tool such as the “Active Directory Users and Computers” administration tool. You cannot add computers through 3Com Network Access Manager. Follow the instructions given in the user documentation provided with Microsoft Active Directory.

Selecting Appropriate Permissions For An Operator

The actions that a Network Operator can apply, can be individually selected for the operator. For example, one operator may be restricted to blocking access for specific users, whereas another operator may be allowed to move users between arbitrary groups.

Selecting the actions that an operator can apply, is achieved through the securities permission of the rule, see [step 7](#) of [“Creating A New NAM Rule”](#) on [page 57](#). By selecting the name of the operator from the *Group or User name* list and ticking the *Allow* box for both read and write, enables the network operator to apply the rule. Not ticking the *Allow* box for read and write permission will prevent the network operator from applying the rule.

By using the permissions model, network administrators can decide who is permitted to apply rules to users, groups and computers to control network access. In some organizations it may not be appropriate to let operators have this responsibility.



Security permissions on a rule do not affect the security permissions on individual users. If a network operator does not have security permission for particular individuals or groups, for example directors of a company, then the operator will not be able to apply a rule to that user or group.

Using the MAC Address Tool

To allow NAM Rules to be successfully assigned to computers 3Com Network Access Manager requires that a computer account should have MAC Address information. You can add or update a MAC Address associated with a Computer account using the MAC Address Tool. Alternatively, you can manually configure the MAC Addresses via the MAC Address tab on the computer’s Properties.



The MAC Address Tool supports retrieval of the MAC Addresses from computers running Microsoft Windows 2000 or later operating systems. It does not support computers running non-Windows operating systems.



MAC Addresses that are not assigned to a computer in Active Directory have the Default rule assigned to them.

You can access the MAC Address tool using one of the following methods:

- Select an item in the left-hand Tree of the main window and use the right-click menu to start the MAC Address Tool.
- From the main menu select *Action > MAC Address Tool*.
- Select one or more computers in the right-hand view and use the right-click menu to start the MAC Address Tool
- Display a Computer's Properties, select the *Mac Address* tab and click *Live MAC Addresses*.

The MAC Tool can be launched after selecting an Organizational Unit or a container, such as the "Computers" container — this will automatically select all the computers contained within the Organizational Unit or container. If the top level domain object is selected then all of the computers in the domain are automatically selected.

When the MAC Address Tool starts it constructs a table of all the Computers to be processed, ordered alphabetically by Name. However, as the MAC Address Tool interrogates information on the actual computer it can only determine the MAC Address if the computer is accessible.

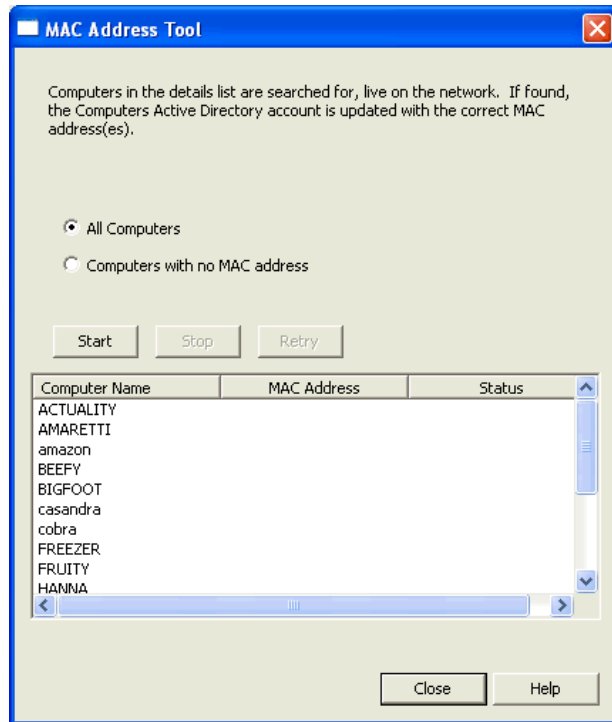
The table includes the columns; *Name*, *MAC Address* and *Status*. *Name* is the unique name of the Computer. *MAC Address* is the list of MAC Addresses for that Computer. *Status* is one of *Waiting*, *Successful*, *Failed*, *Not found* or *Not supported*.

If you wish to use the MAC Address Tool, the following conditions must be met:

- you must have sufficient privileges, for example be a member of the domain admins group
- the computer must be on the network
- the computer's firewall must allow access

- the WMI service must be enabled.

Figure 32 MAC Address Tool



The buttons on the MAC Address Tool main menu are as follows:

All Computers — select to update all computers. This is the default.

Computers with no Mac Address — select to update computers with no MAC Address

Start — select to update the Computers MAC Address.

Stop — select to stop the update process.

Progress bar — shows the the number of completed updates.

Retry — visible if there were problems during the process of updating the Computer accounts.

To add or update a computer account with MAC Address information:

- 1 Select either *All Computers* (default) or *Computers with no MAC Address* to determine the scope of the update.
- 2 Select *Start* to update the table with Computer accounts that have been processed, showing the appropriate Status and Progress bar.

Once all Computers have been processed the progress bar indicates this and the *Stop* button is disabled.

- 3 If any *Failed* or *Not found* status conditions occurred a *Retry* button is visible — click *Retry* to process the Computers that have those status conditions.

For more information on configuring use of the MAC Address Tool, refer to [Appendix D](#).

Using The Operator User Interface

Network Operators use the standard Active Directory Users and Computers interface, accessed from *Programs>Administrative Tools>Active Directory Users and Computers*. 3Com Network Access Manager adds a new tab, named *Network Access*, to the *Properties* pages for Users, Groups and Computers. The *Network Access* tab shows the network operator each rule that they can apply, if the network operator does not have permission to apply a rule then it is not displayed.

Operator Tasks

Providing a network operator has been granted appropriate permissions by the network administrator setting up 3Com Network Access Manager, a network operator can specify:

- if a user is allowed access to the network,
- if a group is allowed access to the network,
- if a computer (defined by its MAC address) is allowed access to the network,
- if a user and/or group and/or computer are allowed access, which VLAN should they connect to, and what Policy should they have,
- if a computer should be isolated from the main network,
- if a user should be isolated from the main network,
- if a group should be isolated from the main network,
- the EFW profile for each user logging into a PC with an EFW installed.

Displaying And Changing Rules Associated With A User

To display and change the rules associated with a user, follow these steps:

- 1 Click on Users in the Tree pane. The Details pane on the right will list the users that the Network Operator can manage.
- 2 Select a user to view and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Network Access* tab, a list of rules associated with the user will be displayed in the window, see [Figure 33](#). The tick box indicates how the rule is to be applied to the user, see [Table 11](#).

Figure 33 Changing Rules Associated With A User

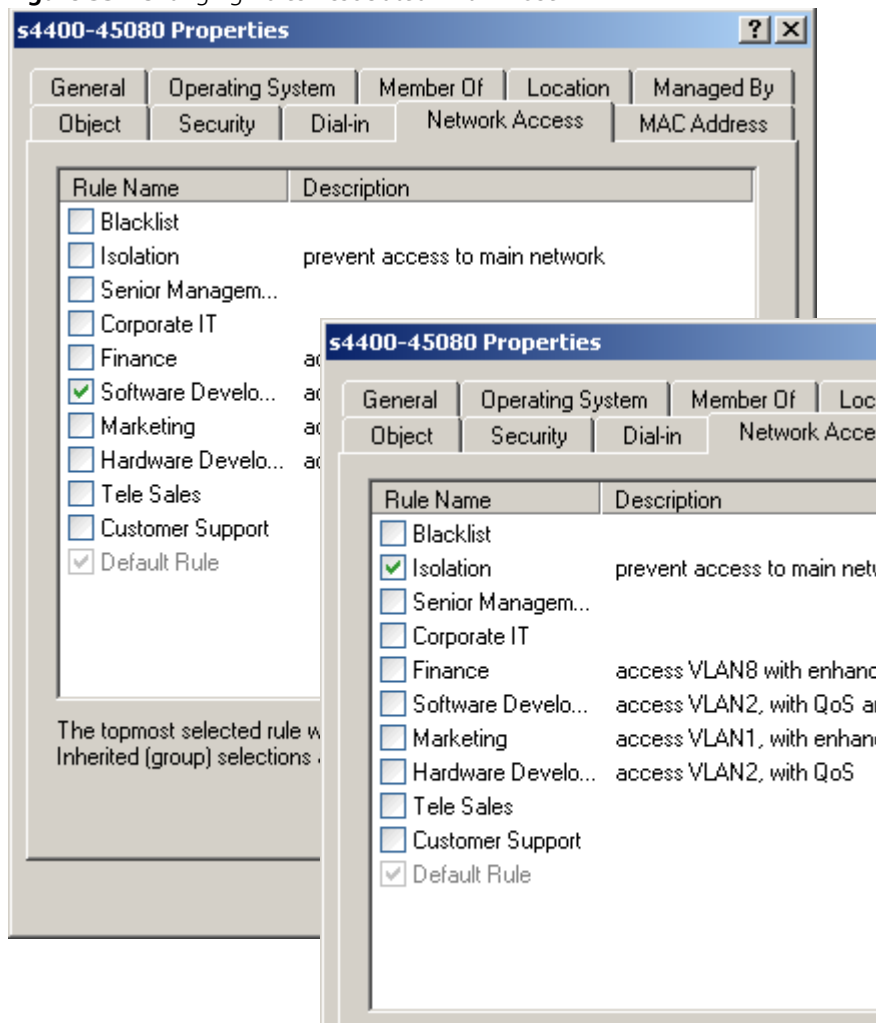


Table 11 Rules Tick Box For A User

Tick Box Setting	Meaning
Black, not ticked	The rule does not apply to this user
Black, ticked	The rule is applied to this user
Grey, ticked	The rule is applied to this user indirectly through the user's membership of one or more groups that have the rule specifically applied

- 4 Change the rules applied to a user by either ticking or removing the tick from rules that are black. To change a rule that is applied indirectly through a group, see [“Displaying And Changing Rules Associated With A Group”](#).
- 5 Click *OK*

This completes displaying and changing the rules associated with a user.

Displaying And Changing Rules Associated With A Group

To display and change the rules associated with a group, follow these steps:

- 1 Click on Groups in the Tree pane. The Details pane on the right will list all of the groups that the Network Operator can manage.



In Microsoft Active Directory Users and Computers tool (Operator UI) the groups are included in the "Users" container (or in the Organizational Units if configured).

- 2 Select a group to view and right-click. Select *Properties*.

The Properties dialog window will appear.

- 3 Select the *Network Access* tab, a list of rules associated with the group will be displayed in the window similar to [Figure 33](#). The tick box indicates how the rule is to be applied to the group, see [Table 12](#).

Table 12 Rules Tick Box for A Group

Tick Box Setting	Meaning
Black, not ticked	The rule does not apply to this group
Black, ticked	The rule is applied to this group
Grey, ticked	The rule is applied to this group indirectly through the group's membership of one or more groups that have the rule specifically applied

- 4 Change the rules applied to a group by either ticking or removing the tick from rules that are black.



To change the rules applied indirectly through being a member of another group, select the other group from the Detail pane and apply steps 1 to 4 above on the other group.

- 5 Click *OK*

This completes displaying and changing the rules associated with a group.

Displaying And Changing The Rule Associated With A Computer

To display and change the rules associated with a computer, follow these steps:

- 1 Click on Computers in the Tree pane. The Details pane on the right will list all of the computers that the Network Operator can manage.
- 2 Select a computer to view and right-click. Select *Properties*.
The Properties dialog window will appear.
- 3 Select the *Network Access* tab, a list of rules associated with the computer will be displayed in the window, see [Figure 34](#). The tick box indicates how the rule is to be applied to the group, see [Table 13](#).

Figure 34 Network Access Tab

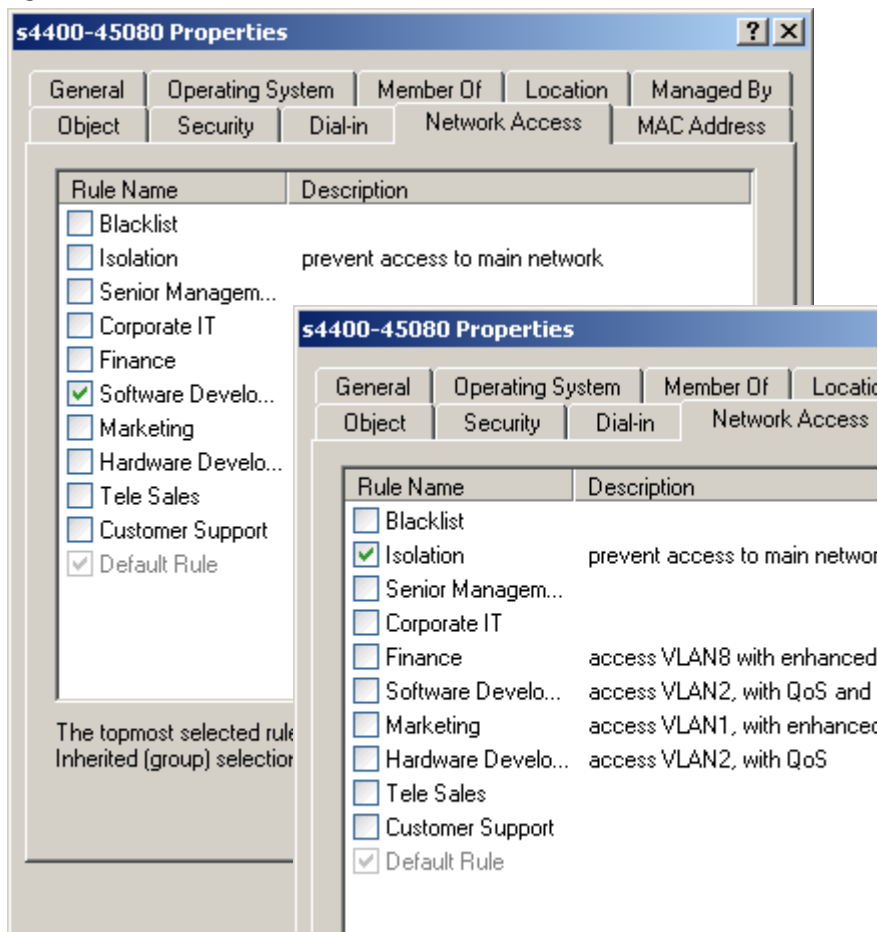


Table 13 Rules Tick Box for A Computer

Tick Box Setting	Meaning
Black, not ticked	The rule does not apply to this computer
Black, ticked	The rule is applied to this computer
Grey, ticked	The rule is applied to this computer indirectly through the computer's membership of one or more groups that have the rule specifically applied

- 4 You can change which of these rules are applied to a computer by either ticking or removing the tick from rules that are black. To change a rule that is applied indirectly through a group, see [“Displaying And Changing Rules Associated With A Group”](#).
- 5 Click *OK*

This completes displaying and changing the rules associated with a computer.

Using the Find Feature

3Com Network Access Manager has a Find feature which can be accessed via the Find button located on the toolbar as shown in [Figure 19](#). It is also available from the *Action > Find* menu and the right-click *Find* menu item when a suitable object is selected in the tree or the results list.

The Find feature provides the capability to find 3Com Network Access Manager associated attributes; NAM Rules, NAM VLANs, NAM Policies and EFW Policies, and Computers by MAC Address.

The *Find* dialog is the same as that available from the Microsoft Active Directory Users and Computers tool. It can also be used to find the standard directory objects (users, computers, groups etc).

This section details some examples of how you can use the Find feature to find objects in the directory.



If the Entire Directory entry is selected in the search scope when searching for 3Com Network Access Manager objects then no results will be found. The search scope must be set to a specific domain or a container in a domain as the 3Com Network Access Manager objects are local to the domain.



When entering a MAC address it must conform with the format *XX-XX-XX-XX-XX-XX* where *X* is hexadecimal number (0-9,A-F). eg "00-09-6B-52-7D-AD". The search will fail if a lower case character is used. Alternatively a partial MAC address may be entered when searching for "Start with" or "Ends with" conditions or a wildcard character '*' can be used (eg "00-09-6B-*").



When searching for rules based upon the rule action, enter "1" in the value field when searching for rules that allow access, and "2" for the rules which deny access.

Find Computer by MAC Address

This example details how to find a computer account in Active Directory based upon a previously configured MAC address.

This example assumes the following have already been set up:

- 3Com Network Access Manager "Active Directory Server" component is installed on a domain controller.
- 3Com Network Access Manager Administration or Operator UI is installed on local computer which is a member of the AD domain.
- MAC addresses are assigned to computer accounts in Active Directory using the 3Com MAC Address attribute.

Network Administrator Tasks

- 1 Start the 3Com Network Access Manager Administration tool or Operator tool (Microsoft Active Directory Users and Computers (ADUC) with 3Com Network Access Manager extension snap-in).
- 2 Select the *Find* action (from the Action menu or context menu).
- 3 Select *Computers* in the *Find* drop-down list.
- 4 Restrict the search scope if desired; e.g. Directory tree nodes.
- 5 Select the *MAC Address (3Com Network Access Manager)* field under the *Advanced* tab and select the search condition and enter the search data. Add further fields if required.
- 6 Click *Find Now*. You can change the displayed columns if desired.

What Happens

Computers matching the MAC address are displayed in the results list. If no computers are found the message *No items match the current search* will be displayed in the results list.

Find a NAM Rule/VLAN/NAM Policy

This example details how to find a NAM Rule, NAM VLAN, NAM Policy or EFW Policy in Active Directory.

This example assumes the following have already been set up:

- 3Com Network Access Manager "Active Directory Server" component installed on a domain controller.
- 3Com Network Access Manager Administration or Operator UI installed on local computer which is a member of the AD domain.
- NAM Rules/NAM VLANs/NAM Policies/EFW Policies exist in Active Directory.

Network Administrator Tasks

- 1 Start the 3Com Network Access Manager Administration tool or Operator tool (Microsoft Active Directory Users and Computers (ADUC) with 3Com Network Access Manager extension snap-in).
- 2 Select the *Find* action (from the Action menu or context menu).
- 3 Select *Custom Search* in the *Find* drop-down list.
- 4 Restrict the search scope if desired; e.g. Directory tree nodes.
- 5 Select the specific search field(s) under the *Custom Search* tab and select the search condition and enter the data. For example, Field: *NAM Rule->Priority*, Condition: *Less than or equal to*, Value: *100*.
- 6 Click *Find Now*. You can change the displayed columns if desired.

What Happens

Directory objects matching the search condition are displayed in the results list. If no objects are found the message *No items match the current search* will be displayed in the results list.

Using The Online Help

Press the F1 key to display the 3Com Network Access Manager online help from the network administrator interface.

4

USING 3COM NETWORK ACCESS MANAGER WITHIN A NETWORK

This chapter provides case studies on how 3Com Network Access Manager can be setup to provide different levels of security on a network.

Case Study Assumptions

All of the case studies described in this chapter assume the following:

- Microsoft's Active Directory working with Microsoft's Internet Authentication Service (IAS) and 3Com Network Access Manager to provide RADIUS authentication of users and computers in the network.
- All authorized users are listed in Active Directory.
- All users and computers are allocated into their relevant organizational group, for example Marketing, or Students.
- The network operator has access to a PC with Windows 2000 Professional or Windows XP Professional installed, and the PC has Active Directory Users and Computers installed (from the Windows Server Admin Pack).

Case Study 1 — Controlling User Access To The Network

This case study describes the tasks that need to be performed in order to control user access to the network using IEEE 802.1X. The MAC Address of the PC is not assigned to any Rule by the network administrator which means that it is assigned the Default Rule during a RADIUS Request. The users Rule has higher priority than the Default Rule providing correct network access settings.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure edge port security is set to IEEE 802.1X on edge ports in the domain.



Edge ports are called 'access ports' on the Switch 5500.

Using 3Com Network Access Manager:

- 2 Select the Default Rule and set the *Network Access* to Deny, see ["Changing NAM Rule Properties"](#) in [Chapter 3](#).
- 3 Create an Authorized Users rule which will allow network access, see ["Creating A New NAM Rule"](#) in [Chapter 3](#).
 - a Set security permissions for the rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for the rule: select the rule priority, and set Network Access to *Allow*, if appropriate select the VLAN, Policy and EFW policy for the rule.
- 4 Associate the Authorized Users rule with users and groups already listed in Active Directory
- 5 Ensure the network operators or those individuals responsible for applying the Authorized Users rule have the Network Operator component of 3Com Network Access Manager installed on their PC.

**Network Operator
Tasks**

The following provides an overview of the tasks for a network operator responsible for controlling user access to the network domain.

On being informed that a specific user or group needs to be granted access to the network, use the Active Directory Users and Computers interface to perform the following:

- 1 Either:
click on Users in the Tree pane, or
if Organizational Units have been created, click on the organizational units subfolders until you reach the desired unit holding the user or group.
- 2 Highlight the specific user or group in the Details pane, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed
- 4 Tick the Authorized Users rule to apply it to the user.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

On being informed that a specific user or group needs to be denied access to the network, use the Active Directory Users and Computers interface to perform the following:

- 1 Either:
click on Users in the Tree pane, or
if Organizational Units have been created, click on the organizational units subfolders until you reach the desired unit holding the user or group.
- 2 Highlight the specific user or group in the Details pane, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed
- 4 Untick the Authorized Users rule.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

**What Happens When
A User Logs In**

The following takes place when a user connects and logs into the network domain.

- 1** The user's PC connects to the network and the user logs in with a username.
- 2** The IEEE 802.1X client on the PC sends the user's ID and credentials to the switch. At this stage, the port on the switch is blocked and the PC cannot connect to the rest of the network.
- 3** The switch sends the user's details via RADIUS to IAS.
 - a** If the user is listed in Active Directory, and the Authorized Users rule has been applied to the user (or a group that the user is a member of), IAS replies Accept and the switch enables the port.
 - b** If the user is listed in Active Directory, but the Authorized Users rule has not been applied to the user (or a group that the user is a member of), then the Default Rule will be applied, IAS replies Reject and the switch disables the port.
 - c** If the user is not listed in Active Directory, IAS replies Reject and the switch disables the port.

Case Study 2 — Restricting Network Access To Known Computers

This case study describes the tasks that need to be performed in order to restrict network access to known computers, using MAC-address based authentication.

This is an example of “block-by-default” or a white-list mode, where the device needs to be listed in the Active Directory before it is allowed access to the network. This mode relies solely on authenticating the MAC address of each attached device. Non-user devices (for example printers and servers) can still connect to the network, while the network blocks rogue devices, such as unknown wireless access devices. This mode does not require user authentication and hence does not provide any network protection against unauthorized user login.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure edge port security is set to MAC-address based authentication (or RADA) on edge ports in the domain.



3Com Network Access Manager requires that a switch performing RADA authentication must supply a fixed user name (as opposed to the MAC address as the user name).



Edge ports are called ‘access ports’ on the Switch 5500.

Using 3Com Network Access Manager:

- 2 Select the Default Rule and set the *Network Access* to Deny, see [“Changing NAM Rule Properties”](#) in [Chapter 3](#).
- 3 Create an Authorized Computers rule which will allow network access, see [“Creating A New NAM Rule”](#) in [Chapter 3](#).
 - a Set security permissions for the rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for the rule: select the rule priority, and set Network Access to *Allow*, if appropriate select the VLAN, NAM Policy and EFW policy for the rule.

- 4 Enter the MAC addresses for all devices in the domain. For information on entering MAC addresses, see [“Using the MAC Address Tool”](#) on [page 75](#) to easily update computers with their MAC addresses.
- 5 Create a new group which will hold the computers that are allowed access, see [“Creating A New Group”](#) in [Chapter 3](#).
- 6 Associate the Authorized Computers rule created in [step 3](#) with the group created in [step 5](#).
 - a Highlight the specific group in the Details pane, and right-click. Select *Properties*.
 - b Select the *Network Access* tab from the Properties dialog window.
 - c Tick the Authorized Computers rule. Click *OK*.
- 7 Associate the computers that are permitted network access with the group created in [step 5](#).
- 8 If required, create an Unauthorized Computers rule to deny network access, which a network operator can apply to specific computers when necessary. Ensure the network operator responsible for applying this rule has the Network Operator component of 3Com Network Access Manager installed on their PC.



An Unauthorized Computers rule must have a higher priority than the Authorized Computers rule in order to override the Authorized Computers rule.

- 9 Maintain the list of computers in Active Directory, ensuring all known computers are listed in Active Directory with their MAC addresses specified.



You can easily maintain the list of computers in Active Directory by periodically using the MAC Address Tool.

