

866 R3000 | Enterprise Filter

# GUIDE for Authentication





Model: R3000IR Release 2.0.00 / Version No.: 1.01

### **R3000 ENTERPRISE FILTER AUTHENTICATION USER GUIDE**

© 2007 8e6 Technologies All rights reserved. 828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published April 2007 To be used with R3000<sup>IR</sup> User Guide version 1.01 for software release 2.0.00

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

The latest version of this document can be obtained from http://www.8e6.com/docs/ir\_r3000\_auth2.pdf.

#### Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# IR-R3.2.0\_AUG\_v1.01-0704

# CONTENTS

About this User Guide	
low to Use this User Guide	
Conventions	
Terminology	
iltering Elements	
Group Types	
Global Group	
IP Groups	
NT Domain Groups	
LDAP Domain Groups	
Filtering Profile Types	
Static Filtering Profiles	
Master IP Group Filtering Profile	
IP Sub-Group Filtering Profile	
Individual IP Member Filtering Profile	14
Active Filtering Profiles	
Global Filtering Profile	14
NT/LDAP Group Filtering Profile	14
NT/LDAP Member Filtering Profile	1
LDAP Container Filtering Profile	
Override Account Profile	
Time Profile	1
Lock Profile	
Filtering Profile Components	10
Library Categories	1
8e6 Supplied Categories	
Custom Categories	1
Service Ports .	
Rules	
Minimum Filtering Level	
Filter Settings	
Filtering Rules	

R3000 Authentication Protocols	
R3000 Authentication Tiers and Optic	ons23
R3000 authentication tiers	
R3000 authentication options	
Authentication Solution Compatibility	
Authentication System Deployment C	Options26
Ports for Authentication System Acce	
Configuring the R3000 for Authentica	
Configuration procedures	
Group section	
CHAPTER 2: NETWORK SETUP	
Environment Requirements	
Workstation Requirements	
Administrator	
End User	
Network Requirements	
Set up the Network for Authenticat	ion34
Specify the operation mode	
Specify the subnet mask, IP address	
Invisible mode	
Router or firewall mode	
Enable authentication, specify criteria	
Net use based authentication	
Web-based authentication	
Enter network settings for authentica	
Create an SSL certificate	
Create, Download a Self-Signed	
Create, Upload a Third Party Cer	
	ate50
	ate52
	ificate53
View log results	
Specify block page settings	
Block Page Authentication	
Standard Links	60

Optional Links Options page Option 1 Option 2 Option 3 Common Customization Enable, disable features Authentication Form Customization Preview sample Authentication Request Form	
Block Page Customization	
Preview sample block page	75
CHAPTER 3: NT AUTHENTICATION SETUP	77
Join the NT Domain	77
Create an NT Domain	
Add an NT domain	
Refresh the NT branch	
View or modify NT domain details	
Domain Settings	
Default Rule	
Delete an NT domain	
Set up NT Domain Groups, Members	
Add NT groups, members to the tree	
Specify a group's filtering profile priority	
Manually add a user's name to the tree	
Manually add a group's name to the tree	
Upload a file of filtering profiles to the tree	91
Create and Maintain NT Profiles	94
Add an NT group, member to the tree list	
Add or maintain an entity's profile	
Category Profile	
Redirect URL	
Filter Options	
Remove an entity's profile from the tree	