Network Operator Tasks

The network operator cannot enter the MAC address for a computer. However, once the computer's MAC address has been entered, the operator can apply any rules to the computer or change the rules applied to the computer if they have been given write permission for the rule.

On being informed that a specific PC can be granted network access, use the Active Directory Users and Computers interface to perform the following:

- 1 Either:
click on Computers in the Tree pane, or
if Organizational Units have been created, click on the organizational units subfolders until you reach the desired unit holding the PC.
- 2 Highlight the specific PC, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed
- 4 Tick the Authorized Computers rule to apply it to the PC.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

On being informed that a specific PC needs to be denied access to the network, use the Active Directory Users and Computers interface to perform the following:

- 1 Either:
click on Computers in the Tree pane, or
if Organizational Units have been created, click on the organizational units subfolders until you reach the desired unit holding the PC.
- 2 Highlight the specific PC in the Details pane, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed
- 4 Tick the Unauthorized Computers rule.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

What Happens The following takes place when a device connects to the network.

- 1 The PC connects to the network
- 2 The switch sends the MAC address of the PC via RADIUS to IAS
 - a If the PC is listed in Active Directory, and the Authorized Computers rule has been applied to the PC, IAS replies Accept and the switch enables the port.

- b If the PC is listed in Active Directory, but either the Default Rule or the Unauthorized Computers rule is applied to the PC, IAS replies Reject and the switch disables the port.
- c If the PC is not listed in Active Directory the Default Rule is applied, IAS replies Reject and the switch disables the port.

Case Study 3 — Blocking A Specific PC From The Network

This case study describes the tasks that need to be performed in order to block a specific PC from the network, using MAC-address based authentication. It is an example of a Blacklist mode in which all devices are allowed network access unless the device is on the blacklist. This is useful in very large networks where you just want to block access to specific PCs.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure edge port security is set to MAC-address based authentication (or RADA) on edge ports in the domain.



Edge ports are called 'access ports' on the Switch 5500.

Using 3Com Network Access Manager:

- 2 Select the Default Rule and set the *Network Access* to Allow, see ["Changing NAM Rule Properties"](#) in [Chapter 3](#).
- 3 Create a Blacklist rule which can be used to deny network access to specific computers.
 - a Set security permissions for the Blacklist rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for the rule:
 - select the rule priority, a Blacklist rule should be assigned a high priority to ensure it takes precedence over other rules
 - set *Network Access* for the Blacklist rule to *Deny* to block network access,

- 4 Ensure the network operators or those individuals responsible for applying the Blacklist rule have the Network Operator component of 3Com Network Access Manager installed on their PC.

When a PC needs to be blacklisted:

- 1 Enter the MAC address for the computer that needs to be blacklisted. For information on entering MAC addresses, see [“Entering MAC Addresses For A Computer”](#) in [Chapter 3](#).
- 2 Associate the Blacklist rule with the computer, see [“Associating Rules With A Computer”](#) in [Chapter 3](#).

**Network Operator
Tasks**

The network operator cannot enter the MAC address for a computer. However, the operator can apply the Blacklist rule to a specific computer once the computer’s MAC address has been entered. The operator can also remove the computer from the blacklist if circumstances require it.

On being informed that a specific PC needs to be denied access to the network, use the Active Directory Users and Computers interface to perform the following:

- 1 Either:
click on Computers in the Tree pane, or
if Organizational Units have been created, click on the organizational units subfolders until you reach the desired unit holding the computer.
- 2 Highlight the specific device in the Details pane, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed.
- 4 Tick the Blacklist rule to apply it to the PC.
- 5 Click *OK* and exit the Active Directory Users and Computers interface

On being informed that a specific PC can be removed from the Blacklist, use the Active Directory Users and Computers interface to perform the following:

- 1 Either:
click on Computers in the Tree pane, or

if Organizational Units have been created, click on the organizational units subfolders until you reach the desired unit holding the computer.

- 2 Highlight the specific device, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed.
- 4 Untick the Blacklist rule applied to the PC.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

What Happens The following takes place when a PC connects to the network.

- 1 The PC connects to the network.
- 2 The switch sends the MAC address of the PC via RADIUS to IAS,
 - a If the PC is on the Blacklist, IAS replies Reject and the switch disables the port,
 - b If the PC is not on the Blacklist and the Default Rule was set to Allow network access, IAS replies Accept and the switch enables the port.

Case Study 4 — Hot Desking

Combining Auto-VLAN/QoS with IEEE 802.1X enables users to login anywhere on the network, and always have access to their network (for example, the Engineering VLAN/QoS, or Marketing VLAN/QoS). This makes hot-desking viable, as users can change desks and still gain access to their network.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure edge port security is set to IEEE 802.1X and Auto-VLAN/QoS is enabled, on edge ports in the domain.



Edge ports are called 'access ports' on the Switch 5500.

Using 3Com Network Access Manager:

- 2 Decide how you want to apply the Default Rule. You can use the Default Rule to either:
deny access to unspecified users, or

allow access to users who are not hot desking and who do not require VLAN and QoS assignments.

- 3 Select the Default Rule and set the *Network Access* to either Deny or Allow, according to your decision in [step 2](#)
- 4 Create VLANs and NAM Policies. Use the same VLAN IDs and NAM Policy IDs as set up in the network access device (switch or wireless access point), otherwise the network access device may not accept the RADIUS response.
- 5 Create rules to support the assignment of a VLAN and NAM Policy to those users and groups permitted to log in. For example, in a school the following rules could be created: Staff, Student, SysAdmin.
 - a Set security permissions for each rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for each rule:
 - select the rule priority,
 - set *Network Access* for the rule, to *Allow* to permit access to the network,
 - select the VLAN ID, NAM Policy and EFW policy (if appropriate) for each rule.
- 6 Associate the new rules with users and groups already listed in Active Directory.
- 7 Ensure the network operators or those individuals responsible for applying the rules have the Network Operator component of 3Com Network Access Manager installed on their PC.

Network Operator Tasks

The following provides an overview of the tasks for a network operator responsible for controlling user access to the network domain.

On being informed that a user or group needs to be granted access to a particular VLAN on the network, use the Active Directory Users and Computers interface to perform the following:

- 1 Either:
 - click on Users in the Tree pane, or

if Organizational Units have been created, click on the organizational units subfolders until you reach the desired unit holding the user or group.

- 2 Highlight the user or group, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed.
- 4 Identify the rule that will enable the user to access the particular VLAN, and tick the rule to apply it to the user.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

What Happens When A User Logs In

The following takes place when a user connects and logs into the network domain.

- 1 The user's PC connects to the network and the user logs in with a username.
- 2 The IEEE 802.1X client on the PC sends the user's ID and credentials to the switch. At this stage, the port on the switch is blocked and the PC cannot connect to the rest of the network.
- 3 The switch sends the user's details via RADIUS to IAS.
 - a If the user is listed in Active Directory, and the new rule allowing access and assigning VLAN and Policy has been applied to the user (or a group that the user is a member of), IAS replies Accept with the VLAN ID and NAM Policy for that user. The switch enables the port and configures the VLAN and NAM Policy of the port as specified.
 - b If the user is listed in Active Directory, but the new rule was not applied, then if the Default Rule was set to Allow, IAS replies Accept and the switch enables the port, otherwise if the Default Rule was set to Deny, IAS replies Reject and the switch disables the port.
 - c If the user is not listed in Active Directory, IAS replies Reject and the switch disables the port.

Case Study 5 — Removing Infected Devices From The Network

Combining Auto-VLAN/QoS with MAC-address based authentication enables infected PCs to be moved to a separate network, until the network administrator has removed any viruses or worms.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure edge port security is set to MAC-address based authentication and Auto-VLAN/QoS is enabled on edge ports in the domain.



Edge ports are called 'access ports' on the Switch 5500.

Using 3Com Network Access Manager:

- 2 Select the Default Rule and set the *Network Access* to Allow, see [“Changing NAM Rule Properties”](#) in [Chapter 3](#).
- 3 Create VLANs and Policies. Use the same VLAN IDs and NAM Policy IDs as set up in the network access device (switch or wireless access point), otherwise the network access device may not accept the RADIUS response.
- 4 Decide which VLAN and Policy will be used for Isolation.
- 5 Create an Isolation rule.
 - a Set security permissions for the Isolation rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for the Isolation rule:
 - select the rule priority, an Isolation rule should have a high priority to ensure it takes precedence over other rules,
 - set *Network Access* to *Allow*,
 - select the Isolation VLAN and Policy.
- 6 Ensure the network operators or those individuals responsible for applying the rule have the Network Operator component of 3Com Network Access Manager installed on their PC.

When a PC needs to be isolated for the first time:

- 1 Enter the MAC address for the computer that needs to be removed from the network. For information on entering MAC addresses, see [“Entering MAC Addresses For A Computer”](#) in [Chapter 3](#).
- 2 Associate the Isolation rule with the computer, see [“Associating Rules With A Computer”](#) in [Chapter 3](#).

Network Operator Tasks

The network operator cannot enter the MAC address for a computer. However, once the computer’s MAC address has been entered, the operator can apply the Isolation rule to the computer if they have been given write permission for the rule. The operator can also reconnect the computer to the main network once the network administrator has removed any viruses or worms.

On being informed that a specific PC needs to be isolated again, use the Active Directory Users and Computers interface to perform the following:

- 1 Click on Computers in the Tree pane,
- 2 Highlight the specific PC, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed.
- 4 Tick the Isolation rule to apply it to the PC.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

On being informed that a specific PC can be returned to the normal network, use the Active Directory Users and Computers interface to perform the following:

- 1 Click on Computers in the Tree pane,
- 2 Highlight the specific PC, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed
- 4 Untick the Isolation rule applied to the PC.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

What Happens The following takes place when a PC connects to the network.

- 1 The switch sends the MAC Address of the PC via RADIUS to IAS.
 - a If the PC is on the Isolation list, IAS replies Accept with the VLAN ID and NAM Policy ID of the Isolation Network. The switch enables the port and configures the VLAN of the port to be in the Isolation Network.
 - b If the PC is unknown the Default Rule is applied, IAS replies Accept and the switch enables the port.

Case Study 6 — Combining Hot Desking With Host Filtering

This case study describes the tasks that need to be performed in order to set up hot desking with the ability to filter out specific hosts. This configuration allows infected PCs to be isolated regardless of where the user has connected to the network in a hot desking office environment. The method combines MAC-address based authentication with IEEE 802.1X authentication and Auto-VLAN.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure edge port security is set to MAC-address based authentication (or RADA) and IEEE 802.1X, and Auto-VLAN/QoS is enabled (for example RADA-Else-Network Login).



Edge ports are called 'access ports' on the Switch 5500.

Using 3Com Network Access Manager:

- 2 Create VLANs and NAM Policy. Use the same VLAN IDs and NAM Policy IDs as set up in the network access device (switch or wireless access point), otherwise the network access device may not accept the RADIUS response.
- 3 Decide which VLAN and Policy will be used for Isolation.
- 4 Create an Isolation rule.
 - a Set security permissions for the Isolation rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for the Isolation rule:

- select the rule priority, an Isolation rule should have a high priority to ensure it takes precedence over other rules,
 - set *Network Access* to *Allow*,
 - select the Isolation VLAN and Policy.
- 5 Ensure the network operators or those individuals responsible for applying the rules have the Network Operator component of 3Com Network Access Manager installed on their PC.

When a PC needs to be isolated for the first time:

- 1 Enter the MAC address for the computer that needs to be removed from the network. For information on entering MAC addresses, see [“Entering MAC Addresses For A Computer”](#) in [Chapter 3](#).
- 2 Associate the Isolation rule with the computer, see [“Associating Rules With A Computer”](#) in [Chapter 3](#).

**Network Operator
Tasks**

The network operator cannot enter the MAC address for a computer. However, once the computer’s MAC address has been entered, the operator can apply the Isolation rule to the computer if they have been given write permission for the rule. The operator can also reconnect the computer to the main network once the network administrator has removed any viruses or worms.

On being informed that a specific PC needs to be isolated again, use the Active Directory Users and Computers interface to perform the following:

- 1 Click on Computers in the Tree pane,
- 2 Highlight the specific PC, and right-click. Select *Properties*.
- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed.
- 4 Tick the Isolation rule to apply it to the PC.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

On being informed that a specific PC can be returned to the normal network, use the Active Directory Users and Computers interface to perform the following:

- 1 Click on Computers in the Tree pane,
- 2 Highlight the specific PC, and right-click. Select *Properties*.

- 3 Select the *Network Access* tab from the Properties dialog window.
A list of rules that the operator has permission to apply will be displayed.
- 4 Untick the Isolation rule applied to the PC.
- 5 Click *OK* and exit the Active Directory Users and Computers interface.

What Happens When A User Logs In

The following takes place when a user connects and logs into the network domain.

- 1 The switch sends both the PC MAC Address and user details via RADIUS to IAS.
- 2 If the Isolation rule has been applied to the PC, IAS replies Accept with the VLAN and NAM Policy ID of the Isolation Network. The switch enables the port and configures the VLAN of the port as specified.
- 3 Otherwise, if the user is listed, IAS replies Accept with the VLAN and NAM Policy ID for that user (determined by the current rule applied to the user, or if the user is assigned to a group then the current rule applied to the group). The switch enables the port and configures the VLAN/QoS of the port as specified.
- 4 Else, if the user is not listed, IAS replies Reject and the switch disables the port.

Case Study 7 — Controlling Guest Access to the Network

This section describes the tasks that need to be performed in order to control guest access to the network using port security mode 'RADA or Network Login'. The fixed RADA username/password pair configured in the switch is used to define the Guest User access rights and Network Login (802.1X) credentials are used to define the known Users access rights.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure edge port security is set to 'RADA or Network Login' on edge ports in areas where Guest access is to be authorized. Configuring the RADA fixed username password with a suitable user account for Guest access. For example, RADAGuest.
- 2 In Active Directory Users' and Computers' create RADA Guest user accounts. For example, RADAGuest from step 1.

Using 3Com Network Access Manager:

- 3 Select the Default Rule and set the Network Access to Deny, see [“Changing NAM Rule Properties”](#) in [Chapter 3](#).
- 4 Create an Authorized Guest Users rule which will allow network access, see [“Creating A New NAM Rule”](#) in [Chapter 3](#).
 - a Set security permissions for the rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for the rule: select the rule priority, and set Network Access to Allow, if appropriate select the VLAN, Policy and EFW policy for the rule.
- 5 Associate the Authorized Guest Users rule with RADA users and groups already listed in Active Directory. For example, RADAGuest from steps 1 and 2.

What Happens When A Guest User Logs In

The following takes place when a user connects and logs into the network domain.

- 1 The user's PC connects to the network and the user logs in with a username.
- 2 The RADA component of the switch obtains the MAC Address of the PC and uses the RADA fixed username to send a RADIUS access request to IAS. At this stage, the port on the switch is blocked and the PC cannot connect to the rest of the network.
- 3 If there is one, the IEEE 802.1X client on the PC sends the user's ID and credentials to the switch. The switch sends the user's details via RADIUS to IAS.
- 4 The RADA fixed username is listed in Active Directory and is assigned to a 3Com Network Access Manager Guest Rule. The MAC Address of the PC is not known in Active Directory and is given the default rule. The Guest Rule is applied, IAS replies *Accept* and the switch enables the port.
- 5 The IEEE 802.1X user is not listed in Active directory and fails authentication. IAS replies with *reject*. Because an *accept* from RADA authentication was received the switch does not block the port, allowing the PC to use the network as a guest.

Case Study 8 — Configure Third-party Device Support with 3Com Network Access Manager



This section describes how to configure 3Com Network Access Manager to supply VLAN/QoS assignments to devices which are not supported by 3Com Network Access Manager by default.

Many third party devices will work with 3Com Network Access Manager by using the Authorization Type = 2 (IETF 3580 Usage).



When creating a custom Authorization Type it is recommended that it is given an identifier value of 100 or above to avoid clashing with 3Com assigned authorization types.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure that the 3Com Network Access Manager Active Directory Server component is installed on a domain controller.
- 2 Ensure the IAS Servers are installed with the 3Com Network Access Manager Internet Authentication Service component on one or more Windows Servers which are members of the AD domain and configured with RADIUS client (switch) accounts.
- 3 Ensure NAM Rules/NAM VLANs/NAM Policies are configured in Active Directory and Users/Groups/Computers assigned to the Rules.
- 4 Ensure switch devices are configured to use IEEE 802.1X/RADA port security and RADIUS.

Using 3Com Network Access Manager:

- 5 Edit the IAS 3Com Network Access Manager plug-in configuration file:
 - a add a user-defined authorization type which specifies the RADIUS attributes (including any standard VSAs) that are to be returned for the VLAN and QoS assignment actions.
 - b Save the file changes and restart the IAS service.
- 6 Use the IAS MMC to create one or more IAS Access Policies that match the access requests from the switch devices. Include the "Authorization Type" VSA or enter the IP Address in the NAS Identification file in the RADIUS attributes to be returned in the access response (this should contain the value of the user defined authorization type defined above).



3Com recommends that the Access Policies being configured to supply the 3Com Authorization Type VSA contain the identifier matching the

custom authorization type defined in the plug-in configuration file when access requests are received from the third-party device. Adding the device IP address to the NAS-Identification file should only be done if this is not possible.

What Happens

Edge devices that are attached to the third-party switch and are successfully authenticated are assigned VLAN and NAM Policies based upon the user or computer account as specified in Active Directory using the RADIUS attributes specified in the user defined authorization type.

Case Study 9 — Configure Third-party Health checking system with 3Com Network Access Manager

This section explains how to configure the 3Com Network Access Manager to work with Third-party health checking systems, or other similar systems, which add extension plug-ins to the IAS Server that also supply VLAN and Policy assignments to the RADIUS clients.

The Microsoft IAS Server supports multiple extension plug-ins that are executed in turn when an access request is received. When using multiple extensions it is important to ensure that they are called in the correct order to avoid conflicts between the changes to the authorization response made by each of the extensions. When the 3Com Network Access Manager plug-in is operating with its default configuration it will replace any VLAN and Policy information in the authorization response with the settings derived from the selected NAM Rule.

This section describes how to modify the behavior of the 3Com Network Access Manager plug-in so that it will no longer replace the VLAN and Policy assignment made by another previously called extension plug-in. Hence, if the 3Com Network Access Manager plug-in is called after another extension which has already assigned the VLAN or Policy the 3Com Network Access Manager plug-in will not modify the authorization response. If the previously called extensions do not add a VLAN or Policy assignment the 3Com Network Access Manager plug-in will add the VLAN and Policy assignment derived from the NAM Rule.



Depending upon how the third-party IAS plug-in operates it may be possible to configure the IAS Server to call the 3Com Network Access Manager plug-in first in which case it will not be necessary to modify the 3Com Network Access Manager configuration.

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain on the network.

- 1 Ensure that the 3Com Network Access Manager "Active Directory Server" component is installed on a domain controller.
- 2 Ensure the IAS Servers are installed with the 3Com Network Access Manager "Internet Authentication Service" component on one or more Windows Servers which are members of the AD domain and configured with RADIUS client (switch) accounts.

Ensure that the IAS Server is configured to call the plug-ins in the required order. Please refer to the Microsoft IAS documentation on how to do this.

- 3 Ensure Rules, VLANs and Policies are configured in Active Directory and the Users, Groups and Computers are assigned to the Rules.
- 4 Ensure switch devices are configured to use IEEE 802.1X/RADA port security and RADIUS.

Using 3Com Network Access Manager:

- 5 Edit the IAS 3Com Network Access Manager plug-in configuration file:
 - a Add a pre-condition attribute checklist that specifies the RADIUS attributes (including any standard VSAs) that the access request must match, or must not match, in order for the access request to be processed by the plug-in.

For example, to stop the 3Com Network Access Manager plug-in processing requests that have been assigned a VLAN or policy add the following checklist:

```
check response
{
    no_match Tunnel-Private-Group-Id
    no_match Filter-Id
}
```

Refer to [“Customizing the Configuration Files”](#) on [page 121](#) for additional information relating to modifying this configuration file.

- b Save the file changes and restart the IAS service.
 - c Use the Microsoft Event Viewer to check the 3Com Network Access Manager event log to confirm that no errors occurred while parsing the configuration file.
- 6 Use the IAS MMC to create one or more IAS Access Policies that match the access requests from the switch devices and include the Authorization Type VSA with the appropriate authorization type for the devices.

What Happens If an access request is received from a device that fails to pass the health requirements then the health check plug-in assigns a VLAN or policy to isolate the device from the network. The 3Com Network Access Manager will not replace these assignments with the rule based assignments.

5

PROBLEM SOLVING

This chapter covers:

- checking the Windows Event Viewer for obvious problems,
- resolving problems related to setting up 3Com Network Access Manager.

Checking the Event Viewer

If you experience network access or RADIUS authentication problems on your network, first check the Windows Event Viewer to see whether the problem can be readily identified and corrected.

Follow these steps:

- 1 Select *Control Panel>Administrative Tools>Event Viewer*.
- 2 Select *System* from the Tree pane, and review the events in the log in the right hand pane, see [Figure 35](#). IAS in the Source column indicates an event was generated by IAS. Use the information in the log to determine the reason an IAS connection attempt was either rejected or discarded. Click on any event to display more information about the event.
- 3 Select *3Com Network Access Manager* from the Tree pane, see [Figure 36](#). Review the events in the 3Com Network Access Manager log to determine whether 3Com Network Access Manager has been set up correctly. Click on any event to display more information about that event, [Figure 37](#) shows computer 'S4400-45080' granted network access to VLAN 2 with Policy ID q2.

Figure 35 System Event Log

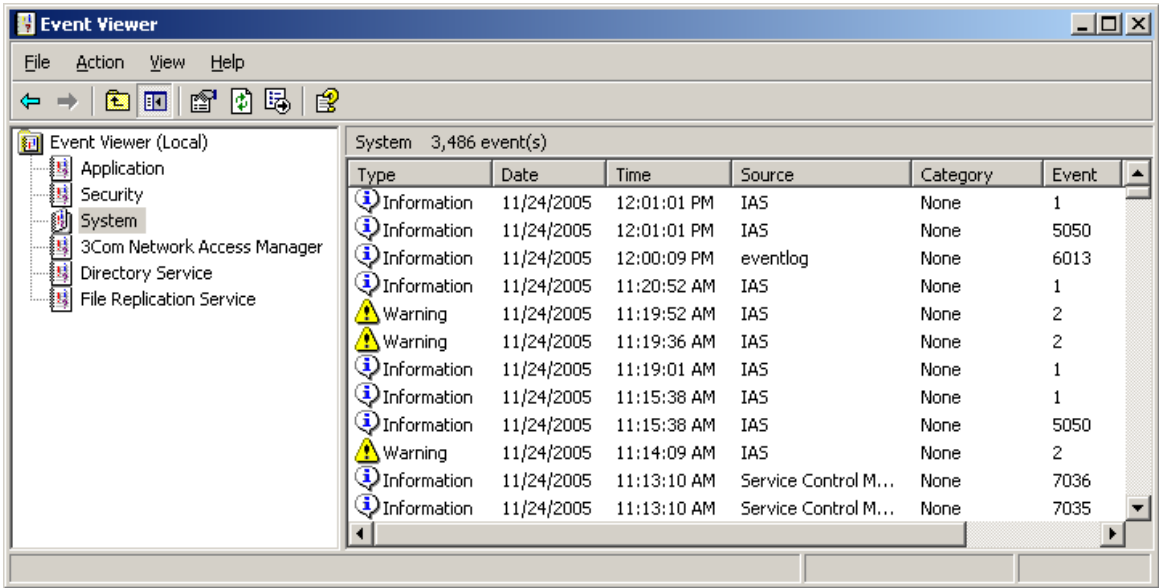


Figure 36 3Com Network Access Manager Authorization Log

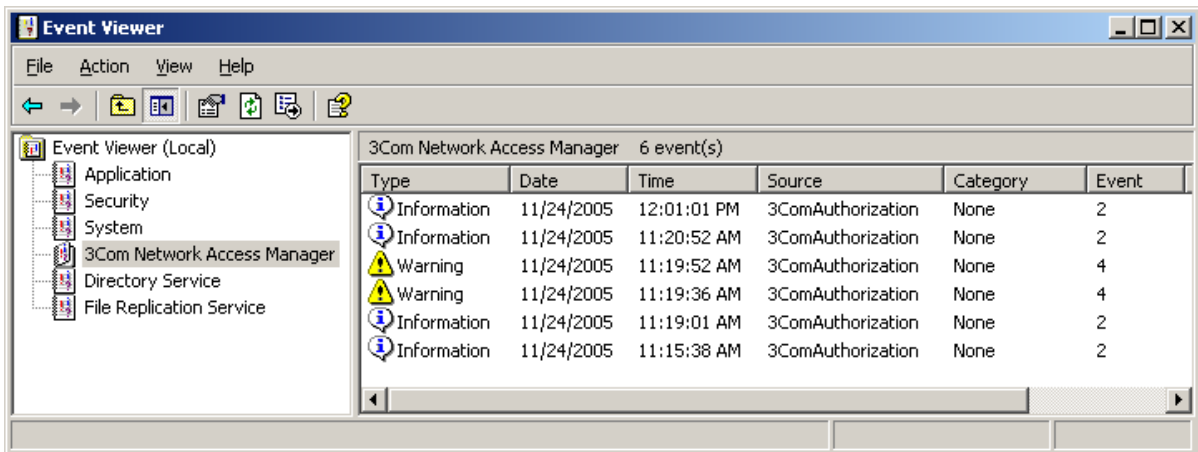
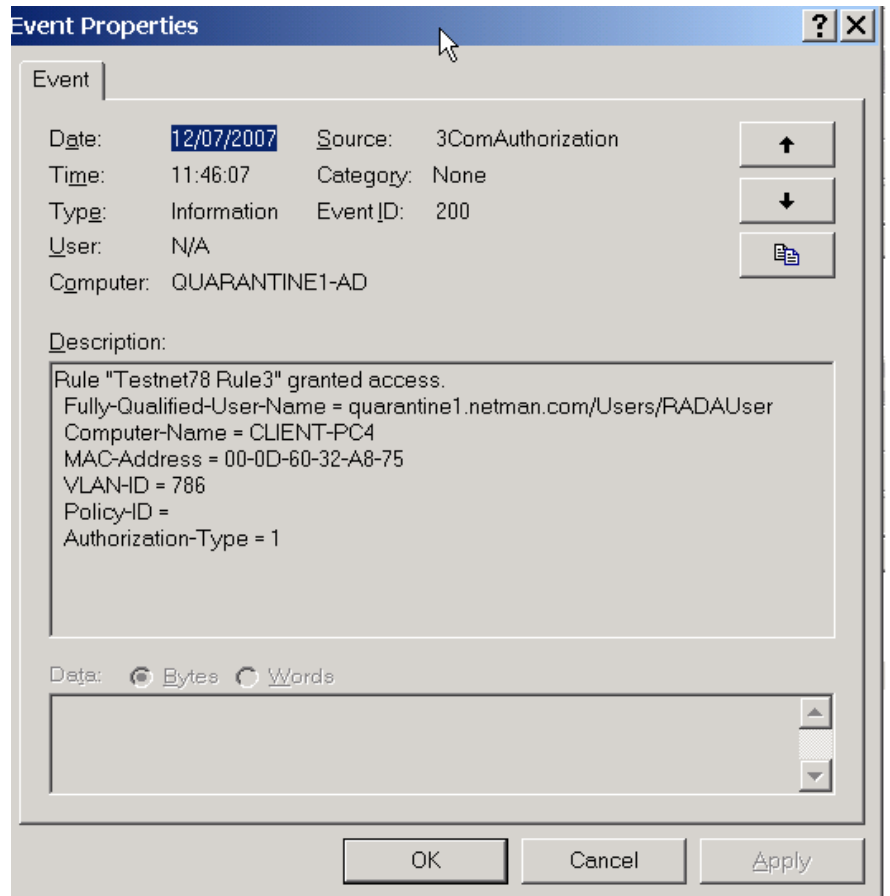


Figure 37 Event detail

Identifying Where The Problem Lies

3Com Network Access Manager is dependent on IAS. A problem with 3Com Network Access Manager may be caused by an underlying issue with IAS. If that is the case then it will be IAS that logs an event and not 3Com Network Access Manager. In these instances you should view the event detail in the system event log, determine the cause of the problem and then resolve the issue.

Problems Related to Setting Up

This section details possible problems that you might experience when setting up and using 3Com Network Access Manager. Each problem is described by a symptom, an explanation of the cause of the problem and a suggestion on what to do to remedy the problem.

The problems are listed in two tables: [Table 14](#) covers problems that you may experience when initially setting up 3Com Network Access Manager, [Table 15](#) lists possible problems related to network access.

Table 14 Problems That May Be Encountered When Setting Up

Symptom	Cause	Remedy
Cannot find <i>3Com Network Access Manager Admin</i> on the PC used by a Network Administrator.	The Administration User Interface component has not been installed on the Network Administrator's PC.	Check that the Network Administrator's PC meets the specifications in Table 5 and Table 6 , in Chapter 2 , install the Administration User Interface component on the PC.
3Com Network Access Manager does not allow you to create rules/ VLANs/Policies/ EFW Policies. When trying to create a rule/ VLAN/ Policy/ EFW Policy the following message is displayed: "Unable to create item. This may be because an item with this name already exists or because of security permission".	Either: You do not have Administrator privileges or are not using the 3Com Network Access Manager Admin tool. Or: The Active Directory component for 3Com Network Access Manager has not been installed on an Active Directory server in the network domain. Or: Changes to the Active Directory schema have not replicated to all Active Directory servers in the domain.	Use the <i>3Com Network Access Manager Admin</i> tool to access the Network Administrator User Interface. Ensure you have appropriate Administrator permissions. Ensure the Active Directory component is installed on one Active Directory server in the domain. If you have already installed the Active directory component on an Active Directory server in the domain, then you may need to wait for the schema changes to replicate to the other Active Directory servers in the domain.
The <i>Network Access</i> tab, accessible by right-clicking <i>Users</i> or <i>Groups</i> or <i>Computers</i> in the Tree pane and selecting <i>Properties</i> , does not display all rules created in 3Com Network Access Manager	You have not been granted read permission for the rules which are not displayed.	Ask the network administrator who created the rules in 3Com Network Access Manager to grant you read permission for the specific rules.

Table 14 Problems That May Be Encountered When Setting Up (continued)

Symptom	Cause	Remedy
<p>Clicking on <i>Rules</i> in the Tree pane displays an empty Display pane.</p> <p>Note: After correct installation the Default Rule will always be shown in the Display pane</p>	<p>Either:</p> <p>The Active Directory component for 3Com Network Access Manager has not been installed on an Active Directory server in the network domain.</p> <p>Or:</p> <p>Changes to the Active Directory schema have not replicated to all Active Directory servers in the domain.</p>	<p>Ensure the Active Directory component for 3Com Network Access Manager is installed on one Active Directory server in the domain.</p> <p>If you have already installed the Active directory component on an Active Directory server in the domain, then you may need to wait for the schema changes to replicate to the other Active Directory servers in the domain, this may take some time. Alternatively, you can 'force' replication between Active Directory servers, consult the Microsoft documentation for further information.</p>
<p>Using the Network Administrator user interface, right-clicking <i>Users</i> or <i>Groups</i> or <i>Computers</i> in the Tree pane and selecting <i>Properties</i> does not display a <i>Network Access</i> tab.</p> <p>The Current Rule column in the Details pane for <i>Users</i>, <i>Group</i> or <i>Computers</i>, shows "Not specified" for all entries</p>	<p>The Active Directory component for 3Com Network Access Manager has either not been installed on an Active Directory server in the network domain, or else has not yet replicated to all of the Active Directory servers in the domain</p>	<p>If you have not installed the Active Directory component for 3Com Network Access Manager, then install the component on one Active Directory server in the domain. The schema changes made by the component will be replicated to all of the Active Directory servers in the domain.</p> <p>If you have already installed the Active directory component on an Active Directory server in the domain, then you may need to wait for the schema changes to replicate to the other Active Directory servers in the domain. Alternatively, you can 'force' replication between Active Directory servers, consult the Microsoft documentation for further information.</p>
<p>"Computer-name = <unknown>" is logged in the 3Com Network Access Manager event log following an authentication attempt from this computer.</p>	<p>This is probably due to the computer's MAC address not having been entered into 3Com Network Access Manager.</p>	<p>Follow the steps in "Entering MAC Addresses For A Computer" in Chapter 3.</p>

Table 14 Problems That May Be Encountered When Setting Up (continued)

Symptom	Cause	Remedy
On a PC used by a Network Operator, selecting <i>Active Directory Users and Computers</i> , then right-clicking <i>Users</i> or <i>Computers</i> in the Tree pane and selecting <i>Properties</i> does not display a <i>Network Access</i> tab	The Operator User Interface component has not been installed on the Network Operator's PC.	Check that the Network Operator's PC meets the specifications in Table 5 and Table 6 in Chapter 2 , install the Operator User Interface component on the PC

Table 15 Possible Problems With Network Access

Symptom	Cause	Remedy
Incorrect RADIUS authorizations within the network domain	<p>Either:</p> <p>You have not installed the IAS component for 3Com Network Access Manager on all of the IAS servers in the domain, or else you have not restarted the servers after installation of the component.</p> <p>Or:</p> <p>You have not correctly set up a Remote Access Policy.</p>	<p>Identify the IAS server(s) issuing the incorrect RADIUS authorizations.</p> <p>For each IAS server suspected of issuing incorrect RADIUS authorizations use the Event Viewer to check for correct functionality of the server.</p> <p>From the Tree pane of Event Viewer, select <i>System Log</i> and look at the IAS responses in the Display pane, this will show the Policy that was used for each authorization from the server.</p> <p>From the Tree pane, select <i>3Com Network Access Manager Log</i>.</p> <p>If <i>3Com Network Access Manager Log</i> is not displayed in the Tree pane, then 3Com Network Access Manager has not been installed on the specific IAS server, or the IAS server has not been restarted after installation. Rectify as appropriate.</p> <p>If clicking on <i>3Com Network Access Manager Log</i> shows an empty Display pane, then 3Com Network Access Manager is installed on the server but the Remote Access Policy is not configured correctly. Refer to Appendix A for step by step instructions on correctly setting up a Remote Access policy.</p>

Table 15 Possible Problems With Network Access (continued)

Symptom	Cause	Remedy
The expected rules for a computer are not applied.	The computer's MAC address has not been entered correctly into 3Com Network Access Manager.	Follow the steps in "Entering MAC Addresses For A Computer" in Chapter 3 .
An event shown in the System event log displays the message: "Computer-Name = <unknown>"	The computer's MAC address has not been entered correctly into 3Com Network Access Manager	Follow the steps in "Entering MAC Addresses For A Computer" in Chapter 3 .
Unpredictable RADIUS authentication of a user, group or computer.	The authentication mode enabled on the network access device may be incompatible with the settings on the Action tab for the rule associated with the user, group or computer	Ensure the authentication mode selected on the network access device matches how the rule has been setup. Either change the rule setting or else select a different authentication mode on the network access device
A user, group or computer associated with a specific rule cannot gain network access.	<p>Either:</p> <p>The rule may be set to Deny network access.</p> <p>Or:</p> <p>The VLAN applied to the rule may not match the VLAN in the network access device (switch or wireless access point).</p> <p>Or:</p> <p>The user or computer does not have remote access permission enabled.</p> <p>Or:</p> <p>The user's password is not stored using reversible encryption.</p> <p>Or:</p> <p>The format of the RADIUS response may not be understood by the network access device.</p>	<p>Select the <i>Action</i> tab for the rule and check the network access setting.</p> <p>The network access setting may be set to Deny for a purpose, for example to blacklist a user or group and prevent network access.</p> <p>Ensure the VLAN set for the rule, matches the VLAN in the network access device. Refer to the user documentation shipped with the network access device for information on determining the VLAN assigned in the network access device.</p> <p>From the Dial-in tab (accessible by right-clicking Users or Groups or Computers in the Tree pane and selecting Properties) under Remote Access Permission, select "Allow access".</p> <p>From the Account tab (accessible by right-clicking Users or Groups or Computers in the Tree pane and selecting Account) under Account options, enable "Store password using reversible encryption".</p> <p>Check the format of the RADIUS response in the RADIUS file. If necessary add a new Authorization Type. See Customizing the Configuration Files.</p>

Table 15 Possible Problems With Network Access (continued)

Symptom	Cause	Remedy
The <i>Network Access</i> tab, accessible by right-clicking <i>Users</i> or <i>Groups</i> or <i>Computers</i> in the Tree pane and selecting <i>Properties</i> does not show the actual rule being applied to the user, group or computer.	<p>You may not have been granted read permission for the rule which is actually being applied to the user, group or computer. In which case the rule will not be listed for you.</p> <p>It is important that network administrators responsible for resolving network access problems are given read access on all rules created in 3Com Network Access Manager.</p>	Ask the network administrator who created the rules in 3Com Network Access Manager to grant you read permission for all rules.
The Current Rule column for User View, and Computer View does not show the actual rule being applied to the user or computer.	<p>You may not have been granted read permission for the rule which is actually being applied to the user, group or computer. In which case the rule will not be listed for you.</p> <p>It is important that network administrators responsible for resolving network access problems are given read access on all rules created in 3Com Network Access Manager</p>	Ask the network administrator who created the rules in 3Com Network Access Manager to grant you read permission for all rules.
The 3Com Network Access Manager Log shows a request as being accepted (displays 3ComAuthorization in the Source column), but user cannot gain network access.	<p>Either:</p> <p>The VLAN applied to the rule associated with the user may not match the VLAN in the network access device that the user connects to.</p> <p>Or:</p> <p>The authentication mode enabled on the network access device may be incompatible with the settings on the Action tab for the rule associated with the user, group or computer.</p> <p>Or:</p> <p>The format of the RADIUS response may be incompatible with the network access device.</p>	<p>Ensure the VLAN set for the rule, matches the VLAN in the network access device. Refer to the user documentation shipped with the network access device for information on determining the VLAN assigned in the network access device.</p> <p>Ensure the authentication mode selected on the network access device matches how the rule has been setup. Either change the rule setting or else select a different authentication mode on the network access device.</p> <p>Ensure the Network Access Manager Plug-in configuration file has the correct format for the device and that the correct Authorization Type is being used by the IAS Remote Access Policy</p>

Table 15 Possible Problems With Network Access (continued)

Symptom	Cause	Remedy
<p>Entry in system event log displays message: "A RADIUS message was received from invalid RADIUS client IP address xx.xx.xx.xx", and no response is returned to the device.</p> <p>There may be a delay before the user is informed of a log-in failure.</p>	<p>A network access device (switch or wireless access point) has not been added to IAS.</p>	<p>Add the network access device to IAS as a radius client with the client-vendor parameter set to '3Com'.</p>
<p>Incorrect EFW Policy is used for an EFW user</p>	<p>Either:</p> <p>Active Directory has not been updated with changes which affect the EFW Policy applied to the user.</p> <p>Or:</p> <p>There is a mismatch in configuration between Active Directory and the EFW Policy Server,</p> <p>Or:</p> <p>The EFW Policy has not been entered into 3Com Network Access Manager, or the EFW policy is not being used by a rule.</p>	<p>Press Recalculate EFW Membership button.</p> <p>Verify that the EFW Policy entered into 3Com Network Access Manager exists on the EFW Policy Server.</p> <p>Enter the EFW Policy information and assign to appropriate rule(s).</p>

Problems Related to Using the MAC Address Tool

This section details possible problems that you might experience when using the MAC Address tool. Each problem is described by a symptom, an explanation of the cause of the problem and a suggestion on what to do to remedy the problem.

The problems are listed in [Table 16](#).

Table 16 Problems That May Be Encountered When Using the MAC Address Tool

Symptom	Cause	Remedy
The MAC Address Tool reports the status for a computer as "Not Found: Computer is offline, or DCOM traffic is being blocked by a firewall"	Either: The computer is not accessible. Or: The computer does not have a supported operating system. Or: The computers Firewall is blocking the request.	If the computer is not running a supported operating system the MAC Address will have to be manually configured. If the computer is running a supported operating system check the Windows Firewall setting and ensure that the remote administration exception is enabled.
The MAC Address Tool reports the status for a computer as "Failed: WMI access permissions denied on this computer" or "Failed: DCOM access permissions denied on this computer"	The user does not have the required WMI or DCOM permissions to access the computer.	Either: Use an account with the appropriate privileges; normally a user who is a member of the Administrators group on the computer will have the appropriate permissions. Or: Update the WMI or DCOM permissions for the account.
The MAC Address Tool reports the status for a computer as "Not Supported: Check WMI service is installed and enabled"	The Windows Management Instrumentation (WMI) Service has been disabled on the computer.	Enable the WMI service on the computer.
The MAC Address Tool reports the status for a computer as "Failed: MAC already assigned to another computer in Active Directory"	Either: The Network Adaptor has been moved between two computers. Or: The computer has been removed from the domain and then rejoined with a different name.	Use the Find command to locate the computer account in Active Directory which has the MAC Address assigned and remove the MAC Address. Execute the MAC Address Tool again.

6

CUSTOMIZING 3Com NETWORK ACCESS MANAGER

Customizing 3Com Network Access Manager provides the following benefits:

- Tailors the response to the individual RADIUS Client (switch) device; this includes non-3Com devices.
- Adds support for new type or class of devices.
- Dynamic control over 3Com Network Access Manager participating in the RADIUS response.
- Dynamic addition of a single Rule when processing RADIUS access request.

For most situations the default format of the RADIUS Response will be compatible with the device (switch) being used to gain access to the network, customization is not normally needed. In a small number of situations customizing the RADIUS Response may be required. Examples would be:

- Support for non-3Com devices that do not conform to IETF RFC 3580
- Support for devices that can use policy setting other than the QoS filter attribute.

Similarly, for most situations the Rules assigned to Users and Computers in Active directory will provide the correct VLAN/QoS for the supplicant (user/computer) accessing the network. In some circumstances it may be appropriate to include additional Rules to be included as part of the authorization process. Examples would be:

- Health Check system that is called before 3Com Network Access Manager would like to have the current access request be placed into a Health Check VLAN/QoS.

- Accessing the network via a particular device requires a supplicant to be placed into a different VLAN/QoS from the normal VLAN/QoS.

3Com Network Access Manager Plug-in Processing

Before customizing 3Com Network Access Manager it is important to understand how IAS and the plug-in interact and how the plug-in processes an authorization request. IAS has two phases for a RADIUS Request: authentication phase and authorization phase. The authentication phase is where the username and password pair is verified, 3Com Network Access Manager has no role to play in this phase. For the authorization phase IAS will do its own processing and then each authorization plug-in currently loaded will be called. 3Com Network Access Manager Plug-in will be called as part of the authorization phase.

The 3Com Network Access Manager Plug-in has two areas of operation:

- At start-up of the RADIUS Server (IAS) the 3ComNAMIAS-Configuration.ini and 3ComNAMIAS-NASIdent.ini files are parsed to obtain the correct responses required for the different RADIUS Requests that can be catered for.
- For the Authorization phase the 3Com Network Access Manager Plug-in first checks that the RADIUS Request is valid for 3Com Network Access Manager processing and then selects the highest priority Rule to either reject the request or accept the request, responding with the VLAN / QoS settings defined in the Rule.

Check RADIUS Request is Valid for 3Com Network Access Manager

"Authorization Type" is a 3Com Vendor Specific Attribute (VSA) used by 3Com Network Access Manager both to identify which RADIUS access request messages are to be processed by the 3Com Network Access Manager Plug-in and, potentially, to control the attributes returned in the RADIUS access response message. If the VSA for Authorization Type is not included in the access request (either supplied by the device itself or set from the IAS Access Policy) then the device shall not receive the 3Com Network Access Manager VLAN or QoS assignments.

To verify that a RADIUS Request is to be processed the plug-in first selects an Authorization Type using the following algorithm:

- If the IP Address of the switch is in 3ComNAMIAS-NASIdent.ini file use the Authorization Type assigned to it.
- Else keep the Authorization Type provided by the Access Policy.

It then confirms it can provide a suitable RADIUS Response by verifying that the Authorization Type is defined in 3ComNAMIAS-Configuration.ini file. Lastly it performs pre-condition checks by parsing the RADIUS Attributes in the access request and response being constructed by IAS (Access Policy and any previous plug-in) for *match* or *no_match* attributes of the selected Authorization Type.

If the selected Authorization Type is defined in the configuration file and the pre-condition checks evaluate to true the plug-in will process the RADIUS request.

Select the Highest Priority Rule

The Plug-in obtains all the appropriate NAM Rules associated with this request from Active Directory these are: Rules associated with the username, Rules associated calling-station MacAddress, Rules provided by the IAS Access Policy and the Default Rule. The highest priority Rule is used to supply the RADIUS Response

Customizing the Configuration Files

The configuration files 3ComNAMIAS-Configuration.ini and 3ComNAMIAS-NASIdent.ini are located in the directory selected during installation of the product; the default location is `C:\Program Files\3Com\Network Access Manager`.

If a file is missing or cannot be parsed the 3Com Network Access Manager IAS plug-in will not return any RADIUS response information. If a file is not found or there is a parsing error an error is logged in the 3Com Network Access Manager Event log with an error event type that can then be viewed via the Microsoft Event Viewer.

The default files installed contain additional information which should be referred to when modifying the files.



CAUTION: Errors in the files will stop the plug-in from working correctly.



Make a copy of the files before changes are made so that a known working version can be restored.



The IAS Server must be restarted for changes to take effect.

3ComNAMIAS-Configuration.ini File

This is an administrator editable (for example, Notepad, etc) file that defines the Authorization Types that 3Com Network Access Manager

should accept and how they should be processed. The installed file includes definitions for the following types:

- 3Com Extended Usage
- IETF RFC 3580 Usage
- 3Com WX Wireless Usage

This file provides the following capabilities:

- Support for different types of RADIUS Client devices
 - Assignment of Authorization Type to RADIUS Response.
 - Defines the RADIUS attributes of the response and their format / type.
 - Create new Authorization Types for new devices.
- Flexible interaction with Policy Servers (i.e. Health)
 - Conditional execution of RADIUS Response

The file is formatted so that for each Authorization Type it defines the attributes to be returned for each 'action' ('Access allowed', 'VLAN assignment' and 'Policy assignment'). The attribute definitions support standard RADIUS attributes including VSAs and specify the syntax of the attribute value including if the name or the ID of the VLAN or QoS profile is included.

Within each Authentication Type it is possible to define pre-condition checks for the 3Com Network Access Manager plug-in that can be used to control if the NAM Rule actions are actually applied to an access attempt. This is done by adding "match" or "no_match" attribute pre-conditions. The pre-conditions identify the RADIUS attributes, including VSAs and optionally the attribute values. For example pre-condition settings can be used to prevent 3Com Network Access Manager from processing a request when a Health Server wants to isolate a device.

3ComNAMIAS-NASId ent.ini File

This is an administrator editable (for example, Notepad, etc) file that associates the Authorization Type to be used by the authorization plug-in based on the IP Address of the device (switch). Normally this is achieved by the IAS Remote Access Policy; however this may not always be possible.

For example a device that provides no vendor or product or name information may only be identified by the IP Address given to the device. Adding the device to this file provides an easy way to define the Authorization Type used to provide a RADIUS Response.

**Customizing IAS
Access Policy**

The IAS Access Policy specifies when 3Com Network Access Manager Plug-in is called and which Authorization Type is used. The RADIUS Response can be influenced by customizing the Access Policy to pass a Rule to the Plug-in. This is achieved using a 3Com VSA that contains the Rule name. When both the Authorization Type VSA and the Authorization Rule Name VSA are configured in the Access Policy the 3Com Network Access Manager authorization plug-in will lookup the rule in Active Directory using the supplied rule name. If a match is found then the Rule will be used in-conjunction with the Computer (MacAddress) and User Rules to determine the highest priority Rule and therefore the authorization response. If the rule is not found then the user/computer rule selection will occur and a Warning event will be logged in the 3Com Network Access Manager event log.

A

CREATING A REMOTE ACCESS POLICY

For 3Com Network Access Manager to authenticate users and computers accessing the network, an IAS Remote Access Policy must first be created.

This appendix provides step by step instructions on creating a remote policy when [Using Microsoft Windows Server 2003 Operating System](#).

Introduction to IAS Remote Access Policies

The IAS Remote Access Policies are an ordered set of rules that control how RADIUS access requests are processed. Each Remote Access Policy defines the following:

- one or more conditions that are used to determine if the policy is applied to an access request,
- a number of profile settings that control the processing of the access request,
- a remote access permission to allow or deny access.

If an access request matches with the conditions in several Remote Access Policies only the first Remote Access Policy in the list is applied.

When adding or modifying a Remote Access Policy for an IAS Server in which multiple Remote Access Policies are configured the administrator should check the various Policy Conditions and the order of the policies to ensure that the correct Access Policy is selected for different access requests.