#### CHAPTER 4: LDAP AUTHENTICATION SETUP ...... 102

Create an LDAP Domain	
Add the LDAP domain	
Refresh the LDAP branch	
View, modify, enter LDAP domain details	104
LDAP Server Type	105
Group Objects	106
User Objects	108
Address Info	
Account Info	
SSL Settings	
Alias List	
Default Rule	
LDAP Backup Server Configuration	
Configure a backup server	
Modify a backup server's configuration	
Delete a backup server's configuration	
Delete a domain	128
Set up LDAD Demain Groups, Members	400
Set up LDAP Domain Groups, Members	
Add LDAP groups, users to the tree	
Perform a basic search	
Options for search results	
Apply a filtering rule to a profile	
Delete a rule Specify a group's filtering profile priority	
Manually add a user's name to the tree	
Manually add a group's name to the tree	
Upload a file of filtering profiles to the tree	
	130
Create, Maintain LDAP Profiles	
Add an LDAP group, member to the tree	
Add or maintain an entity's profile	
Category Profile	
Redirect URL	
Filter Options	
Remove an entity's profile from the tree	
CHAPTER 5: AUTHENTICATION DEPLOYMENT	147
Test Authentication Settings	147
Test Web-based authentication settings	

Step 1: Create an IP Group, "test"	149
Step 2: Create a Sub-Group, "workstation"	150
Step 3: Set up "test" with a 32-bit net mask	
Step 4: Give "workstation" a 32-bit net mask	
Step 5: Block everything for the Sub-Group	
Step 6: Use Authentication Request Page for redirect URL .	
Step 7: Disable filter options	
Step 8: Attempt to access Web content .	
Test net use based authentication settings	
Activate Authentication on the Network	159
Activate Web-based authentication for an IP Group	160
Step 1: Create a new IP Group, "webauth"	
Step 2: Set "webauth" to cover users in range	
Step 3: Create an IP Sub-Group .	
Step 4: Block everything for the Sub-Group	
Step 5: Use Authentication Request Page for redirect URL .	
Step 6: Disable filter options	
Step 7: Set Global Group to filter unknown traffic	
Activate Web-based authentication for the Global Group	
Step 1: Exclude filtering critical equipment	
Step 1A: Block Web access, logging via Range to Detect	
Range to Detect Settings	
Range to Detect Setup Wizard	
Step 1B: Block Web access via IP Sub-Group profile	
Step 2: Modify the Global Group Profile	
Activate NT authentication	
Step 1: Modify the 3-try login script	
Step 2: Modify the Global Group Profile	
CHAPTER 6: TECHNICAL SUPPORT	191
	-
Hours	191
Contact Information	191
Domestic (United States)	
International	
E-Mail	
Office Locations and Phone Numbers	
8e6 Corporate Headquarters (USA)	
8e6 Taiwan	
	132

Support Procedures	193
APPENDIX A: AUTHENTICATION OPERATIONS	194
Authentication Tier Selections	194
Tier 1: Net use based authentication	194
Tier 2, Tier 3: Web-based authentication	195
Tier 1: Single Sign-On Authentication	196
Net use based authentication process	196
Re-authentication process	198
Tier 1 authentication methods	198
SMB protocol	198
SMB Signing	198
LDAP protocol	199
Name resolution methods	200
Configuring the authentication server	201
Login scripts	201
Enter net use syntax in the login script	201
View login script on the server console	202
Block page authentication login scripts	202
LDAP server setup rules	203
Tier 2: Time-based, Web Authentication	204
Tier 2 implementation in an environment	205
Tier 2 Script	206
Tier 1 and Tier 2 Script	207
Tier 3: Session-based, Web Authentication	209
8e6 Authenticator	210
Environment requirements	210
Minimum system requirements	210
Recommended system requirements	
Workstation requirements	
Work flow in a Windows environment	
8e6 Authenticator configuration priority	213
8e6 Authenticator configuration syntax	
Sample command line parameters	
Sample configuration file	
Sample R3000 configuration update packet 'PCFG'	

Table of parameters	215
Novell eDirectory Agent	218
Environment requirements	
Novell eDirectory servers	
Client workstations .	
Novell clients	219
Novell eDirectory setup	219
R3000 setup and event logs	220
Active Directory Agent	221
Product feature overview	221
Windows server requirements	222
Work flow in a Windows environment	222
Set up AD Agent	223
Step 1: AD Agent settings on the R3000	223
Step 2: Configure the domain, service account	
Step 3: AD Agent installation on Windows server	226
Step 3A: Download DCAgent.msi	226
Step 3B: Run AD Agent installation setup	
Step 3C: Run AD Agent configuration wizard	
Use the Active Directory Agent console	233
Activity tab	
Sessions tab	
Session table spreadsheet	
Session Properties window	
Workstation Interactive Probe window	
Active Directory Agent Configuration window	
Service page	
Appliance page	
Agent hosts page	
Add a satellite	
Remove a satellite	
Configure a satellite	
Check the status of a satellite	
Options page	
Notifications page	254
APPENDIX B: DISABLE SMB SIGNING REQUIREMENTS	. 256
SMB Signing Compatibility	256

Disable SMB Signing in Windows 2003	257
APPENDIX C: OBTAIN, EXPORT AN SSL CERTIFIC	ATE 262
Export an Active Directory SSL Certificate	
Export a Novell SSL Certficate	270
Obtain a Sun ONE SSL Certificate	272
APPENDIX D: LDAP SERVER CUSTOMIZATIONS	273
OpenLDAP Server Scenario Not all users returned in User/Group Browser	
APPENDIX E: USER/GROUP FILE FORMAT AND RU	ULES 274
Username Formats	274
Username Formats Rule Criteria	
	<b>275</b> <b>278</b> 279 280 281
Rule Criteria File Format: Rules and Examples NT User List Format and Rules NT Group List Format and Rules LDAP User List Format and Rules	<b>275</b> <b>278</b> 279 280 281 283
Rule Criteria File Format: Rules and Examples NT User List Format and Rules NT Group List Format and Rules LDAP User List Format and Rules LDAP Group List Format and Rules	275 278 279 280 281 283 284 285 285

AdwareSafe Pop-up Blocker If pop-up blocking is enabled Temporarily disable pop-up blocking	
Mozilla Firefox Pop-up Blocker Add override account to the white list	
Windows XP SP2 Pop-up Blocker Set up pop-up blocking Use the Internet Options dialog box Use the IE toolbar Temporarily disable pop-up blocking Add override account to the white list Use the IE toolbar Use the IE toolbar Use the Information Bar Set up the Information Bar Access your override account	290 290 291 291 291 292 292 292 293 293
APPENDIX G: GLOSSARY	295
Definitions	
INDEX	303

# **CHAPTER 1: INTRODUCTION**

The R3000 Authentication User Guide contains information about setting up authentication on the network.

# About this User Guide

This user guide addresses the network administrator designated to configure and manage the R3000 server on the network.

Chapter 1 provides information on how to use this user guide, and also includes an overview of filtering components and authentication solutions.

Chapters 2, 3, and 4 describe the R3000 Administrator console entries that must be made in order to prepare the network for using authentication for NT and/or LDAP domains.



**NOTE**: Refer to the R3000IR Quick Start Guide for information on installing the R3000 on the network. This document also provides information on how to access the R3000 console to perform the initial installation setup defined in Chapter 2: Network Setup.

After all settings have been made, authentication is ready to be used on the network. Chapter 5 outlines the step you need to take to test and to activate your settings before deploying authentication on the network.

Chapter 6 provides support information. Appendices at the end of this user guide feature instructions on authentication operations; steps to modify the SMB protocol to disable SMB Signing requirements; information on how to obtain or export an SSL certificate and upload it to the R3000; notes on customizations to make on specified LDAP servers; filtering profile file components and setup; tips on how to override pop-up windows with pop-up blocker software installed; a glossary on authentication terms, and an index.

# How to Use this User Guide

## Conventions

The following icons are used throughout this user guide:



**NOTE**: The "note" icon is followed by italicized text providing additional information about the current subject.



, TIP: The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.

WARNING: The "warning" icon is followed by italicized text Cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.

## Terminology

The following terms are used throughout this user guide. Sample images (not to scale) are included for each item.

 alert box - a message box that opens in response to an entry you made in a dialog box, window, or screen. This box often contains a button (usually

Message	×
Successfully saved Alert email(s).	
OK	
Java Applet Window	

labeled "OK") for you to click in order to confirm or execute a command.

 button - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.