When creating multiple Remote Access Policies to match different device types the Remote Access Policies should normally be ordered such that the more specific are earlier in the list then the more general policies in order to limit the number of Policies that need to be defined.



When creating Remote Access Policies to process access requests from different devices where it is not possible to easily distinguish between them (based upon the contents of the access request), then the RADIUS

Clients can be assigned names that can be used to filter the devices in the policy conditions.

For example, to create different policies that process access requests from 3Com Wireless switches, 3Com Wireless Access Points and 3Com Wired switches you could use the following Policy Conditions:

3Com Wireless Switch Policy

Client-Vendor	matches "3Com"
Client-Friendly-Name	matches "WX*"
NAS-Port-Type	matches "Wireless-IEEE 802.11"

NOTE: * is used as a wildcard that matches with the remaining part of the RADIUS Client name.

3Com Wireless Access Point Policy

Client-Vendor	matches "3Com"
NAS-Port-Type	matches "Wireless-IEEE 802.11"

3Com Wired Switch Point Policy

Client-Vendor	matches "3Com"
NAS-Port-Type	matches "Ethernet"

If each 3Com Wireless switch is assigned an IAS Friendly Name that starts "WX" they will receive the first policy. While the 3Com Wireless Access Points which should be assigned a Friendly Name that does not begin with "WX", will receive the second policy.

Using Microsoft Windows Server 2003 Operating System

Follow these steps to create a new remote access policy within IAS using Microsoft Windows Server 2003 Operating System. The example used in this section details setting up for a Wired Switch such as the Switch 5500 or X-Family devices. Where the procedure for setting up a Wireless Switch differs this is highlighted.



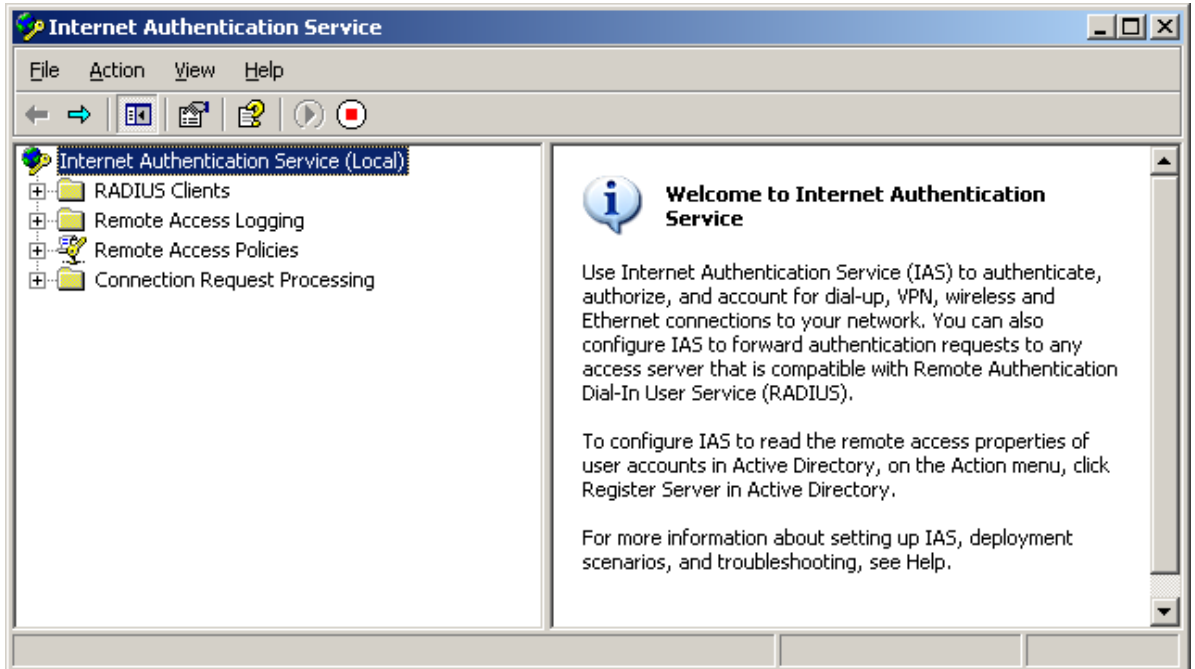
The "IAS Connection Request Policies" must be configured to allow the IAS Server to process the access requests from the switch. The default IAS connection policy created when IAS is installed allows all access requests to be processed by the IAS server.

Creating a New Remote Access Policy

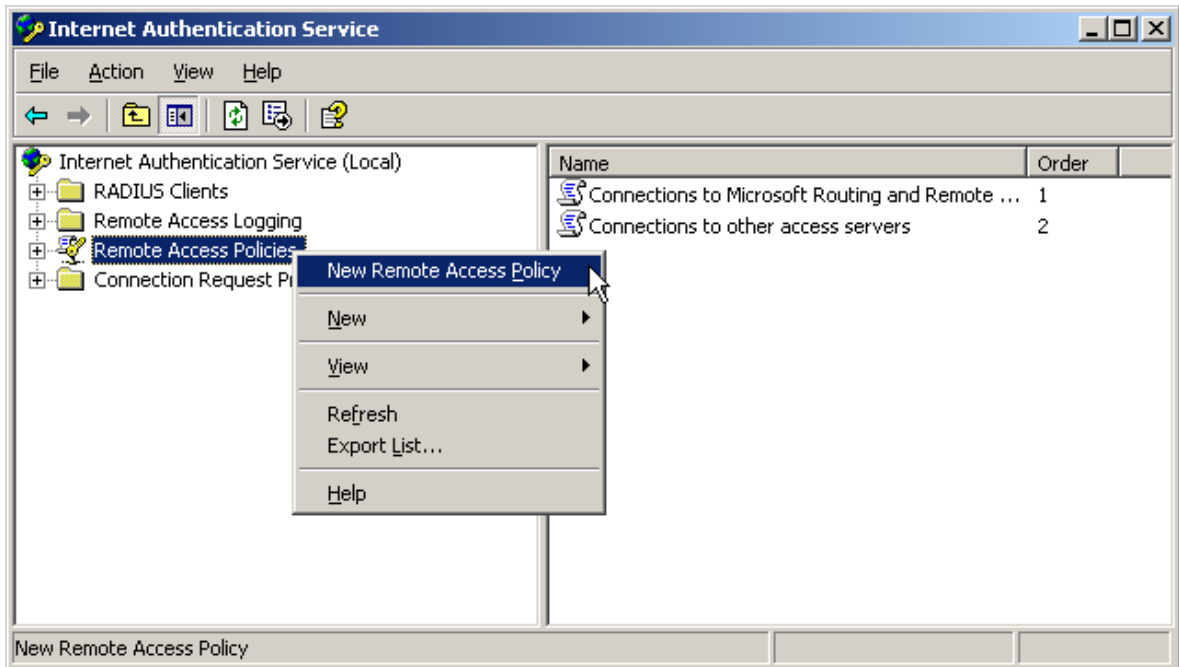
This section details how to create a remote access policy.

- 1 Select *Programs>Administrative Tools>Internet Authentication Service*

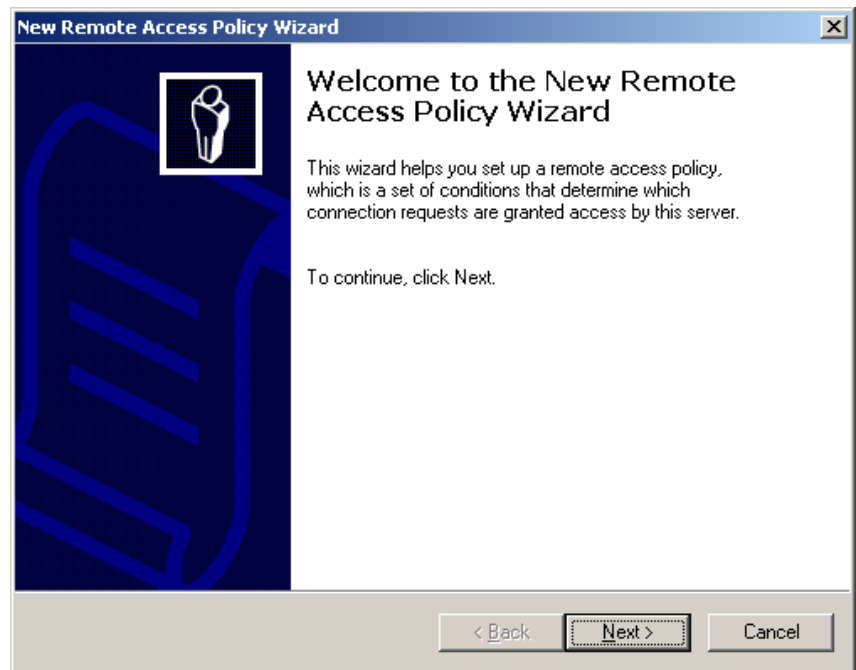
Figure 38 IAS Main Window



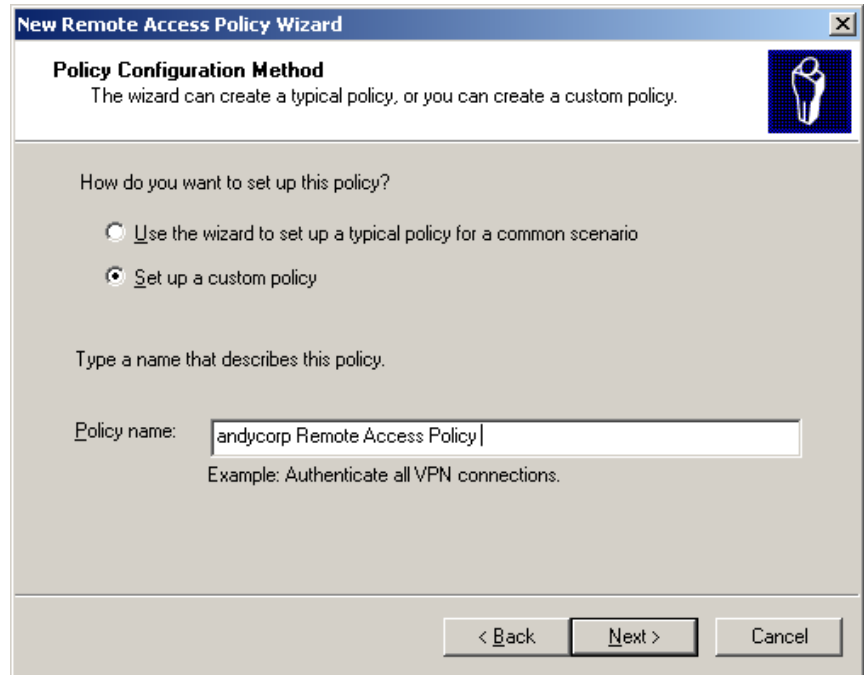
- 2 Right-click *Remote Access Policies* in the Tree pane and select *New Remote Access Policy*, see [Figure 39](#).

Figure 39 New Remote Access Policy

- 3 The New Remote Access Policy Wizard will be displayed, [Figure 40](#). Select *Next*.

Figure 40 New Remote Access Policy Wizard.

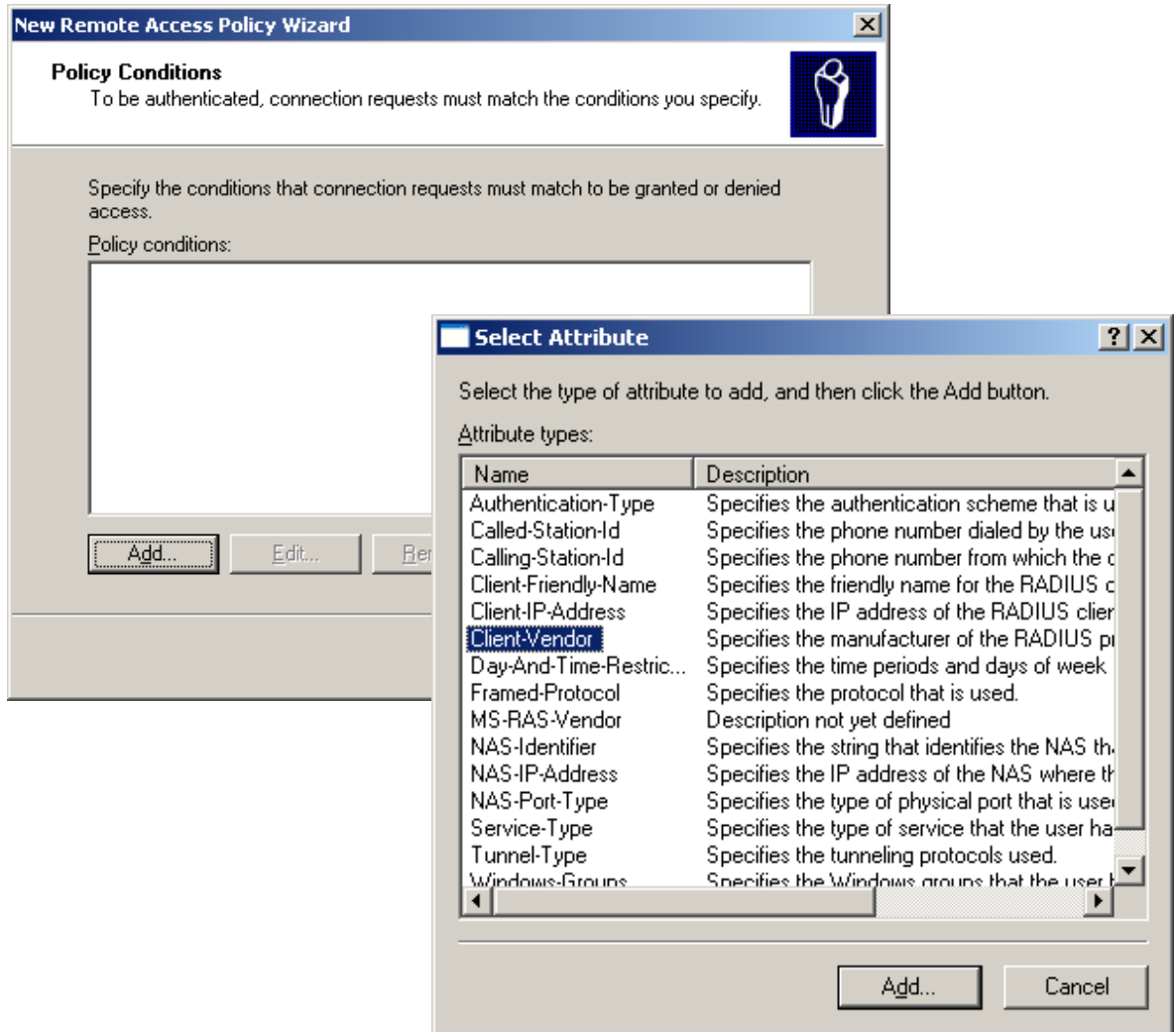
- 4 Select *Set up a custom policy* and type the name of the policy. Click *Next*.

Figure 41 Set Up A Custom Policy

You now need to add a condition that will cause the Remote Access Policy to run.

- 5 Add the conditions that will match the access requests to be processed by this Remote Access Policy. For example, to match access requests from 3Com Wired switches add conditions for the Client Vendor and the NAS-Port-Type as follows:

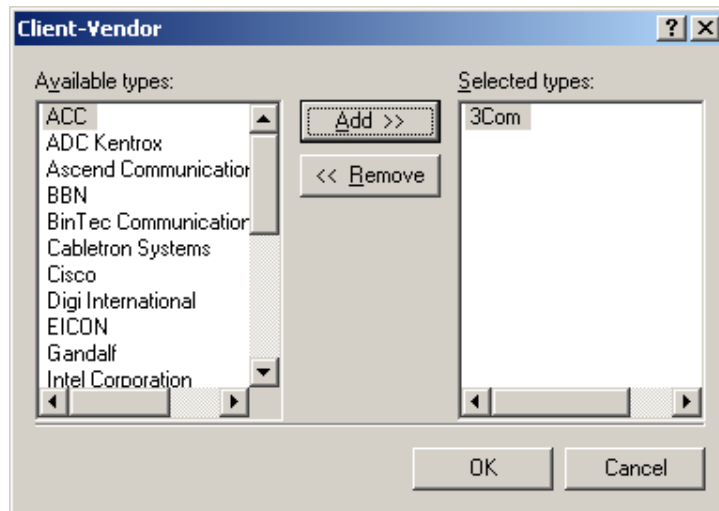
On the *Policy Conditions* dialog, click *Add*. On the *Select Attribute* dialog select `client vendor` and click *Add*, see [Figure 42](#).

Figure 42 Selecting Attributes for Remote Access Policy

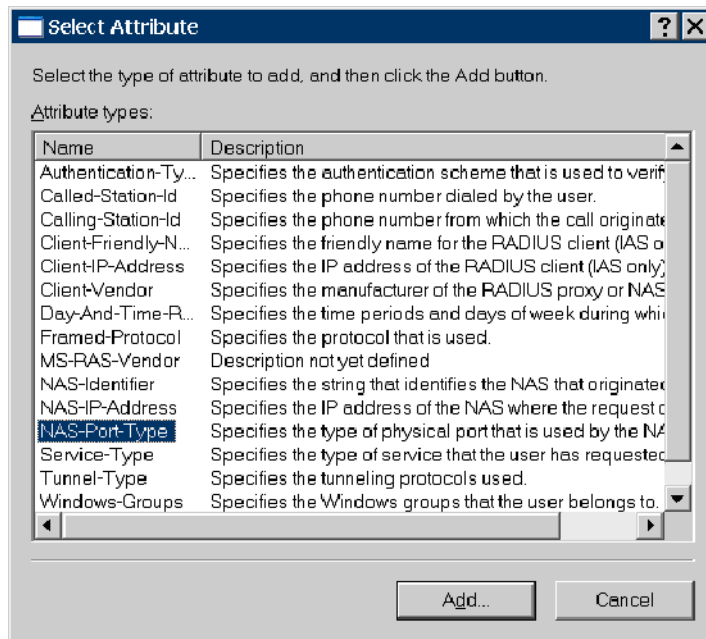
- 6 Highlight 3com in the *Available types* list and use the *Add>>* button to move 3com to the *Selected types* list, see [Figure 43](#). Click *OK*.



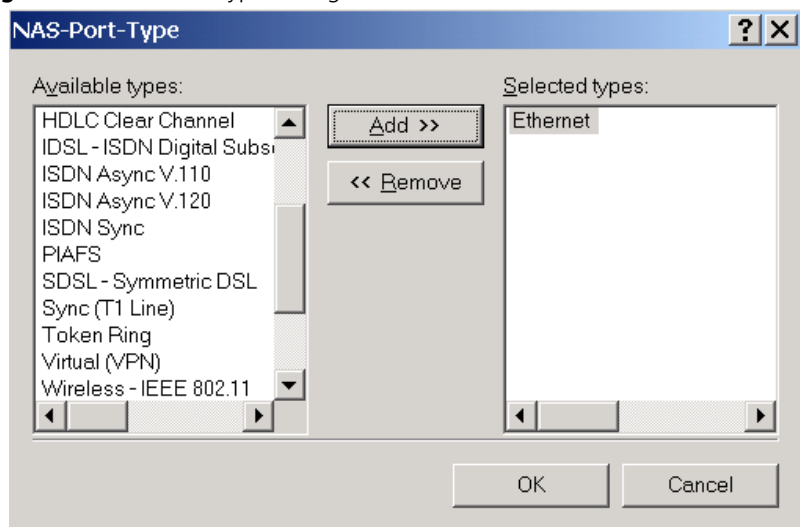
The IAS RADIUS Clients that correspond to the 3Com switches must be configured with the Client-Vendor property set to "3Com".

Figure 43 Selecting 3Com as Client-Vendor for Remote Access Policy

On the Policy Conditions dialog, click *Add*, on the Select Attribute dialog select *NAS-Port-Type* and click *Add*, see [Figure 44](#).

Figure 44 Select Attribute Dialog

In the NAS-Port-Type dialog select *Ethernet* in the *Available types* and click *Add>>* to move *Ethernet* to the *Selected types*, see [Figure 45](#). Click *OK*.

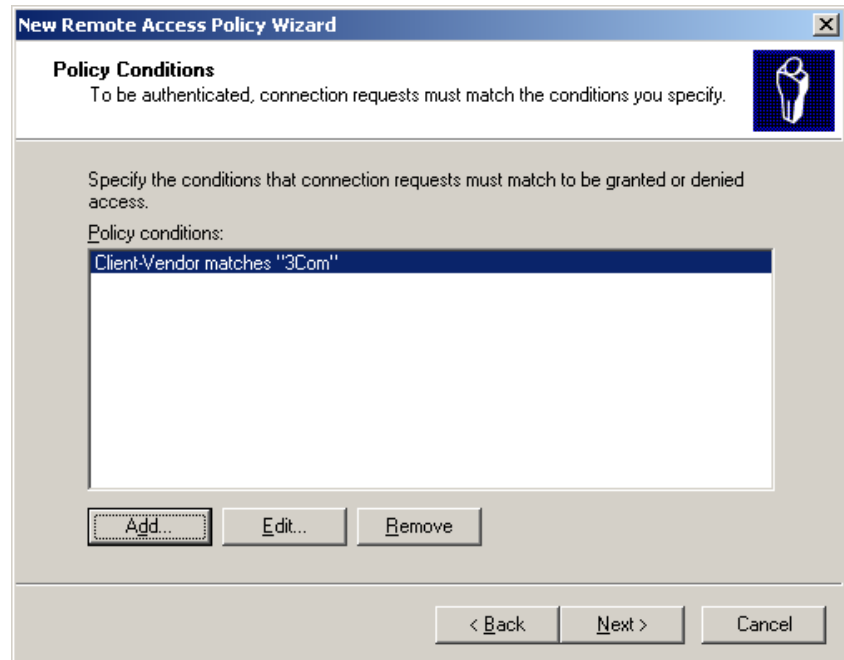
Figure 45 NAS-Port-Type Dialog



If the Remote Access Policy is to be used to match wireless devices then add Wireless - 802.11 to the Selected types for the NAS-Port-Type Policy Conditions.

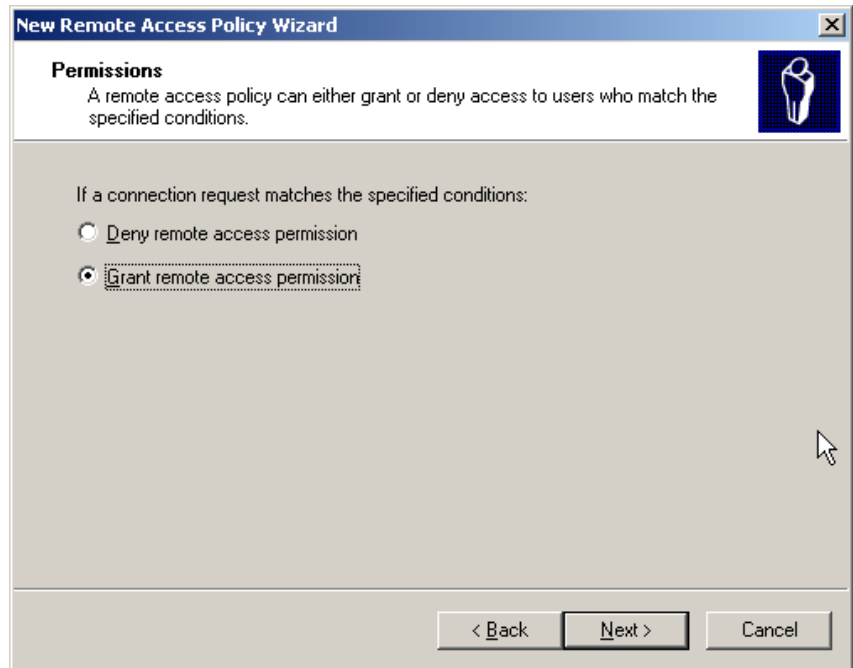
- 7 On the *Policy Conditions* dialog, [Figure 46](#), click *Next*

Figure 46 Setting Policy Conditions on Remote Access Policy



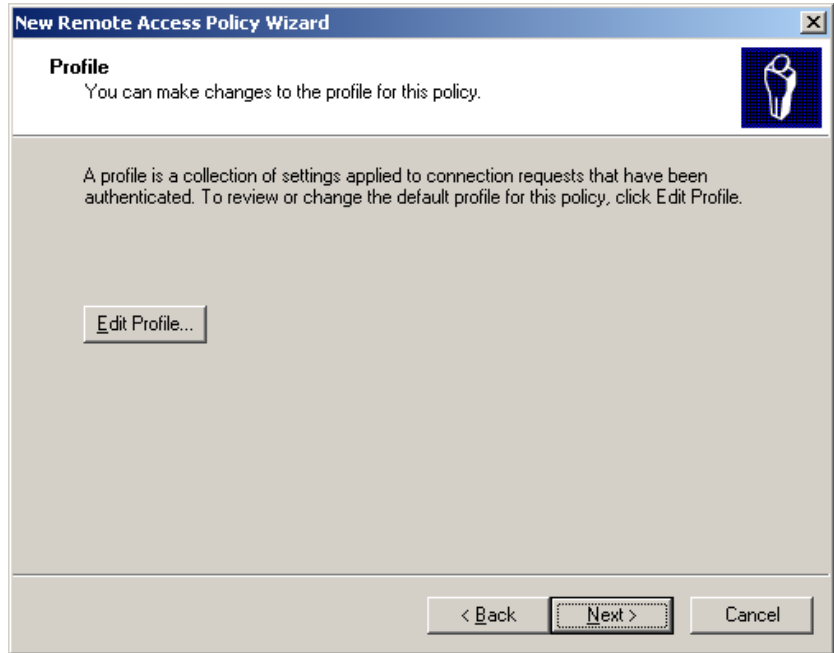
- 8 On the *Permissions* dialog, [Figure 47](#), select *Grant remote access permission* and click *Next*.