<u>A</u> pply

- checkbox a small square in a dialog box, window, or screen used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an "X" is placed, indicating that you selected the option. When this box is not checked, the option is not selected.
- dialog box a box that opens in response to a command made in a window or screen, and requires your input. You must choose an option by

Select an Option
Are you sure you want to save the profile?
Yes
Java Applet Window

clicking a button (such as "Yes" or "No", or "Next" or "Cancel") to execute your command. As dictated by this box, you also might need to make one or more entries or selections prior to clicking a button.

 field - an area in a dialog box, window, or screen that either accommodates your data

lame	СНАТ
------	------

entry, or displays pertinent information. A text box is a type of field.

 frame - a boxed-in area in a dialog box, window, or screen that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, check-

Page Content			
🗹 Basic			
🗖 Filter Info			
🗌 Override Account			

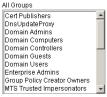
boxes, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function or purpose.

 grid - an area in a frame that displays rows and columns of

	Date	Filename	Content	Comment
	Jul 22, 2003	lib1.tar.gz	LIBRARY_ONLY	backup old library
- Ja	Jul 23, 2003	config3.tar.gz	CONFIG_ONLY	backup old configurations
- [	Jul 22, 2003	config1.tar.gz	CONFIG_ONLY	testing
	Jul 22, 2003	both.tar.gz	CONFIG_AND_LIBRARY	backup library and configs

data, as a result of various processes. This data can be reorganized in the R3000 console, by changing the order of the columns.

- list box an area in a dialog box, window, or screen that accommodates and/or displays entries of items that can be added or removed.
- navigation panel the panel that displays at the left of a screen. This panel can contain links that can be clicked to open windows or dialog boxes at the right of the screen. One or more tree lists also can display in this panel. When an item in the tree list is doubleclicked, the tree list opens to reveal items that can be selected.





 pop-up box or pop-up window - a box or window that opens after you click a button in a dialog box, window, or screen. This box or window may display infor-

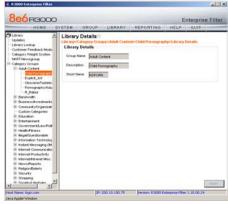


mation, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.

pull-down menu - a field in a dialog box, window, or screen

that contains a down-arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.

- radio button a small, circular object
   On O off
   in a dialog box, window, or screen
   used for selecting an option. This object allows you to
   toggle between two choices. By clicking a radio button, a
   dot is placed in the circle, indicating that you selected the
   option. When the circle is empty, the option is not
   selected.
- screen a main object of an application that displays across your monitor. A screen can contain panels, windows, frames, fields, tables, text boxes, list boxes, icons, buttons, and radio buttons.



 sub-topic - a subset of a main topic that displays as a menu item for the topic. The menu of subtopics opens when a perti-



nent topic link in the left panel—the navigation panel—of a screen is clicked. If a sub-topic is selected, the window for that sub-topic displays in the right panel of the screen, or a pop-up window or an alert box opens, as appropriate.

- text box an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See "field".)
- topic a topic displays as a link in the left panel—the navigation panel—of a screen. By clicking the link for a topic, the window for that topic displays in the right panel of the screen, or



a menu of sub-topics opens.

Group Global Group

⊡\_\_\_\_\_admin ⊡\_\_\_\_\_\_tech

bkupserver

Apply

💷 cpike

- tree a tree displays in the navigation panel of a screen, and is comprised of a hierarchical list of items. An entity associated with a branch of the tree is preceded by a plus (+) sign when the branch is collapsed. By double-clicking the item, a minus (-) sign replaces the plus sign, and any entity within that branch of the tree displays. An item in the tree is selected by clicking it.
- window a window displays on a screen, and can contain frames, fields, text boxes, list boxes, buttons, checkboxes, and radio buttons. A window for a topic or sub-topic displays in the right panel of the screen. Other types

ystem>Control>Filter	
Local Filtering	
Local Filtering	© on C o
VLAN Detection	C On @ C
Service Blocking	
Instant Messaging	C on @ o
P2P	C on @ c
HTTPS Filtering	
HTTPS Filtering Level	C None C Low @ Medium C Hig
Service Control	
Proxy Pattern Blocking	Con @ c
Target(s) Filtering	
All Target(s) Filtering	Con Co

of windows include pop-up windows, login windows, or ones from the system such as the Save As or Choose file windows.



# **Filtering Elements**

Filtering operations include the following elements: groups, filtering profiles and their components, and rules for filtering.

# Group Types

In the Group section of the Administrator console, group types are structured in a tree format in the navigation panel. There are four group types in the tree list:

- Global Group
- IP groups
- NT domain groups
- LDAP domain groups

**NOTE**: If authentication is enabled, the global administrator who has all rights and permissions on the R3000 server—will see all branches of the tree: Global Group, IP, NT, and LDAP. If authentication is disabled, only the Global Group and IP branches will be seen.

### **Global Group**

The first group that must be set up is the global group,

represented in the tree structure by the global icon <sup>(2)</sup>. The filtering profile created for the global group represents the default profile to be used by all groups that do not have a filtering profile, and all users who do not belong to a group.

#### **IP Groups**

The IP group type is represented in the tree by the IP icon



📕 . A master IP group is comprised of sub-group members

and/or individual IP members 💻

The global administrator adds master IP groups, adds and maintains override accounts at the global level, and establishes and maintains the minimum filtering level.

The group administrator of a master IP group adds subgroup and individual IP members, override account and time profiles, and maintains filtering profiles of all members in the master IP group.

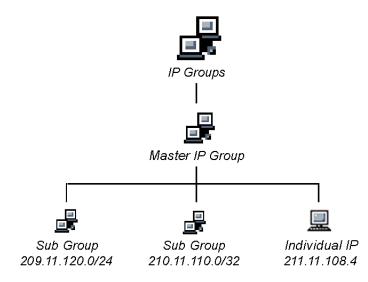


Fig. 1-1 IP diagram with a sample master IP group and its members

#### **NT Domain Groups**

An NT domain on a network server is comprised of Windows NT groups and their associated members (users), derived from profiles on the network's domain controller.

The NT group type is represented in the tree by the NT icon

📲 . This branch will only display if authentication is enabled. Using the tree menu, the global administrator adds

and maintains NT domains  $\Delta_{a}^{a}$ , and profiles of NT groups and members within the domain.

Filtering profiles can be created for a specified group

user  $\overset{\circ}{\square}$ . If users belong to more than one group, the global administrator sets the priority for group filtering.

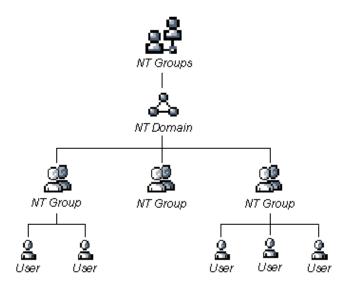


Fig. 1-2 NT domain diagram, with sample groups and members

#### LDAP Domain Groups

An LDAP (Lightweight Directory Access Protocol) domain on a network server is comprised of LDAP groups and their associated members (users), derived from profiles on the network's authentication server.

The LDAP group type is represented in the tree by the

LDAP icon 🖳 This branch will only display if authentication is enabled. Using the tree menu, the global adminis-

trator adds and maintains LDAP domains  $\square$ , and profiles of LDAP groups and members within the domain.

For Active Directory or "Other" server types, filtering profiles

can be created for a specified primary or static group

user 🕌, or container 🍑. For Novell eDirectory, SunOne, Sun IPlanet, or Netscape Directory server types, filtering

profiles can also be created for a dynamic group 强.