Figure 47 Granting Remote Access Permission



- 9 You now need to specify the profiles of the users who match the condition you have specified. Click the *Edit Profile* button, see [Figure 48](#).

Figure 48 Editing the Profile

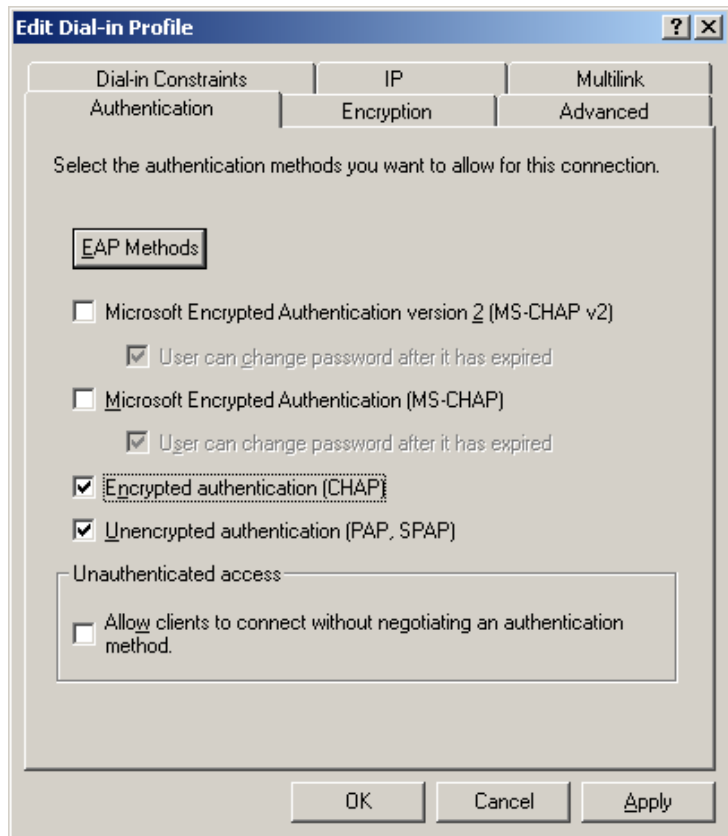


- 10 Select the *Authentication* tab, and select the appropriate authentication methods according to your network security policy and the devices on the network, see [Figure 49](#).

Configure the EAP methods if the policy is intended to be used with IEEE 802.1X based authentications.

Select the CHAP and PAP settings if the policy is intended to be used for MAC Address based authentications. These options should be deselected if only using IEEE802.1X.

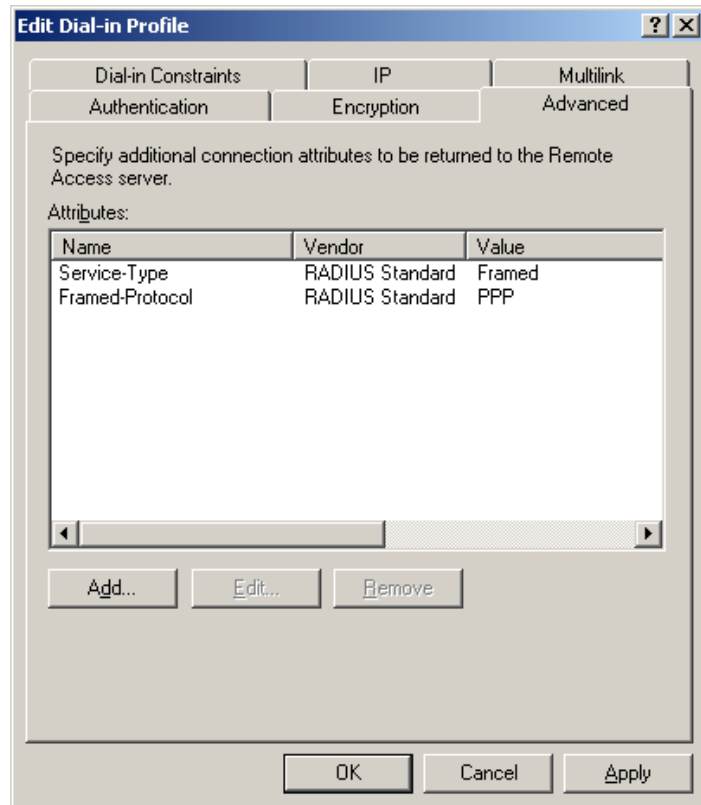
Figure 49 Selecting Encryption Methods



Ensure that the EAP type selected for the policy is consistent with the IEEE802.1X client settings.

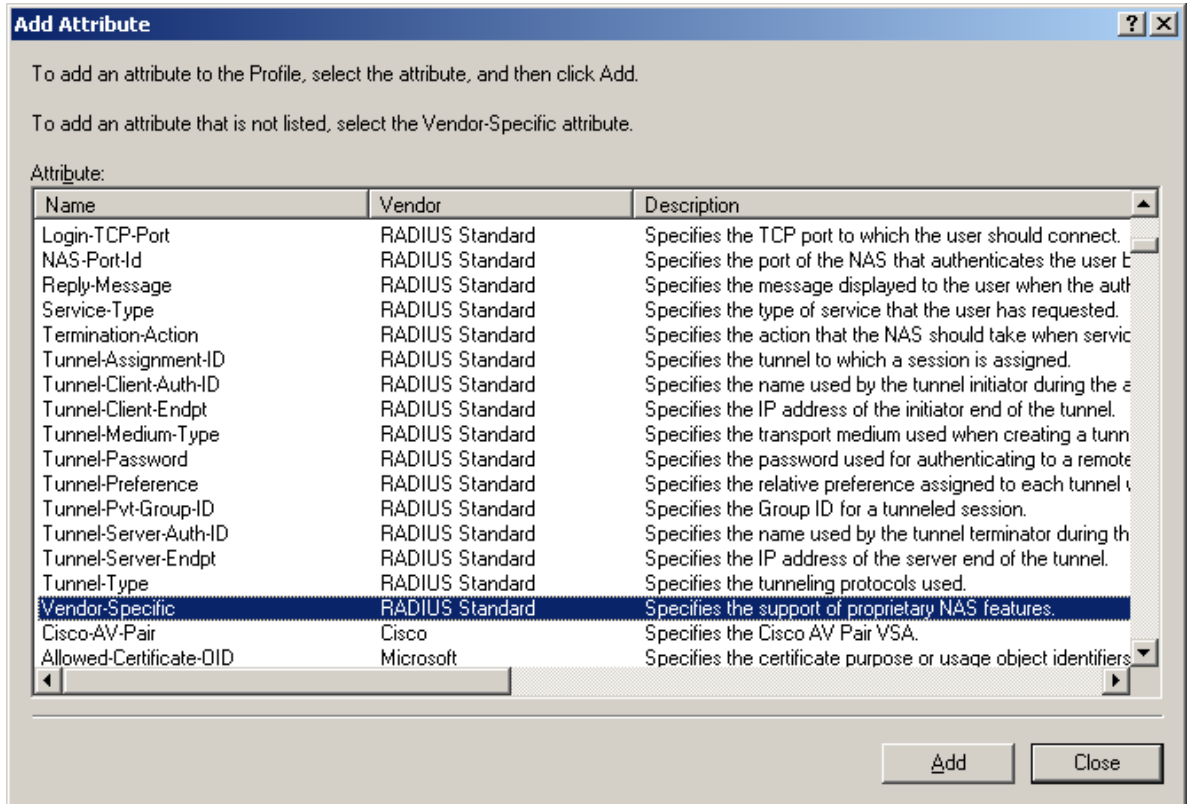
- 11 Add the 3Com Authorization Type VSA to the profile as follows: select the *Advanced* tab and click *Add*, see [Figure 50](#).

Figure 50 Editing the Dial-in Profile



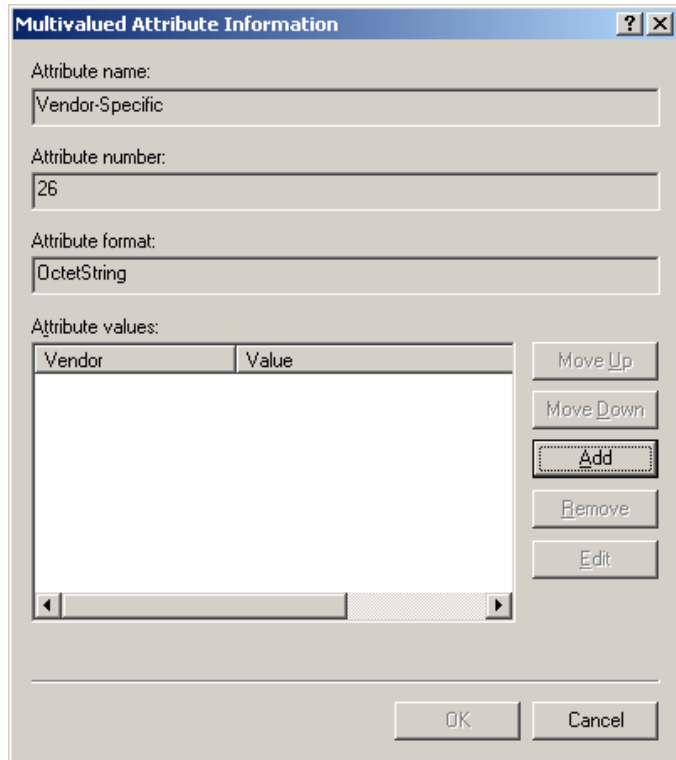
- 12 Select `vendor specific` from the list of RADIUS attributes and click *Add*, see [Figure 51](#).

Figure 51 Adding Vendor-Specific Attributes



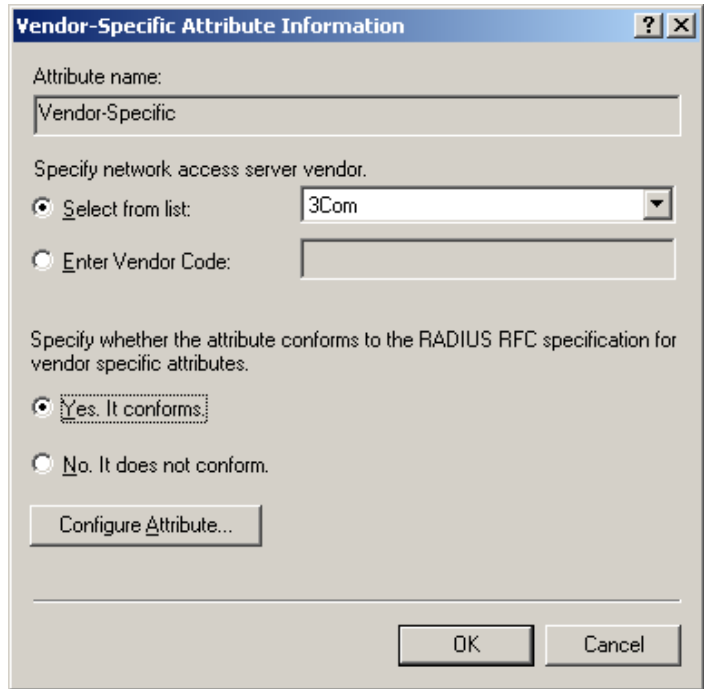
- 13 On the *Multivalued Attribute Information* dialog, see [Figure 52](#), click *Add*

Figure 52 Multivalued Attribute Information Dialog



- 14 Select 3Com from the pull down list, click *YES. It conforms* and click *Configure Attribute*, see [Figure 53](#)

Figure 53 Configuring Vendor-Specific Attribute



Vendor-Specific Attribute Information

Attribute name:
Vendor-Specific

Specify network access server vendor.

Select from list: 3Com

Enter Vendor Code:

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

Yes. It conforms.

No. It does not conform.

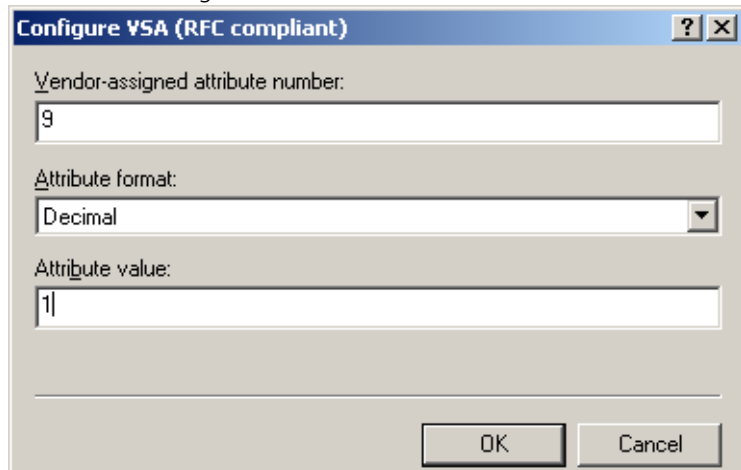
Configure Attribute...

OK Cancel

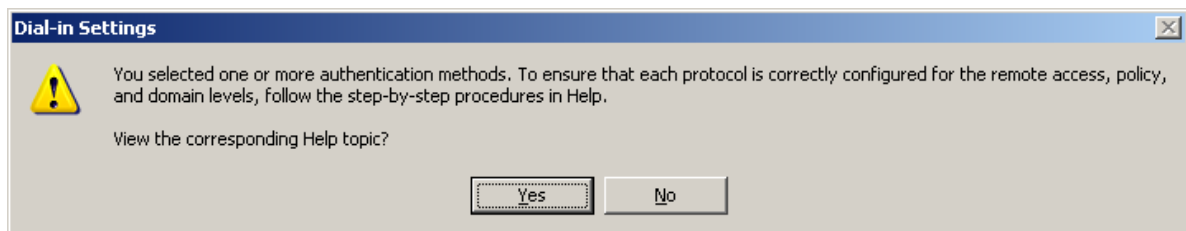
- 15 Type 9 as the vendor assigned value, select **Decimal** as the Attribute format, and type 1 as the Attribute value. See [Figure 54](#). Click *OK*.



The Attribute value entered must match with the appropriate Authorization Type for the device (for example, 1 for the Switch 5500). (See [Table 3](#) on [page 20](#) for a list of supported devices.). This tells the 3Com Network Access Manager IAS plug-in that it should process this access request and controls the format of the 3Com Network Access Manager authorization response (VLAN and Policy).

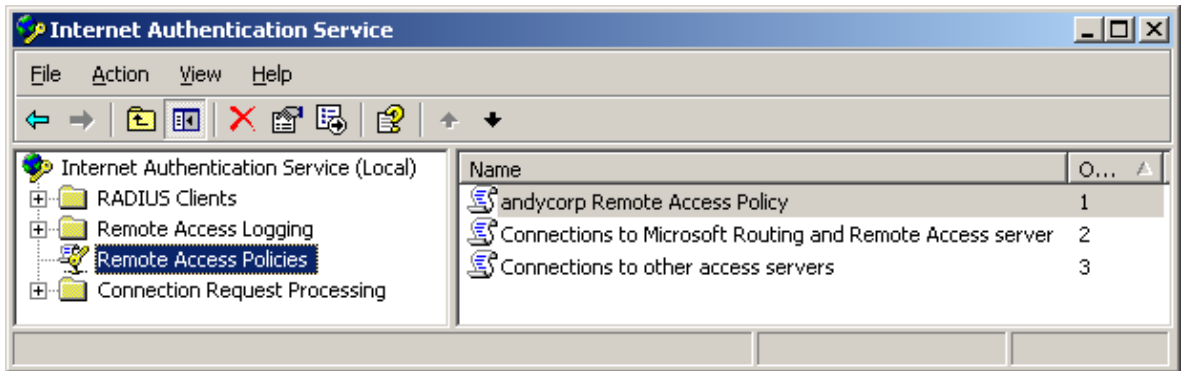
Figure 54 Vendor Assigned Attributes for 3Com

- 16 Click *OK* to close the *Vendor-Specific Attribute Information* dialog
- 17 Click *OK* to close the *Multivalued Attribute Information* dialog
- 18 Click *Close* to close the *Add Attributes* dialog
- 19 Click *OK* to close the *Edit Dial-In Profile* dialog
- 20 If you selected authentication method(s) in [step 10](#), you will be given the opportunity to view the IAS Online Help to check that you have configured the protocol correctly, see [Figure 55](#).

Figure 55 View Protocol Help Topic.

- 21 After viewing the Online Help, click *Finish*. The remote access policy that you have just created will be added to the list of policies, see [Figure 56](#)

Figure 56 New Remote Access Policy Added to List



- 22 Select the new remote access policy from the list in the Detail pane. Use the \updownarrow buttons on the tool bar at the top of the window to increase or decrease the priority of the new remote access policy with respect to other specific policies that you have created, and to match your network security requirements.
- 23 This completes creating a new remote access policy using Microsoft Windows Server 2003 Operating System.



In a mixed-vendor network where only 3Com switches are to be authenticated through 3Com Network Access Manager, the Remote Access Policy needs to be adjusted to only match 3Com devices. This should only be undertaken by a network administrator familiar with the process.

B

USING MICROSOFT WINDOWS SERVER 2008 OPERATING SYSTEM

Windows Server 2008 is not due to ship until 2008 therefore the behavior and user interface of Windows Server 2008 may change. 3Com Network Access Manager V1.2 was tested using Windows Server 2008 Beta 3 release which may not be identical to the shipping product. The information contained in this guide is correct at the time of publication.

Network Policy Server (NPS) is the new version of Internet Authentication Service (IAS). NPS provides Network Access Protection (NAP). 3Com Network Access Manager v1.2 is designed to be compatible with NAP.

For 3Com Network Access Manager to authenticate users and computers accessing the network, an NPS Remote Access Policy must first be created.

This appendix provides step-by-step instructions on creating a remote policy when using Microsoft Windows Server 2008 Operating System.

It details the following scenarios:

- [Configuring NPS for Health Checking with a 3Com Network Access Manager Response](#)
- [Configuring NPS for Network Access with a 3Com Network Access Manager Response](#)
- [Case Study — Microsoft NAP Health Checking with 3Com Network Access Manager Response](#)

This guide assumes that you are using Active Directory for your 'Users and Computers' management and that it is already installed and the server is the Domain Controller.

Configuring NPS for Health Checking with a 3Com Network Access Manager Response

This section describes how to configure a Network Policy Server (NPS) for health checking with a 3Com Network Access Manager response.

NPS Configuration

Follow these steps to create a new Network Access Policy in NPS that will receive and process the authentication request and also pass it onto 3Com Network Access Manager for further processing.



Windows Server 2008 contains a new feature called User Account Control (UAC) that requires the user to approve certain actions in the system. Several of the configuration tasks to follow require UAC approval. When prompted you should click Continue to authorize these changes.

Install the NPS Server Role

- 1 Click *Start > Server Manager*.
- 2 Under *Roles Summary*, click *Add roles*, and then click *Next*.
- 3 Select the *Network Policy and Access Services* check box, and then click *Next* twice.
- 4 Select the *Network Policy Server* check box, click *Next*, and then click *Install*.
- 5 Verify the installation was successful, and then click *Close* to close the Add Roles Wizard dialog box
- 6 Close the Server Manager window.

Configure the NPS to be a NAP Health Policy Server

- 1 Click *Start > Administrative Tools > Network Policy Server*.
- 2 Double-click *RADIUS Clients and Servers*.
- 3 Right-click *RADIUS Clients*, and then click *New RADIUS Client*.
- 4 In the *New RADIUS Client* dialog box, under *Friendly name*, type **802.1x switch**. Under *Address (IP or DNS)*, type **<your switch ip>**, under *Vendor name* select *3Com*.
- 5 Under *Shared secret*, type **<secret password>**.
- 6 Under *Confirm shared secret*, re-type **<secret password>**.

- 7 Select the *Request must contain the Message Authenticator attribute* check box, and then click *OK*.
- 8 In the left pane, click *RADIUS Clients*. Your new RADIUS client should be displayed in the middle pane.
- 9 Double-click the new RADIUS client to display the New RADIUS Client dialog box as shown in [Figure 57](#).
- 10 Tick the *Enable this RADIUS client* check box.
- 11 Ensure the *RADIUS client is NAP-capable* check box is cleared.

Figure 57 New RADIUS Client Dialog Box

The screenshot shows the 'New RADIUS Client' dialog box with the following configuration:

- Enable this RADIUS client
- Name and Address**
 - Friendly name: 802.1X Switch
 - Address (IP or DNS): 192.168.0.3
- Vendor**
 - Vendor name: 3Com
- Shared Secret**
 - Manual Generate
 - Shared secret: [Redacted]
 - Confirm shared secret: [Redacted]
- Additional Options**
 - Access-Request messages must contain the Message-Authenticator attribute
 - RADIUS client is NAP-capable

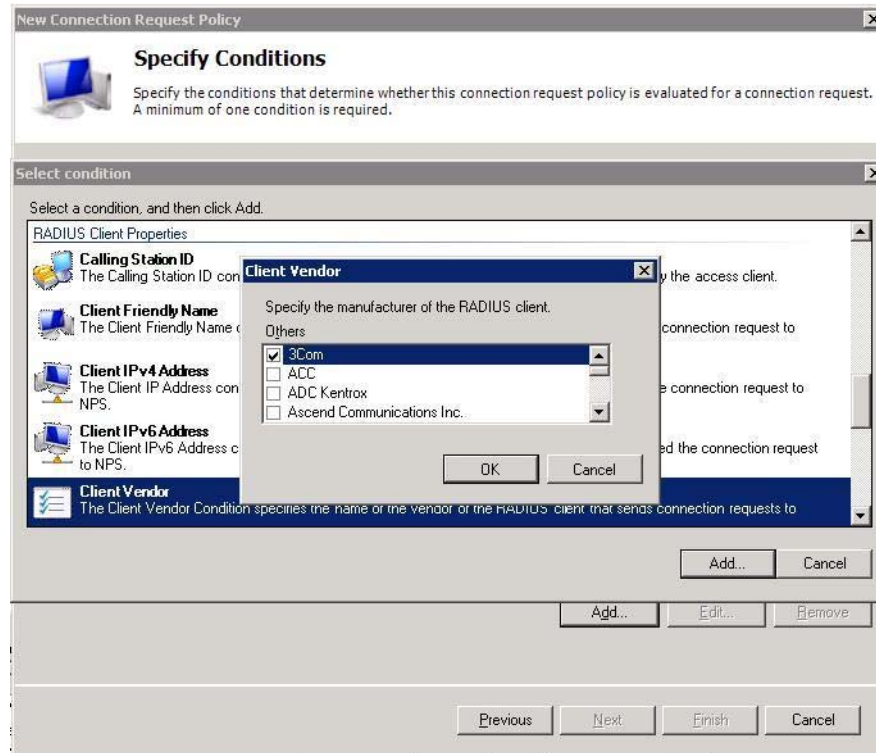


The RADIUS shared secret entered here must be identical to the one entered on your switch.

Configure Connection Request Policy

- 1 Double-click on *Policies*, and then select *Connection Request Policies*.
- 2 Disable the default Connection Request Policy found under the *Policy Name* area: right-click the policy, and then click *Disable*.
- 3 Right-click on *Connection Request Policies*, and then select *New*.
- 4 In the *Specify Connection Request Policy Name and Connection Type* window, under *Policy name*, type **NAM PEAP Policy**.
- 5 Click *Next*, and then click *Add*.
- 6 Double-click *Client-Vendor*, select *3Com* from the list, and then click *OK*.

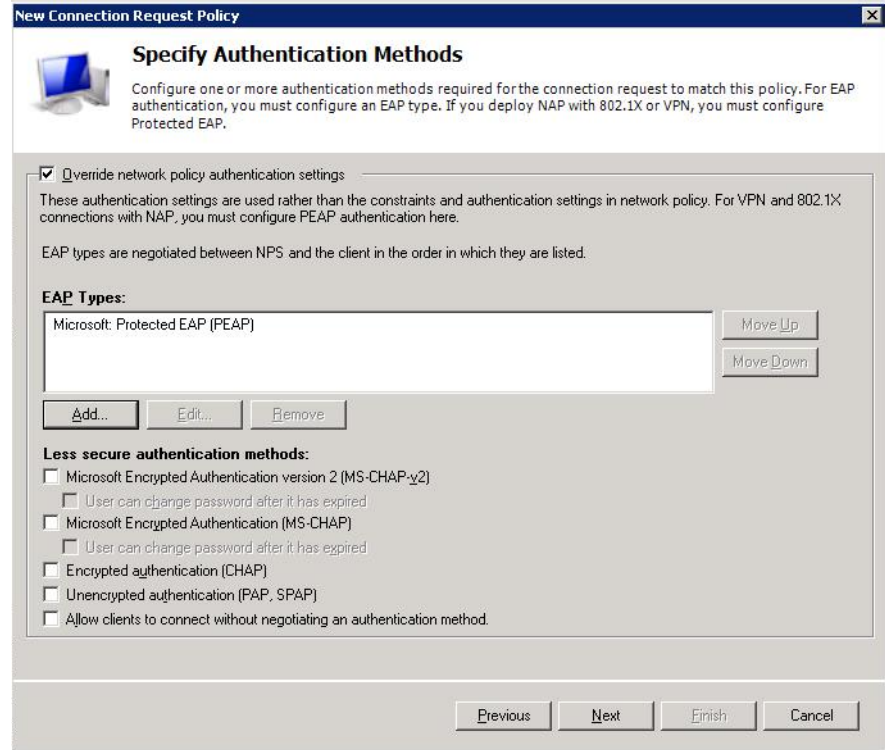
Figure 58 New Connection Request Policy Dialog Box — Specify Conditions



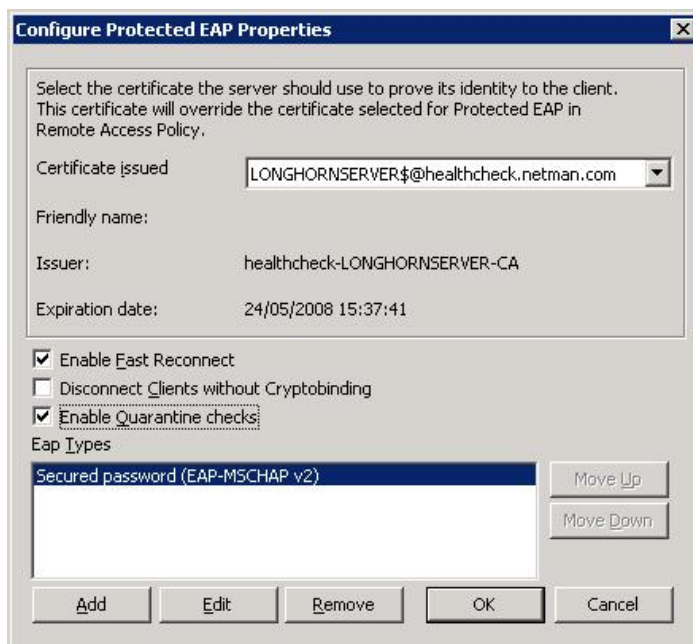
- 7 Click *Next*, verify that *Authenticate requests on this server* is selected, and then click *Next*.
- 8 In the *Specify Authentication Methods* window, select *Override network policy authentication settings*, and then click *Add*.

- 9 In the *Add EAP* dialog box, under *Authentication methods*, select *Microsoft: Protected EAP (PEAP)*, and then click *OK*. Select any other modes that are used on the network.

Figure 59 New Connection Request Policy Dialog Box — Specify Authentication Methods

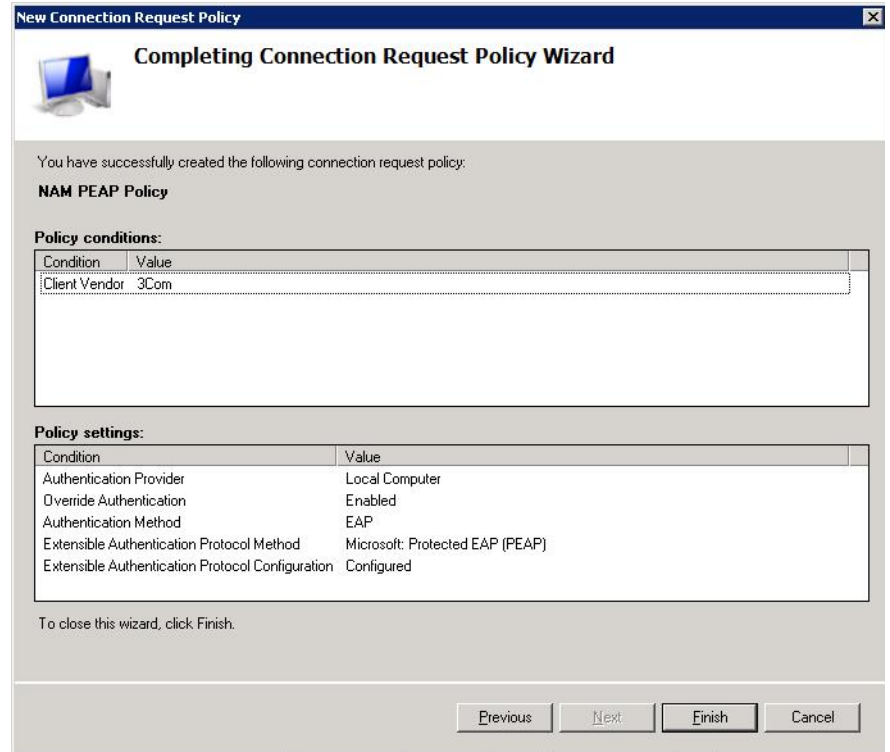


- 10 Click *Edit*, and verify that *Enable Quarantine checks* is selected, and your domain appears next to *Certificate issued*.

Figure 60 Configured Protected EAP Properties Dialog Box

- 11 Click *OK*. Then click *Next* twice, and then click *Finish*. This completes the configuration of your PEAP connection request policy.

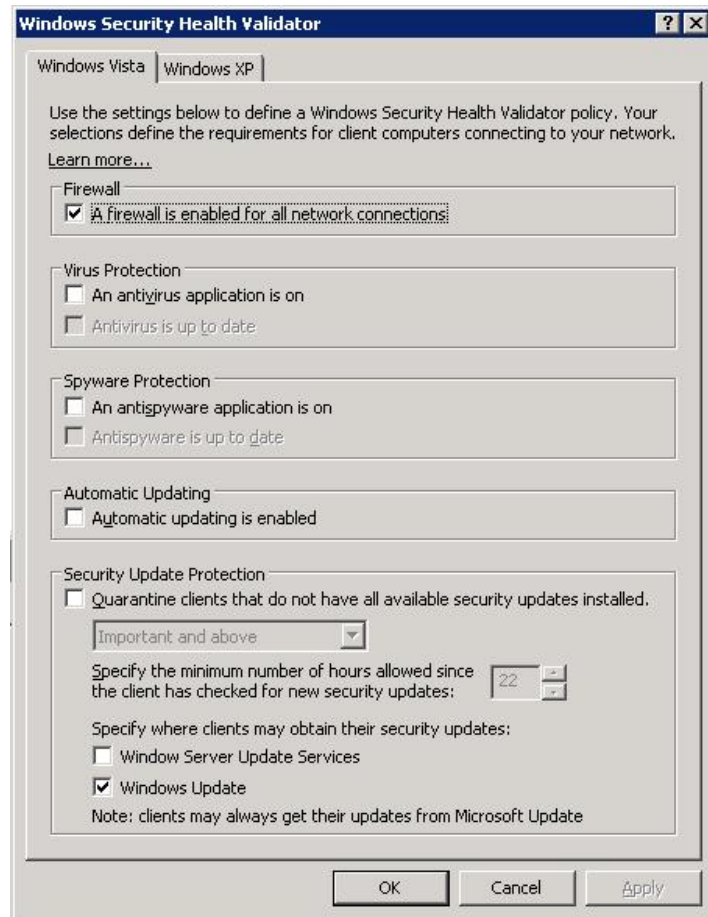
Figure 61 New Connection Request Policy Dialog Box — Completing Connection Request Policy Wizard



Configure System Health Validators

System Health Validators provide a list of the basic requirements a computer should meet that wants access to the network. For this configuration we will only require that the Windows Firewall is enabled.

- 1 Double-click *Network Access Protection*, and then select *System Health Validators*.
- 2 In the middle pane under *Name*, double-click *Windows Security Health Validator*.
- 3 In the Windows Security Health Validator Properties dialog box, click *Configure*.
- 4 Clear all check boxes except *A firewall is enabled for all network connections*. You do not need to clear the *Windows Update* check box.

Figure 62 Windows Security Health Validator Properties Dialog Box

- 5 Click *OK* to close the Windows Security Health Validator dialog box, and then click *OK* to close the Windows Security Health Validator Properties dialog box.

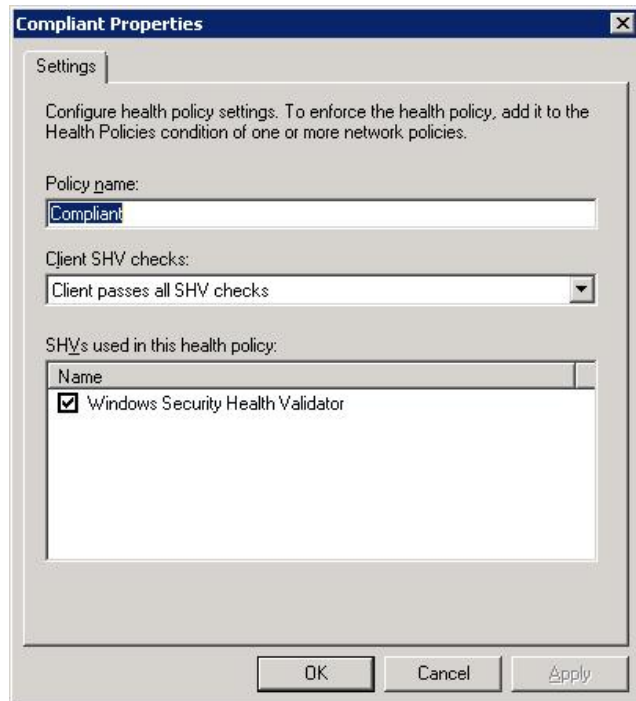
Configure Health Policies

Health policies define which Security Health Validators (SHVs) are evaluated, and how they are used in validating the configuration of computers that attempt to connect to your network. Based on the results of SHV checks, health policies classify client health status. This test lab

defines two health policies, one that corresponds to a compliant health state and one that corresponds to a noncompliant health state.

- 1 Double-click *Polices*.
- 2 Right-click *Health Policies*, and then select *New*.
- 3 In the Create New Health Policy dialog box, under *Policy Name*, type **Compliant**.
- 4 Under *Client SHV checks*, verify that *Client passes all SHV checks* is chosen.
- 5 Under *SHVs used in this health policy*, select the *Windows Security Health Validator* checkbox, as shown in the following example, and then click *OK*.

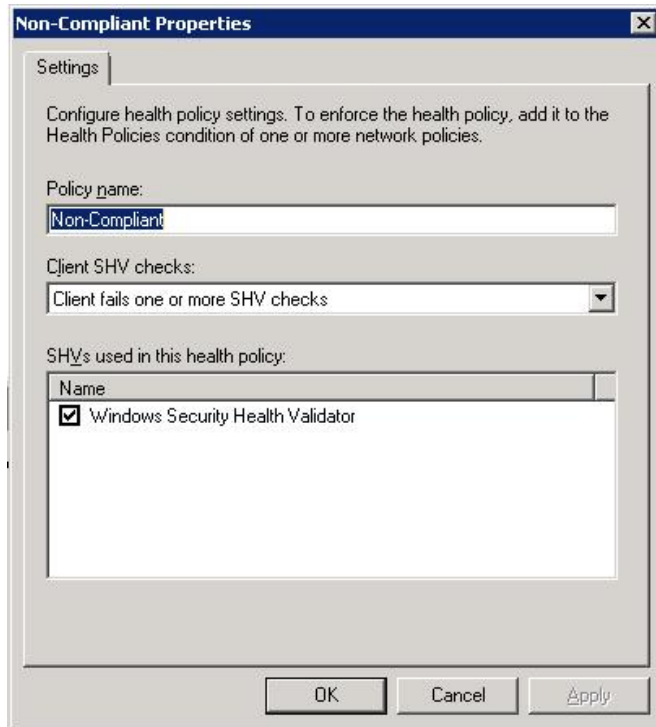
Figure 63 Create New Health Policy Dialog Box — Compliant Properties



- 6 Right-click *Health Policies*, and then select *New*.
- 7 In the Create New Health Policy dialog box, under *Policy name*, type **Noncompliant**.
- 8 Under *Client SHV checks*, choose *Client fails one or more SHV checks*.

- 9 Under *SHVs used in this health policy*, select the *Windows Security Health Validator* check box.

Figure 64 Create New Health Policy Dialog Box — Non-Compliant Properties



- 10 Click *OK*.

Configure Network Policies

Network policies allow you to configure who is authorized to access the network and the circumstances in which they can and cannot connect to the network. It allows you to specify which VLAN etc. the client should be placed on depending on the circumstances. With NAM we can get NPS to tell NAM which rule it should use and it is down to NAM to assign the appropriate VLAN/Policy based on the rule it is given.

a) Configure a Network Policy for Noncompliant Client Computers

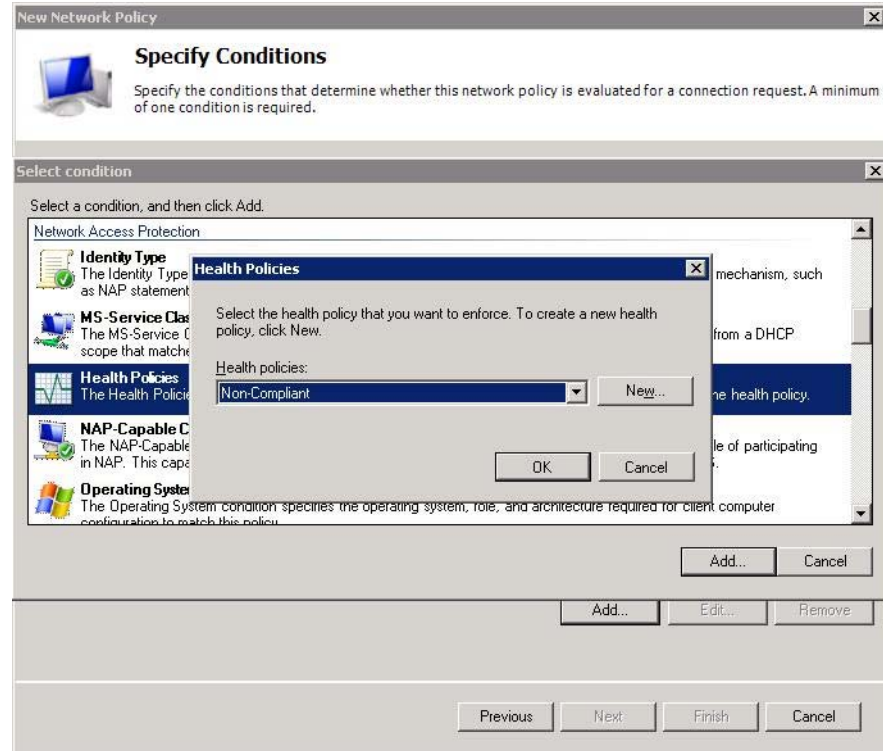
Firstly, create a network policy to match network access requests made by noncompliant client computers.

- 1 Right-click *Network Policies*, and then select *New*.
- 2 In the Specify Network Policy Name and Connection Type window, under *Policy name*, type *Noncompliant-Restricted*, and then click *Next*.

Figure 65 New Network Policy Dialog Box — Specify Network Policy Name and Connection Type

The screenshot shows a dialog box titled "New Network Policy" with a sub-title "Specify Network Policy Name and Connection Type". Below the sub-title is a small icon of a computer and a descriptive sentence: "You can specify a name for your network policy and the type of connections to which the policy is applied." The main area contains a "Policy name:" label followed by a text box containing "Non-Compliant Restricted". Below this is a section titled "Network connection method" with a descriptive sentence: "Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required." There are two radio buttons: "Type of network access server:" (which is selected) and "Vendor specific:". Under "Type of network access server:" is a dropdown menu currently showing "Unspecified". Under "Vendor specific:" is a text box containing "10". At the bottom right of the dialog box are four buttons: "Previous", "Next", "Finish", and "Cancel".

- 3 In the Specify Conditions window, click *Add*.
- 4 In the Select Condition dialog box, double-click *Health Policies*.
- 5 In the Health Policies dialog box, under *Health policies*, select *Noncompliant*, and then click *OK*.

Figure 66 New Network Policy Dialog Box — Specify Conditions

- 6 In the Specify Conditions window, verify that Health Policy is specified under Conditions with a value of *Noncompliant*, and then click *Next*.
- 7 In the Specify Access Permission window, verify that *Access granted* is selected.

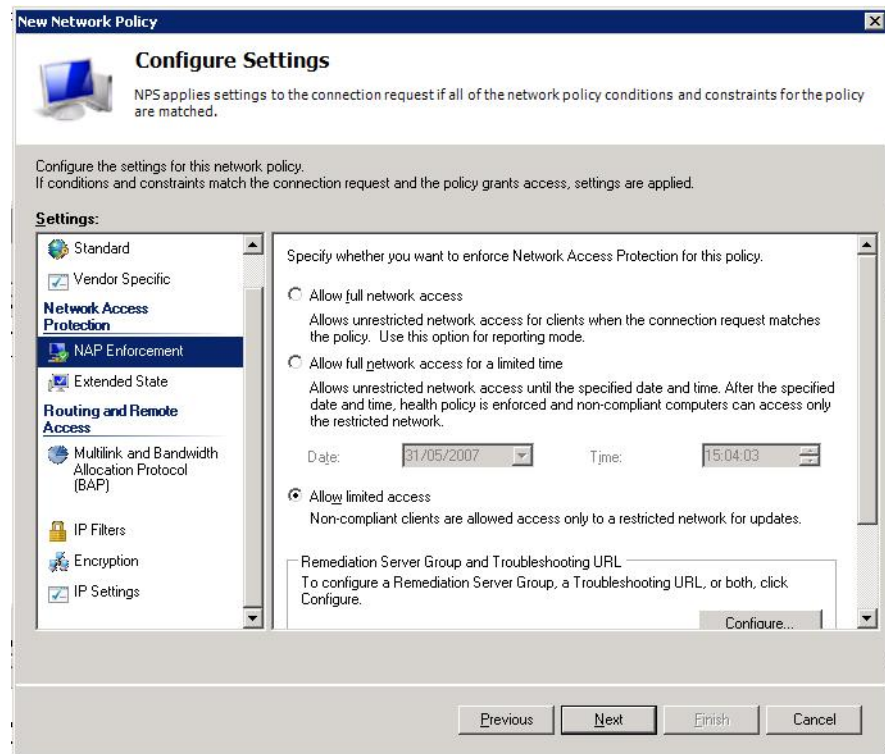


Access granted does not mean that noncompliant clients are granted full network access. It means that clients matching these conditions should continue to be evaluated by the policy.

- 8 Click *Next* on each of the next three screens.
- 9 In the Configure Settings window, click *NAP Enforcement*. Choose *Allow limited access* and select *Enable auto-remediation of client computers*.



The configuration of any locations of remediation servers is also done here. Configure these now if you have any.

Figure 67 New Network Policy Dialog Box — Configure Settings

b) 3Com Network Access Manager Specific Configuration

- 10 Under *RADIUS Attributes*, click *Vendor Specific*, and then click *Add*.
- 11 Select *Vendor-Specific* from the *Attributes list box*, and then click *Add*.
- 12 Click *Add*, then select *3Com* from the *Select from list* combo box.
- 13 Select *Yes. It conforms* and then click *Configure Attributes*.
- 14 Enter *9* in the *Vendor-assigned attribute number* text box, then select *Decimal* from the *Attribute format* and enter the *Authorization Type* corresponding for the switch device (eg. 1 for the Switch 5500) in the *Attribute value* text box. (See [Table 3](#) on [page 20](#) for a list of supported devices.) Click *OK* and *OK* again.

This tells the 3Com Network Access Manager IAS plug-in that it should process this access request and controls the format of the 3Com Network Access Manager authorization response (VLAN and Policy).

- 15 Click *Add*, then select *3Com* from the *Select from list* combo box.

- 16 Select *Yes. It conforms* and then click *Configure Attributes*.
- 17 Enter **10** in the *Vendor-assigned attribute number* text box, then select *String* from the *Attribute format* and enter the NAM rule you want applied for non-compliance exactly as it appears in NAM into the *Attribute value* text box. Click *OK* and *OK* again.

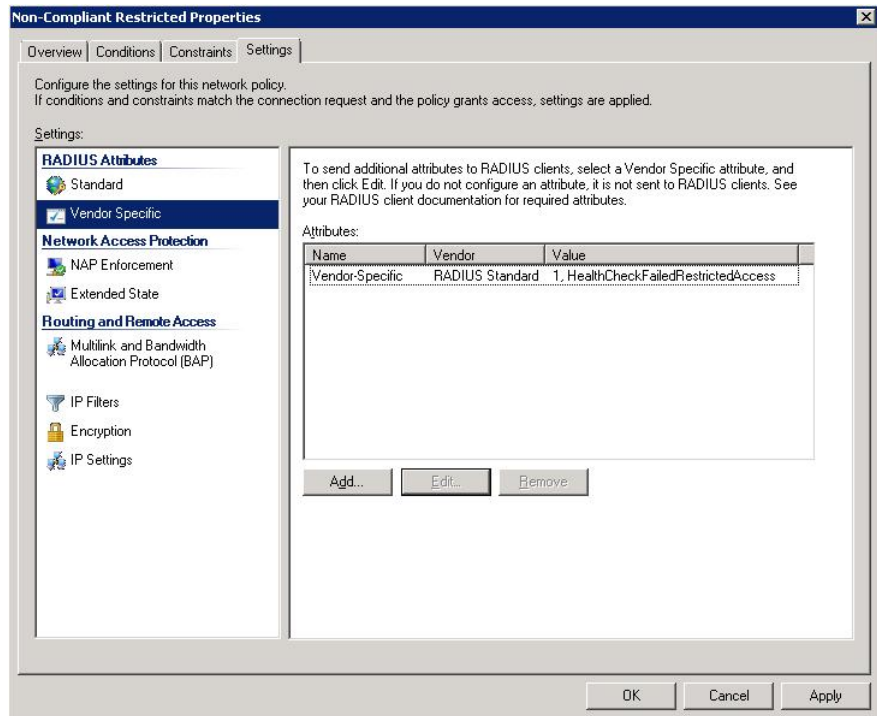
This tells the 3Com Network Access Manager IAS plugin that it should add the supplied rule to the user that is currently requesting access to the network. This will ultimately affect their VLAN/Policy that is deployed to the port.



The NAM Rule supplied for non-compliant devices should normally have a higher priority than the rules assigned to the user so that it will override the users rule.

- 18 Click *OK* then *Close* to complete the Vendor specific attributes configuration.

Figure 68 Non Compliant Restricted Properties Dialog Box



- 19 In the *Configure Settings* window, click *Next*.

- 20 Click *Finish* to complete configuration of your noncompliant network policy.

c) Configure a Network Policy for Compliant Client Computers

Next, create a network policy to match network access requests made by compliant client computers.

- 1 Right-click *Network Policies*, and then select *New*.
- 2 In the Specify Network Policy Name and Connection Type window, under *Policy name*, type **Compliant Full Access**, and then click *Next*.