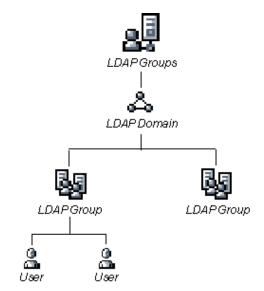


Fig. 1-3 LDAP domain diagram, with sample groups and members

If users belong to more than one group, the global administrator sets the priority for group filtering.

## Filtering Profile Types

A filtering profile is used by all users who are set up to be filtered on the network. This profile consists of rules that dictate whether a user has access to a specified Web site or service on the Internet.

The following types of filtering profiles can be created, based on the set up in the tree menu of the Group section of the console:

#### **Global Group**

• **global filtering profile** - the default filtering profile positioned at the base of the hierarchical tree structure, used by end users who do not belong to a group.

#### IP group (Master Group)

- **master group filtering profile** used by end users who belong to the master group.
- **master time profile** used by master group users at a specified time.

#### **IP** group member

- **sub-group filtering profile** used by a sub-group member.
- **individual filtering profile** used by an individual IP group member.
- **time profile** used by a sub-group/individual IP group member at a specified time.

#### Authentication filtering profiles

• NT/LDAP group filtering profile - used by an NT or LDAP group.

- NT/LDAP member filtering profile used by an NT or LDAP group member.
- LDAP container filtering profile used by an LDAP container in an LDAP domain.

#### Other filtering profiles

• **override account profile** - set up in either the global group section or the master group section of the console.

**NOTE**: An override account set up in the master IP group section of the R3000 console takes precedence over an override account set up in the global group section of the console.

• **lock profile** - set up under X Strikes Blocking in the Filter Options section of the profile.

## **Static Filtering Profiles**

Static filtering profiles are based on fixed IP addresses and include profiles for master IP groups and their members.

#### **Master IP Group Filtering Profile**

The master IP group filtering profile is created by the global administrator and is maintained by the group administrator. This filtering profile is used by members of the group including sub-group and individual IP group members—and is customized to allow/deny users access to URLs, or warn users about accessing specified URLs, to redirect users to another URL instead of having a block page display, and to specify usage of appropriate filter options.

#### **IP Sub-Group Filtering Profile**

An IP sub-group filtering profile is created by the group administrator. This filtering profile applies to end users in an IP sub-group and is customized for sub-group members.

#### Individual IP Member Filtering Profile

An individual IP member filtering profile is created by the group administrator. This filtering profile applies to a specified end user in a master IP group.

### **Active Filtering Profiles**

Active filtering profiles include the global group profile, NT/ LDAP authentication profile, override account profile, time profile, and lock profile.

#### **Global Filtering Profile**

The global filtering profile is created by the global administrator. This profile is used as the default filtering profile. The global filtering profile consists of a customized profile that contains a list of library categories to block, open, add to a white list, or assign a warn setting, and service ports that are configured to be blocked. A URL can be specified for use instead of the standard block page when users attempt to access material set up to be blocked. Various filter options can be enabled.

#### **NT/LDAP Group Filtering Profile**

An NT or LDAP group filtering profile is created by the global administrator. This profile can be customized to allow/deny group users access to URLs, or warn users about accessing specified URLs, to redirect users to another URL instead of having the standard block page display, and to specify usage of appropriate filter options.

If users belong to more than one group, all groups to which they belong must be ranked to determine the priority each filtering profile takes over another.

#### **NT/LDAP Member Filtering Profile**

An NT or LDAP member filtering profile is created by the global administrator. This profile can be customized to allow/deny a user access to URLs, or warn a user about accessing specified URLs, to redirect the user to another URL instead of the standard block page, and to specify usage of appropriate filter options.

#### LDAP Container Filtering Profile

An LDAP container filtering profile is created by the global administrator. This profile can be customized to allow/deny users access to URLs, or warn users about accessing specified URLs, to redirect users to another URL instead of the standard block page, and to specify usage of appropriate filter options.