Figure 69 New Network Policy Dialog Box — Specify Network Policy Name and Connection Type

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
Compliant Full Access

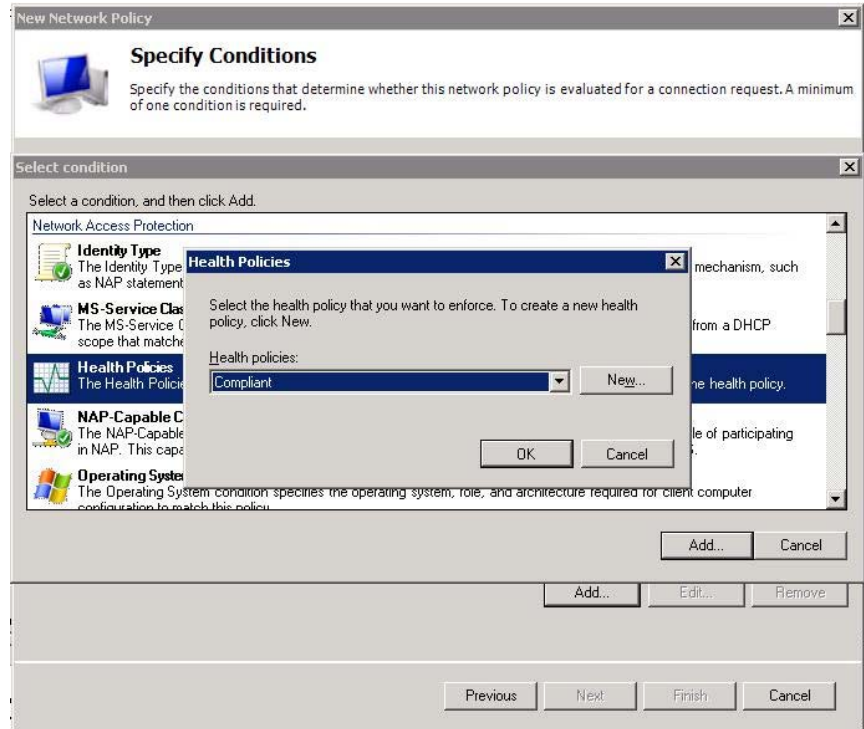
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required.

Type of network access server:
Unspecified

Vendor specific:
10

Previous Next Finish Cancel

- 3 In the Specify Conditions window, click *Add*.
- 4 In the Select Condition dialog box, double-click *Health Policies*.
- 5 In the Health Policies dialog box, under *Health policies*, select *Compliant*, and then click *OK*.

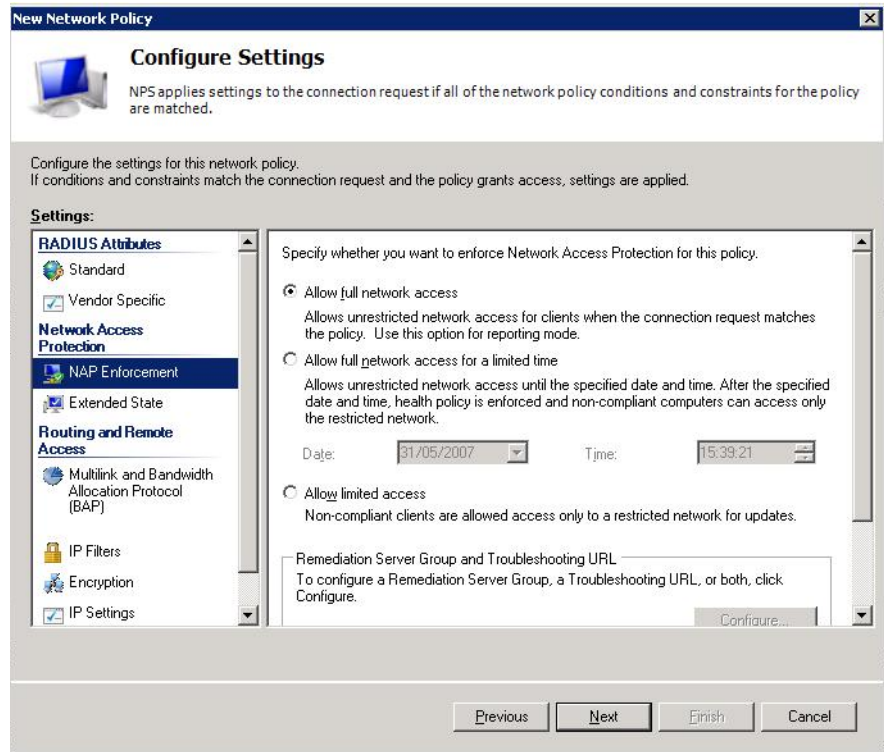
Figure 70 New Network Policy Dialog Box — Specify Conditions

- 6 In the Specify Conditions window, verify that *Health Policy* is specified under *Conditions* with a value of *Compliant*, and then click *Next*.
- 7 In the Specify Access Permission window, verify that *Access granted* is selected.



Access granted does not mean that noncompliant clients are granted full network access. It means that clients matching these conditions should continue to be evaluated by the policy.

- 8 Click *Next* on each of the next three screens.
- 9 In the Configure Settings window, click *NAP Enforcement*. Choose *Allow full network access*.

Figure 71 New Network Policy Dialog Box — Configure Settings

d) 3Com Network Access Manager Specific Configuration

- 10 Under *RADIUS Attributes*, click *Vendor Specific*, and then click *Add*.
- 11 Select *Vendor-Specific* from the *Attributes* list box, and then click *Add*.
- 12 Click *Add*, then select *3Com* from the *Select from list* combo box.
- 13 Select *Yes. It conforms* and then click *Configure Attributes*.
- 14 Enter *9* in the *Vendor-assigned attribute number* text box, then select *Decimal* from the *Attribute format* and enter *1* in the *Attribute value* text box. Click *OK* and *OK* again.

This tells the 3Com Network Access Manager IAS plug-in that it should process this access request.



Steps 15-17 are optional if the administrator wishes to include another NAM Rule to the NAM rules assigned to the user/computer from which the highest priority rule is selected to determine the authorization response.

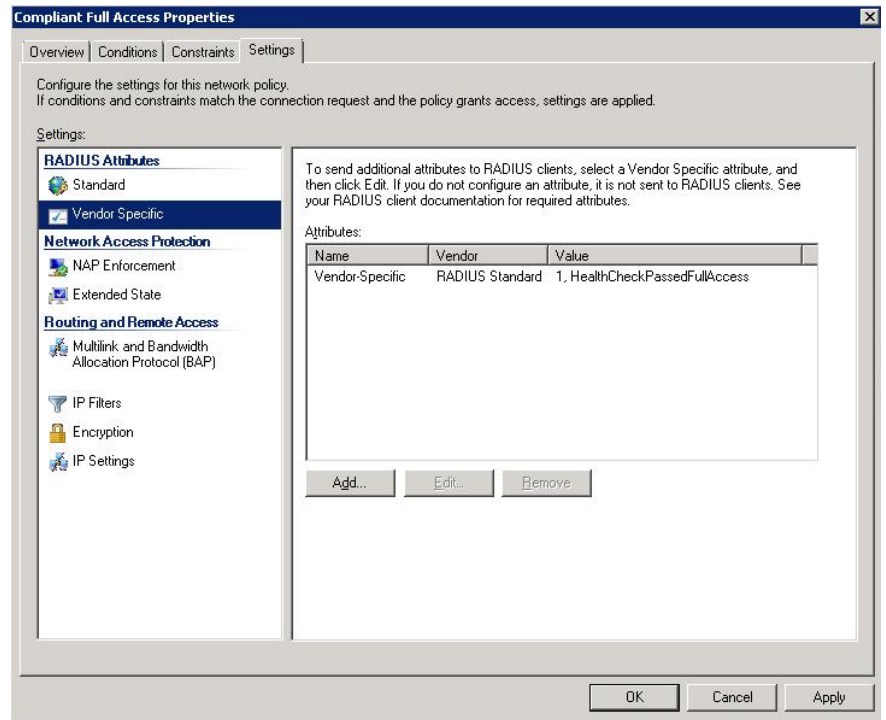
- 15 Click *Add*, then select *3Com* from the *Select from list* combo box.
- 16 Select *Yes. It conforms* and then click *Configure Attributes*.
- 17 Enter **10** in the *Vendor-assigned attribute number* text box, then select *String* from the *Attribute format* and enter the 3Com Network Access Manager rule you want applied for compliance exactly as it appears in 3Com Network Access Manager into the *Attribute value* text box. Click *OK* and *OK* again.

This tells the 3Com Network Access Manager IAS plugin that it should add the supplied rule to the user that is currently requesting access to the network. This will ultimately affect their VLAN/Policy that is deployed to the port.



The NAM Rule supplied for compliant devices should normally have a lower priority than the rules assigned to the user so that any rule assigned to the user will have precedence over the compliant device rule.

- 18 Click *OK* then *Close* to complete the Vendor specific attributes configuration.

Figure 72 Compliant Full Access Properties Dialog Box

- 19 In the Configure Settings window, click *Next*.
- 20 Click *Finish* to complete configuration of your compliant network policy.

Configuring NPS for Network Access with a 3Com Network Access Manager Response

This section describes how to configure a Network Policy Server (NPS) for Network Access with a 3Com Network Access Manager response.

This guide assumes that you are using Active Directory for your 'Users and Computers' management and that it is already installed and the server is the Domain Controller.



Windows Server 2008 contains a new feature called User Account Control (UAC) that requires the user to approve certain actions in the system. Several of the configuration tasks to follow require UAC approval. When prompted you should click Continue to authorize these changes.

NPS Configuration Follow these steps to create a new Network Access Policy in NPS that will receive and process the authentication request and also pass it onto 3Com Network Access Manager for further processing.

Install the NPS Server Role

- 1 Click *Start > Server Manager*.
- 2 Under *Roles Summary*, click *Add roles*, and then click *Next*.
- 3 Select the Network Policy and Access Services check box, and then click *Next* twice.
- 4 Select the Network Policy Server check box, click *Next*, and then click *Install*.
- 5 Verify the installation was successful, and then click *Close* to close the Add Roles Wizard dialog box.
- 6 Close the Server Manager window.

Configure the NPS for Network Access

- 1 Click *Start > Administrative Tools > Network Policy Server*.
- 2 Double-click *RADIUS Clients and Servers*.
- 3 Right-click *RADIUS Clients*, and then click *New RADIUS Client*.
- 4 In the New RADIUS Client dialog box, under *Friendly name*, type **802.1X switch**. Under *Address (IP or DNS)*, type **<your switch ip>**, under *Vendor name* select *3Com*.
- 5 Under *Shared secret*, type **<secret password>**.
- 6 Under *Confirm shared secret*, re-type **<secret password>**.
- 7 Select the *Request must contain the Message Authenticator attribute* check box, and then click *OK*.
- 8 In the left pane, click *RADIUS Clients*. Your new RADIUS client should be displayed in the middle pane.
- 9 Double-click the new RADIUS client to display the New RADIUS Client dialog box as shown in [Figure 73](#).
- 10 Tick the *Enable this RADIUS client* check box.
- 11 Ensure the *RADIUS client is NAP-capable* check box is cleared.

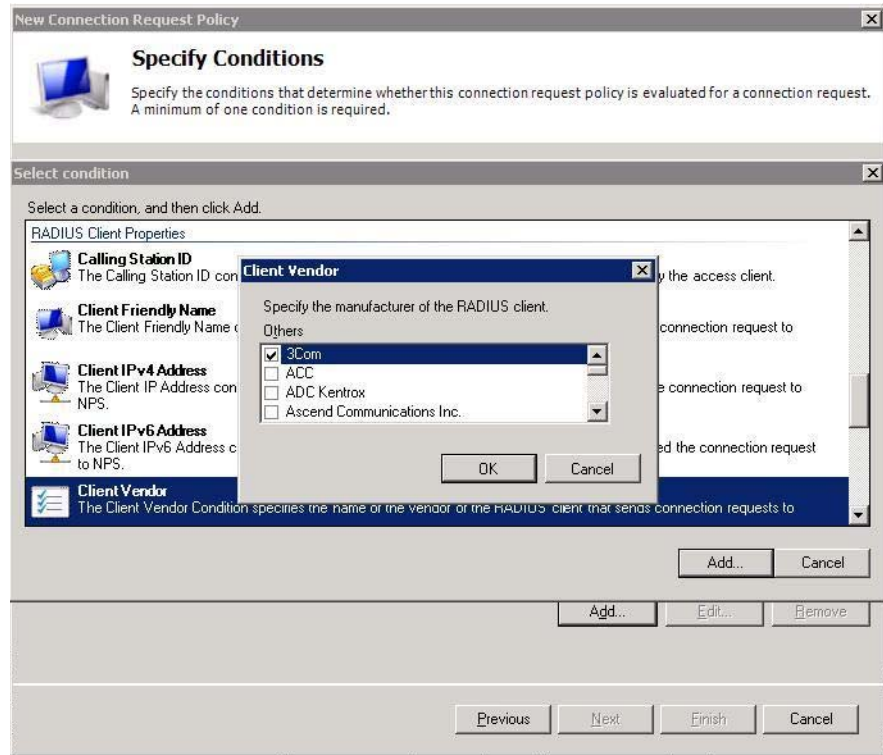
Figure 73 New RADIUS Client Dialog Box



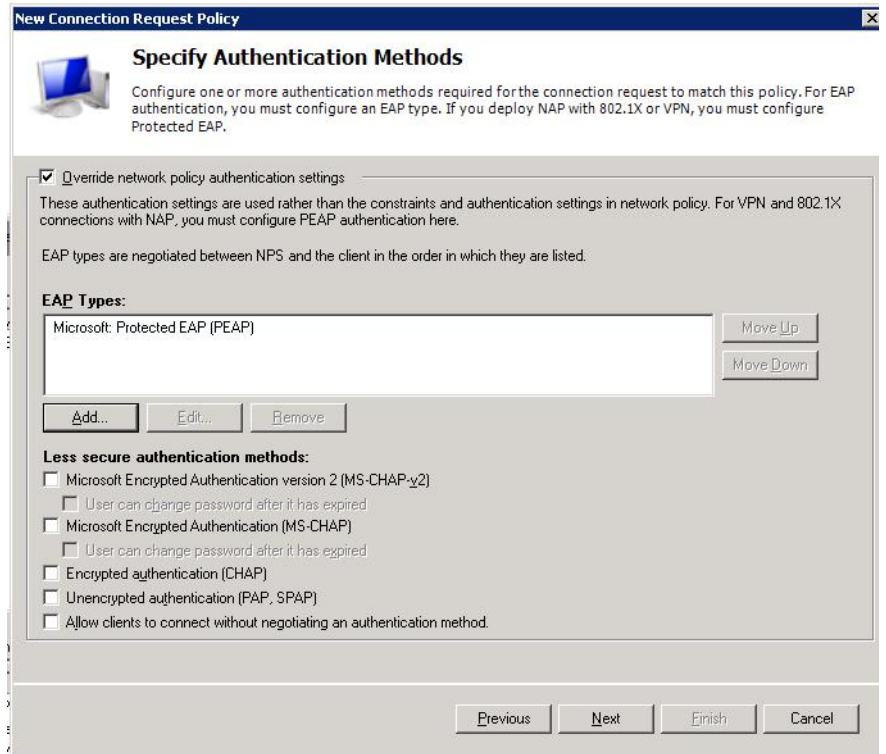
The RADIUS shared secret entered here must be identical to the one entered on your switch.

Configure Connection Request Policy

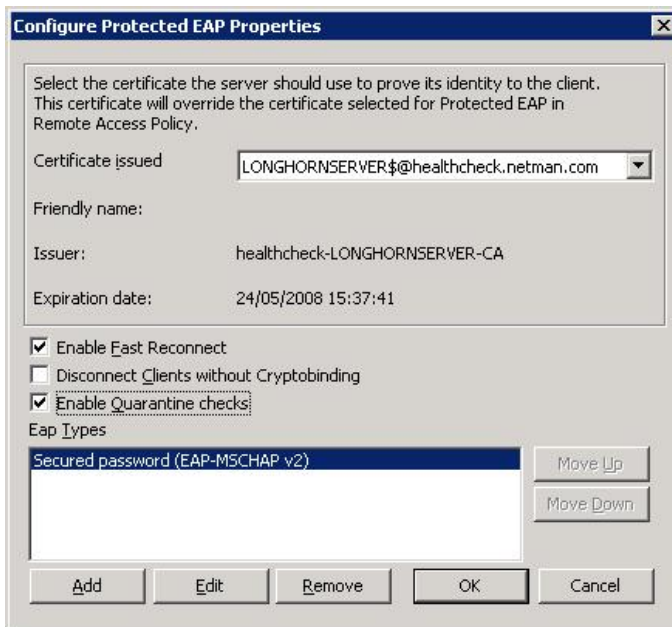
- 1 Double-click on *Policies*, and then select *Connection Request Policies*.
- 2 Disable the default *Connection Request Policy* found under the *Policy Name* area: right-click the policy, and then click *Disable*.
- 3 Right-click on *Connection Request Policies*, and then select *New*.
- 4 In the Specify Connection Request Policy Name and Connection Type window, under *Policy name*, type **NAM PEAP Policy**.
- 5 Click *Next*, and then click *Add*.
- 6 Double-click *Client-Vendor*, select *3Com* from the list, and then click *OK*.

Figure 74 New Connection Request Policy Dialog Box — Specify Conditions

- 7 Click *Next*, verify that *Authenticate requests on this server* is selected, and then click *Next*.
- 8 In the Specify Authentication Methods window, select *Override network policy authentication settings*, and then click *Add*.
- 9 In the Add EAP dialog box, under *Authentication methods*, select *Microsoft: Protected EAP (PEAP)*, and then click *OK*. Select any other modes that are used on the network.

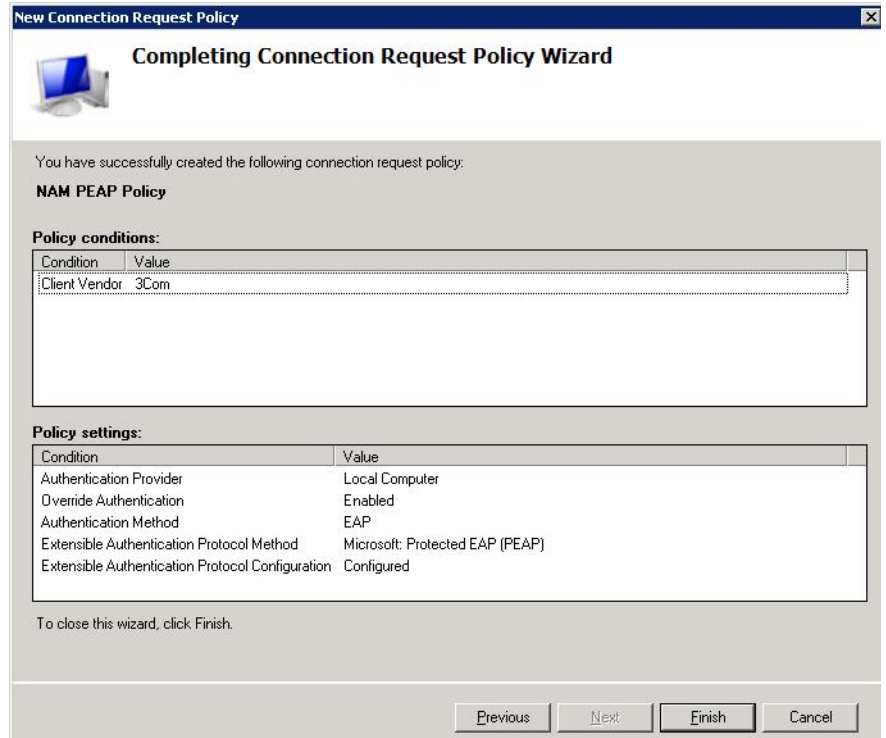
Figure 75 New Connection Request Policy Dialog Box — Specify Authentication Methods

10 Click *Edit*, and verify that your domain appears next to *Certificate issued*.

Figure 76 Configure Protected EAP Properties

- 11 Click *OK*. Then Click *Next* twice, and then click *Finish*. This completes the configuration of your PEAP connection request policy.

Figure 77 New Connection Request Policy Dialog Box — Completing Connection Request Policy Wizard



Configure Network Policies

Network policies allow you to configure who is authorized to access the network and the circumstances in which they can and cannot connect to the network. It allows you to specify which VLAN etc. the client should be placed on depending on the circumstances.

a) Configure a Network Access Policy

Firstly, create a network policy to match network access requests made by the users.

- 1 Right-click *Network Policies*, and then select *New*.
- 2 In the Specify Network Policy Name and Connection Type window, under *Policy name*, type **NAM Policy**, and then click *Next*.

Figure 78 New Network Policy Dialog Box — Specify Network Policy Name and Connection Type

New Network Policy

Specify Network Policy Name and Connection Type
You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
NAM Policy

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required.

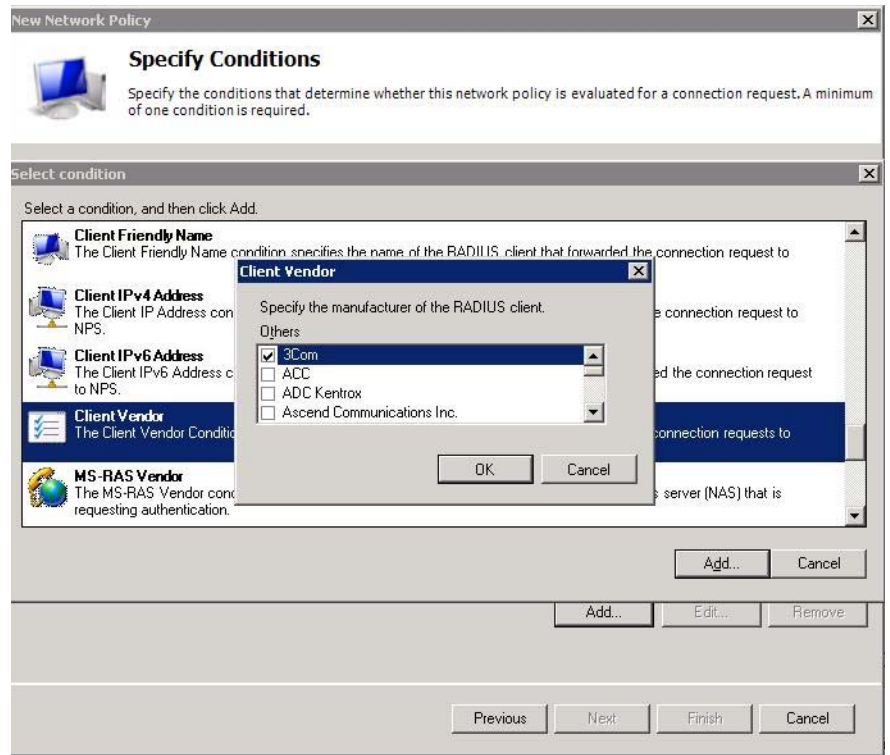
Type of network access server:
Unspecified

Vendor specific:
10

Previous Next Finish Cancel

- 3 In the Specify Conditions window, click *Add*.
- 4 In the Select Condition dialog box, double-click *Client-Vendor*.
- 5 Select *3Com* from the list and then click *OK* and then click *Next*.

Figure 79 New Network Policy Dialog Box — Specify Conditions



- 6 In the Specify Access Permission window, verify that *Access granted* is selected.



Access granted means that clients matching these conditions should continue to be evaluated by the policy.

- 7 Click *Next* for the next three screens.

b) 3Com Network Access Manager Specific Configuration

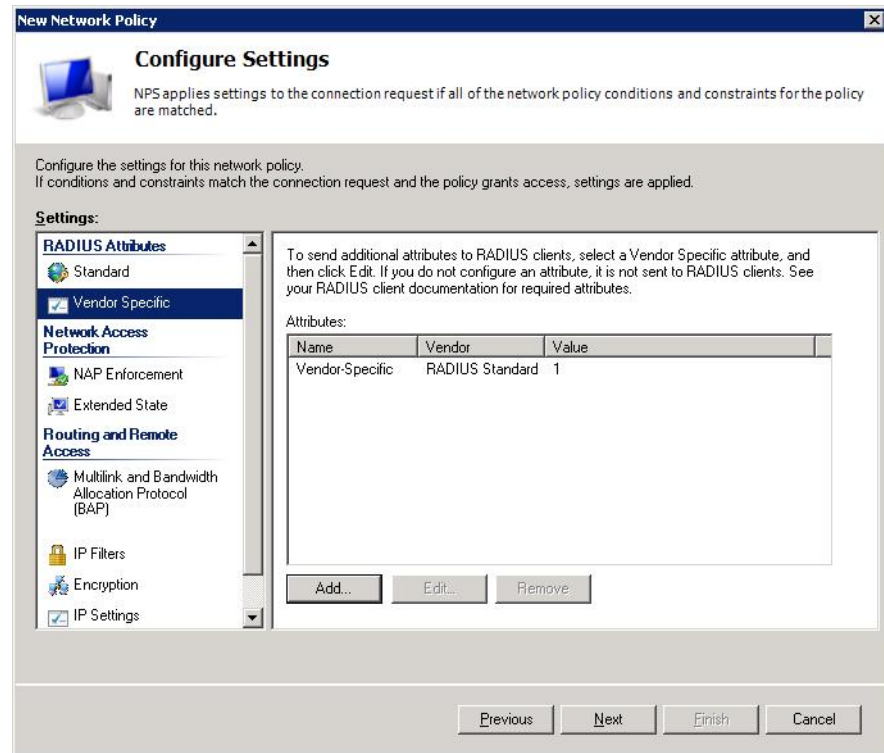
- 1 Under *RADIUS Attributes*, click *Vendor Specific*, and then click *Add*.
- 2 Select *Vendor-Specific* from the *Attributes* list box, and then click *Add*.
- 3 Click *Add*, then select *3Com* from the *Select from list* combo box.
- 4 Select *Yes. It conforms* and then click *Configure Attributes*.
- 5 Enter *9* in the *Vendor-assigned attribute number* text box, then select *Decimal* from the *Attribute format* and enter the "Authorization Type" corresponding to the switch device (for example, 1 for the Switch 5500)

in the *Attribute value* text box. (See [Table 3](#) on [page 20](#) for a list of supported devices.) Click *OK* and *OK* again.

This tells the 3Com Network Access Manager IAS plug-in that it should process this access request and controls the format of the 3Com Network Access Manager authorization response (VLAN and Policy).

- 6 Click *OK* then *Close* to complete the Vendor specific attributes configuration.

Figure 80 New Network Policy Dialog Box — Configure Settings



- 7 In the Configure Settings window, click *Next*.
- 8 Click *Finish* to complete configuration of your NPS for Network Access with a 3Com Network Access Manager response policy.

Case Study — Microsoft NAP Health Checking with 3Com Network Access Manager Response

This section explains how to setup 3Com Network Access Manager to deploy different VLANs depending on whether a Microsoft NAP client is compliant or non-compliant with the health check required. This section assumes that you have already completed the steps specified in [“Configuring NPS for Health Checking with a 3Com Network Access Manager Response”](#).

Network Administrator Tasks

The following provides an overview of the tasks for a network administrator responsible for the domain and security on the network.

- 1 Ensure edge port security is set to IEEE 802.1X on edge ports in the domain.



Edge ports are called 'access ports' on the Switch 5500.

Using 3Com Network Access Manager:

- 2 Select the Default Rule and ensure that the Network Access is set to Deny, see [“Changing NAM Rule Properties”](#) in [Chapter 3](#).
- 3 Create an full access Users rule (for successful health checks) which will allow network access, see [“Creating A New NAM Rule”](#) in [Chapter 3](#). This needs to be given the same name that is in the Vendor Specific attribute when configuring the NPS network policy for compliant clients.
 - a Set security permissions for the rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.
 - b Set the Actions for the rule: select the rule priority, and set Network Access to Allow and select the appropriate VLAN, and Policy for the normal access rule.
- 4 Create an restricted access Users rule (for unsuccessful health checks) which will allow network access but on a restricted VLAN or Network Policy, see [“Creating A New NAM Rule”](#) in [Chapter 3](#). This needs to be given the same name that is in the Vendor Specific attribute when configuring the NPS network policy for non-compliant clients from section
 - a Set security permissions for the rule. Grant READ and WRITE access to the users/groups permitted to apply the rule, grant READ access to all Network Administrators in the domain to ensure they can see that the rule exists even if they are not permitted to apply the rule.

- b** Set the Actions for the rule: select the rule priority, and set Network Access to Allow and select the appropriate VLAN, and Policy for the restricted access rule.

C

FORMAT OF 3COM NETWORK ACCESS MANAGER RADIUS VENDOR SPECIFIC ATTRIBUTES

The 3COM Network Access Manager IAS Plug-in recognises the following 3Com RADIUS Vendor Specific Attributes (VSA). These are used to control how the plug-in behaves when an access request is received. These VSAs are normally configured in the IAS Remote Access Policies that correspond to the access requests to be processed by the plug-in.

These VSAs are based upon the recommendations contained in IETF RFC-2865 "Remote Authentication Dial In User Service (RADIUS)" and contains the Vendor-Id for 3Com followed by a vendor type field, vendor length field and attribute specific field.

3Com Authorization Type VSA

This attribute indicates if an access request is to be processed by the plug-in and also indicates how the authorization response is to be formatted.

The 3Com type field must contain the number 9.

The attribute data field must be formatted as a 4 octet number that contains the authorization type. This must match with an authorization type configured in the plug-in configuration file (see [Chapter 6 "Customizing 3Com Network Access Manager"](#)).

If an access request is received by the plug-in which does not contain this VSA or the authorization type is not found in the plug-in configuration file then the access request will not be modified by the plug-in.

3Com Authorization Rule Name VSA

This optional attribute allows a named NAM Rule to be supplied which is combined with the rules assigned to the user and computer identified in the access request when determining the highest priority rule. The plug-in will use this rule to authorize the access request if it has a higher priority than the rules assigned to the user or the computer.

The 3Com type field must contain the number 10.

The attribute data must contain a string containing the name of a NAM rule.

If the named rule is not found then the plug-in will use the highest priority rule assigned to the user or the computer or it will use the Default Rule if no rules are assigned to the user and computer.

Details of the authorization response for the authorization types 1,2 and 3 are:

Auth Type = 1 (3Com Extended Usage)

VLAN Assignment :

Tunnel-Type = 13 (VLAN)
 Tunnel-Medium-Type = 6 (IEEE-802)
 Tunnel-Private-Group-ID = <The VLAN ID from the NAM VLAN>

Policy Assignment

Filter-Id = profile=<The Policy ID from the NAM Policy>

Auth Type = 2 (IETF 3580 Usage)

VLAN Assignment :

Tunnel-Type = 13 (VLAN)
 Tunnel-Medium-Type = 6 (IEEE-802)
 Tunnel-Private-Group-ID = <The VLAN ID assigned to the NAM VLAN>

Policy Assignment

Filter-Id = <The Policy ID from the NAM Policy>

Auth Type = 3 (3Com WX Wireless switch Usage)

VLAN Assignment :

3Com-Wireless-VLAN-Selector = <The name of the NAM VLAN>

Policy Assignment

Filter-Id = profile=<The Policy ID from the NAM Policy>

The only difference between authorization type 1 and 2 is the "profile=" prefix for the Filter-Id attribute.

Authorization type 3 uses a 3Com Vendor Specific Attribute (VSA) containing the name of the VLAN in place of the standard RADIUS tunnel attributes.



Auth Type 1 matches the behavior of 3Com Network Access Manager prior to version 1.2.

D

CONFIGURING USE OF THE MAC ADDRESS TOOL

This appendix provides information to assist administrators with configuring use of the MAC Address Tool (for more general information about the tool, see [“Using the MAC Address Tool”](#) on [page 75](#)). This section covers configuring the MAC Addresses for the computers in Active Directory by retrieving the MAC Addresses from the actual computers.



The MAC Address Tool uses the Microsoft Windows Management Interface (WMI) to retrieve the MAC Addresses associated with the network adapters installed on a computer. This technology makes use of the Microsoft Distributed Component Object Model (DCOM) services.

To successfully retrieve the MAC addresses from another computer the following conditions must apply:

- The computer must be turned on and connected to the network.
- The computer must be running the Microsoft Windows 2000 or later operating system.
- If the Windows Firewall is enabled on the computer then it must be configured to allow inbound WMI connections to pass through the firewall.
- The WMI service must be enabled.
- The user using the MAC Address Tool must use an account that has sufficient privileges to access WMI on the computer. Typically this will be an account that is a member of the Administrators group on the computer. Starting with Windows Vista the account must also be a domain account.



It is possible to restrict remote access to WMI by modifying the DCOM access permission settings and the WMI security settings.



To update the MAC Addresses for a computer in Active Directory the user must also have sufficient privileges to update the computers' account.

Configuring the Windows Firewall to Allow Access by the MAC Address Tool



The default Windows Firewall configuration will not allow access for the MAC Address Tool.

The Windows Firewall can be configured to allow access by one of the following methods:

- 1 Configure the Group Policy settings for the domain or the organizational unit containing the computer, this allows multiple computers to be configured centrally.
- 2 Configure the Local Computer Policy for the individual computer.
- 3 Directly configure the Windows Firewall.

The specific details of these methods are dependent upon the operating system version.



When configuring the Firewall to allow access by the MAC Address Tool it is recommended that the Firewall exception includes an IP address filter to limit the network scope from which the access is allowed. For example, the IP filter could be set to the IP address of the administrators computer.

Using Windows Vista or Windows Server 2008 or Later

Starting with Windows Vista the following methods may be used to enable remote access to the MAC Address information.

- 1 Configure the Firewall exception via Group Policy settings

The following will configure the Firewall remote administration exception on all computers associated with a group policy when the computer is next restarted.

- a Install the Group Policy Management feature if it is not already installed.

The following command may be entered at the command line to configure the Firewall WMI exception on a specific computer. This command does not support remote configuration:

```
netsh advfirewall firewall set rule group="Windows Management
Instrumentation (WMI)" new enable=yes
```

Using Windows XP SP2 or Windows Server 2003 SP1

This section is applicable if you are using Windows XP SP2 or Windows Server 2003 SP1.

1 Configure the Firewall exception via Group Policy

The following will configure the firewall remote administration exception on all computers associated with the selected group policy when the computer is next restarted.

- a Start the Active Directory Users and Computers MMC tool.
- b Select the domain or organizational unit object containing the computer.
- c Select the *Properties* option from the *Action* menu, this will display the Properties dialog. Click on the *Group Policy* tab.
- d Click the appropriate group policy object and then click on the *Edit* button, this will launch the *Group Policy Editor*.
- e Double-click the *Computer Configuration* then *Administrative Templates, Network, Network Connections, Windows Firewall* and *Domain Profile*.
- f Double-click on the *Windows Firewall: Allow remote administration exception* then click on *Enabled* and then click on the *OK* button.

2 Configure the Firewall exception via Local Computer Policy

The following will configure the Firewall Remote Administration exception on a specific computer.

- a Start the MMC tool and add the Group Policy Editor and connect to the computer.
- b Double-click on the *Local Computer Policy* and then double-click on the *Computer Configuration* then *Administrative Templates, Network, Network Connections* and then *Windows Firewall*.
- c Then double-click *Domain Profile* if the computer is a member of a domain, otherwise double click *Standard Profile*.

- d Double-click the *Windows Firewall:Allow remote administration exception* then click on *Enabled* and then click on the *OK* button.
- 3 Configuring the Firewall exception via the command line
- The following command may be entered at the command line to configure the Firewall Remote Administration exception on a specific computer. This command does not support remote configuration.

```
netsh firewall set service RemoteAdmin enable
```

Configuring Security Settings for the MAC Address Tool

To use the MAC Address Tool to retrieve the MAC Addresses for a remote computer it is normally sufficient to use an account that is a member of the Administrator group on the computer being accessed. Starting with Vista the account must also be a domain account.

To configure remote access for another user or group do the following:

- 1 Logon to the computer (this can not be configured remotely).
- 2 Click *Start*, click *Run*, then enter **DCOMCNFG**, and then click *OK*.
- 3 In the Component Services window, double-click on *Component Services*, then double-click *Computers*, and then click on *My Computer*.
- 4 Select the *Properties* option on the *Action* menu; this will display the *My Computer Properties* dialog.
- 5 Click on the *COM Security* tab.
- 6 Under *Launch and Activation Permissions*, click the *Edit Limits* button. In the *Launch Permission* dialog add the user or group and enable the *Remote Launch* and *Remote Activation* permissions, and then click *OK*.

To enable remote access to WMI for a user do the following:

- 1 Start the WMI Control MMC Tool and connect to the remote computer.
- 2 Click on the *WMI Control* and select the *Properties* option from the *Action* menu; this will launch the WMI Control Properties dialog.
- 3 In the *Security* tab, select the *Root* namespace and click *Security*.
- 4 Add the user or group. Click on the *Advanced* button and edit the permissions entry for the user or group, select the *Remote Enable* check box in the *Permissions* list and change the *Apply onto* setting to *This namespace and subnamespaces*. Then click *OK*.

E

OBTAINING SUPPORT FOR YOUR 3COM PRODUCTS

3Com offers product registration, case management, and repair services through eSupport.3com.com. You must have a user name and password to access these services, which are described in this appendix.

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at:

<http://eSupport.3com.com/>

3Com eSupport services are based on accounts that are created or that you are authorized to access.

Solve Problems Online

3Com offers the following support tool:

- **3Com Knowledgebase** — Helps you to troubleshoot 3Com products. This query-based interactive tool is located at:

<http://knowledgebase.3com.com>

It contains thousands of technical solutions written by 3Com support engineers.

Purchase Extended Warranty and Professional Services

To enhance response times or extend your warranty benefits, you can purchase value-added services such as 24x7 telephone technical support, software upgrades, onsite assistance, or advanced hardware replacement.

Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. For more information on 3Com Extended Warranty and Professional Services, see:

<http://www.3com.com/>

Contact your authorized 3Com reseller or 3Com for additional product and support information. See the table of access numbers later in this appendix.

Access Software Downloads

You are entitled to *bug fix / maintenance releases* for the version of software that you initially purchased with your 3Com product. To obtain access to this software, you need to register your product and then use the Serial Number as your login. Restricted Software is available at:

<http://eSupport.3com.com/>

To obtain software releases that *follow* the software version that you originally purchased, 3Com recommends that you buy an Express or Guardian contract, a Software Upgrades contract, or an equivalent support contract from 3Com or your reseller. Support contracts that include software upgrades cover feature enhancements, incremental functionality, and bug fixes, but they do not include software that is released by 3Com as a separately ordered product. Separately orderable software releases and licenses are listed in the 3Com Price List and are available for purchase from your 3Com reseller.

Contact Us

3Com offers telephone, Internet, and e-mail access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL, or e-mail address from the table in the next section.

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

<http://eSupport.3com.com/>

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at <http://eSupport.3com.com/>. First-time users must apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:

<http://csoweb4.3com.com/contactus/>

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim — Telephone Technical Support and Repair			
Australia	1800 075 316	Philippines	1800 144 10220 or 029003078
Hong Kong	2907 0456	PR of China	800 810 0504
India	000 800 440 1193	Singapore	800 616 1463
Indonesia	001 803 852 9825	South. Korea	080 698 0880
Japan	03 3507 5984	Taiwan	00801 444 318
Malaysia	1800 812 612	Thailand	001 800 441 2152
New Zealand	0800 450 454		

Country	Telephone Number	Country	Telephone Number
Pakistan	Call the U.S. direct by dialing 00 800 01001, then dialing 800 763 6780		
Sri Lanka	Call the U.S. direct by dialing 02 430 430, then dialing 800 763 6780		
Vietnam	Call the U.S. direct by dialing 1 201 0288, then dialing 800 763 6780		

You can also obtain non-urgent support in this region at this email address ap_r technical_support@3com.com
 Or request a return material authorization number (RMA) by FAX using this number: +61 2 9937 5048, or send an email at this email address: ap_rma_request@3com.com

Europe, Middle East, and Africa — Telephone Technical Support and Repair

From anywhere in these regions not listed below, call: +44 1442 435529

From the following countries, call the appropriate number:

Austria	0800 297 468	Luxembourg	800 23625
Belgium	0800 71429	Netherlands	0800 0227788
Denmark	800 17309	Norway	800 11376
Finland	0800 113153	Poland	00800 4411 357
France	0800 917959	Portugal	800 831416
Germany	0800 182 1502	South Africa	0800 995 014
Hungary	06800 12813	Spain	900 938 919
Ireland	1 800 553 117	Sweden	020 795 482
Israel	180 945 3794	Switzerland	0800 553 072
Italy	800 879489	U.K.	0800 096 3266

You can also obtain support in this region using this URL: <http://emea.3com.com/support/email.html>

You can also obtain non-urgent support in this region at these email addresses:

Technical support and general requests: customer_support@3com.com

Return material authorization: warranty_repair@3com.com

Contract requests: emea_contract@3com.com

Latin America — Telephone Technical Support and Repair

Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

You can also obtain support in this region in the following ways:

- Spanish speakers, enter the URL: <http://lat.3com.com/lat/support/form.html>
- Portuguese speakers, enter the URL: <http://lat.3com.com/br/support/form.html>
- English speakers in Latin America, send e-mail to: lat_support_anc@3com.com

Country	Telephone Number	Country	Telephone Number
US and Canada — Telephone Technical Support and Repair			
All locations:	Network Jacks; Wired or Wireless Network Interface Cards:		1 800 876 3266
	All other 3Com products:		1 800 876 3266

INDEX

Numbers

- 3Com Enterprise Management Suite 25
- 3Com Knowledgebase tool 185
- 3Com Network Access Manager
 - authorization log 109
 - before setting up 47
 - changing installation 37
 - devices supported 20
 - edge port security modes 21
 - installation 26
 - interfaces 13
 - network administrator responsibilities 13
 - network operator responsibilities 14
 - online help 85
 - repairing installation 37
 - uninstalling 39
 - users 13
- 3Com Network Director 25
- 3Com Professional Services 186
- 3Com resources, directory 187
- 3Com switches
 - configuration 25
 - edge port security 25
- 3Com wireless access points
 - configuration 25

A

- activate NAM 42
- Active Directory
 - schema configuration 26
 - what is 16
- Active Directory Server
 - component installation 26
- authentication
 - IEEE 802.1X 19
 - MAC-address based 19

authorization 20

B

- backing up data 16
- blocking PC network access 94
- bug fixes 186
- button
 - NAM rule priority 58
 - new EFW policy 55
 - new NAM Policy 51
 - new NAM rule 57
 - new NAM VLAN 48
 - recalculate EFW membership 15, 62, 63, 70

C

- computer
 - associating rules 72
 - changing the associated rules 74
 - changing the MAC address 74
 - entering mac address 71
 - view 70
- Connection Assistant 185
- conventions
 - notice icons 10
 - text 10

D

- directory of 3Com resources 187

E

- edge port security modes 21
- EFW policy
 - changes that affect 15
 - creating 54
 - deleting 55
 - displaying associated rules 56
 - NIC based 15
 - renaming 56
 - server support 15
 - task sequence 15

- user-based 15
- view 53
- e-mail support 186
- End User License Agreement 29, 35
- engineering services 186
- error message 27, 33, 112
- Event Viewer 109
- Express services contract 186
- extended warranty options 186

F

- Find 83

G

- group
 - associating rules 68
 - changing associated rules 69
 - view 68
- Guardian services contract 186

H

- hot desking 96
 - network access 96
 - with host filtering 101

I

- IAS Remote Access Policy 25
- installation
 - checks 27
 - components 27
- Internet Authentication Service
 - component installation 26
 - remote access policy 17, 25, 125, 145
 - what is IAS 16
- internet support 186
- isolating
 - infected PCs 99

K

- Knowledgebase 185

L

- license keys 186

M

- MAC Address tab 72
- maintenance releases 186

N

- NAM Policies
 - view 50
- NAM Policy
 - changing ID 52
 - creating 51
 - deleting 52
 - displaying associated rules 53
 - renaming 52
- NAM Rule
 - changing members 63
 - changing priorities 62
 - changing properties 63
 - controlling permissions to apply 62
 - creating 57
 - Default Rule 18
 - deleting 61
 - displaying members 63
 - highest priority 18
 - network access setting 18
 - priority 18
 - view 56
 - what is 17
- NAM VLANs
 - changing ID 49
 - creating 48
 - deleting 49
 - displaying associated rules 50
 - renaming 49
 - view 47
- network access
 - block specific PC 94
 - control user access 88
 - restrict to known computers 91
- network administrator
 - user interface 45
- network operator
 - permissions 75
 - user interface 78

O

obtaining technical support 186
 online help 85
 online problem solving 185
 Organizational Units 64, 89, 93, 95, 96, 98

P

problem solving
 related to network access 114
 related to set up 112
 related to using the MAC Address tool 118
 product registration 185, 186
 Professional Services from 3Com 186
 purchasing license keys 186
 purchasing software upgrades 186

R

RADIUS
 authorization 19
 server 16
 registering your product 185, 186, 187
 remote access policy
 creating 126
 Vendor Specific Attributes 141
 repair authorization number by FAX, Asia and Pacific Rim 188
 repair services 186
 repair support for Latin America 188
 repair support for US and Canada 189
 repair support, Europe, Middle East, and Africa 188
 resolving problems 111
 restoring data 16
 Restricted Software 186
 restricting network access 91
 return authorization number (RMA) 187
 RMA numbers 187

S

screen shots 9
 sending products to 3Com for repair 187
 service benefits 185, 187
 services, repair 186
 software upgrades contract 186
 solving problems
 related to network access 114
 related to set up 112

solving problems online 185
 support, e-mail 186
 support, internet 186
 support, technical 186
 system event log 109

T

table of 3Com support contact numbers 186
 technical support, Asia and Pacific Rim 187
 technical support, Europe, Middle East, and Africa 188
 telephone support 186
 telephone technical support 186
 telephone technical support for Latin America 188
 telephone technical support for US and Canada 189
 telephone technical support, Asia and Pacific Rim 187
 telephone technical support, Europe, Middle East, and Africa 188

U

uninstalling components 39
 user
 associating rules 65
 changing associated rules 67
 creating 67
 view 64
 using 83

V

Vendor Specific Attributes 141

W

warranty registration 185

3COM END USER SOFTWARE LICENSE AGREEMENT

IMPORTANT: READ BEFORE INSTALLING THE SOFTWARE

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION ("3COM") TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE "I AGREE" OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.

LICENSE: 3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the "Software") and accompanying documentation (the "Documentation"), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce one (1) copy of the Software and Documentation for backup or archive purposes, provided that such copy contains 3Com's and its licensors' proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

ASSIGNMENT; NO REVERSE ENGINEERING: You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union ("EU") resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

EXPORT: This product, Software and/or technical data (collectively "Product") may contain encryption. This Product is subject to U.S. and EU export control laws and regulations and may be subject to export or import regulations in other countries, including controls on encryption products. You agree that you will not export, reexport or transfer the Product (or any copies thereof) or any products utilizing the Product in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, reexport, transfer or import the Product.

In addition to the above, the Product may not be used by, or exported or reexported to (i) any U.S. or E.U. sanctioned or embargoed country, or to nationals or residents of such countries; or (ii) to any person, entity, organization or other party identified on the U.S. Department of Commerce's Table of Denial Orders or the U.S. Department of Treasury's lists of "Specially Designated Nationals and Blocked Persons," as published and revised from time to time; (iii) to any party engaged in nuclear, chemical/biological weapons or missile proliferation activities, unless authorized by U.S. and local (as required) law or regulations.

TRADE SECRETS; TITLE: You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

UNITED STATES GOVERNMENT LEGENDS: The Software and Documentation are iCommercial Items(s)i as defined in 48 C.F.R. B2.101, consisting of iCommercial Computer Softwarei and iCommercial Computer Software Documentationi, as such terms are used in 48 C.F.R. B 12.212 or 48 C.F.R. B227.7202, as applicable. Consistent with 48 C.F.R. B12.212 or 48 C.F.R. B227-7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Therefore, if you are licensing the Software and/or Documentation for acquisition by the U.S. Government or any contractor therefore, you will license consistent with the policies set forth in 48 C.F.R. B12.212 (for civilian agencies) and 48 C.F.R. B227-7202-1 and 227.7202-4 (for the Department of Defense), and their successors.

TERM AND TERMINATION: The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

LIMITED WARRANTIES AND LIMITATION OF LIABILITY: All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software. Such warranties and limitations of liability are incorporated herein in their entirety by this reference.

GOVERNING LAW: This Agreement shall be governed by the laws of the Commonwealth of Massachusetts, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

SEVERABILITY: In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

ENTIRE AGREEMENT: This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write: 3Com Corporation, Customer Support Information, 350 Campus Drive, Marlborough, MA 01752-3064 USA

3Com Corporation
350 Campus Drive,
Marlborough, MA 01752-3064 USA

Copyright © 2004-2007 3Com Corporation and its licensors. All rights reserved. 3Com is a registered trademark of 3Com Corporation.