#### **Override Account Profile**

If any user needs access to a specified URL that is set up to be blocked, the global administrator or group administrator can create an override account for that user. This account grants the user access to areas set up to be blocked on the Internet.

#### Time Profile

A time profile is a customized filtering profile set up to be effective at a specified time period for designated users.

#### Lock Profile

This filtering profile blocks the end user from Internet access for a set period of time, if the end user's profile has the X Strikes Blocking filter option enabled and he/she has received the maximum number of strikes for inappropriate Internet usage.



**NOTE**: Refer to the R3000 User Guide for additional information on the Override Account Profile, Time Profile, and Lock Profile.

## Filtering Profile Components

Filtering profiles are comprised of the following components:

- **library categories** used when creating a rule, minimum filtering level, or filtering profile for the global group or any entity
- **service ports** used when setting up filter segments on the network, creating the global group (default) filtering profile, or establishing the minimum filtering level
- rules specify which library categories should be blocked, left open, assigned a warn setting, or white listed
- filter options specify which features will be enabled: X Strikes Blocking, Google/Yahoo! Safe Search Enforcement, Search Engine Keyword Filter Control, URL Keyword Filter Control
- **minimum filtering level** takes precedence over filtering profiles of entities who are using a filtering profile other than the global (default) filtering profile
- filter settings used by service ports, filtering profiles, rules, and the minimum filtering level to indicate whether users should be granted or denied access to specified Internet content

#### **Library Categories**

A library category contains a list of Web site addresses and keywords for search engines and URLs that have been set up to be blocked or white listed. Library categories are used when creating a rule, the minimum filtering level, or a filtering profile.

#### **8e6 Supplied Categories**

8e6 furnishes a collection of library categories, grouped under the heading "Category Groups" (excluding the "Custom Categories" group). Updates to these categories are provided by 8e6 on an ongoing basis, and administrators also can add or delete individual URLs within a specified library category.

#### **Custom Categories**

Custom library categories can be added by either global or group administrators. As with 8e6 supplied categories, additions and deletions can be made within a custom category. However, unlike 8e6 supplied categories, a custom category can be deleted.

٢

**NOTE**: 8e6 cannot provide updates to custom categories. Maintaining the list of URLs and keywords is the responsibility of the global or group administrator.

#### **Service Ports**

Service ports are used when setting up filter segments on the network (the range of IP addresses/netmasks to be detected by the R3000), the global (default) filtering profile, and the minimum filtering level.

When setting up the range of IP addresses/netmasks to be detected, service ports can be set up to be open (ignored). When creating the global filtering profile and the minimum filtering level, service ports can be set up to be blocked or filtered.

Examples of service ports that can be set up include File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Network News Transfer Protocol (NNTP), Secured HTTP Transmission (HTTPS), and Secure Shell (SSH).

#### **Rules**

A rule is comprised of library categories to block, leave open, assign a warn setting, or include in a white list. Each rule that is created by the global administrator is assigned a number. A rule is selected when creating a filtering profile for an entity.

### **Minimum Filtering Level**

The minimum filtering level consists of library categories set up at the global level to be blocked or opened, and service ports set up to be blocked or filtered. If the minimum filtering level is created, it applies to all users in IP, NT, and LDAP groups, and takes precedence over filtering settings made for group and member filtering profiles.

The minimum filtering level does not apply to any user who does not belong to a group, and to groups that do not have a filtering profile established.



**NOTE**: If the minimum filtering level is not set up, global (default) filtering settings will apply instead.

#### **Filter Settings**

Categories and service ports use the following settings to specify how filtering will be executed:

- block if a category or a service port is given a block setting, users will be denied access to the item set up as "blocked"
- **open** if a category or the filter segment detected on the network is given an open (pass) setting, users will be allowed access to the item set up as "opened"
- **always allowed** if a category is given an always allowed setting, the category is included in the user's white list and takes precedence over blocked categories
- **warn** If a category is given a warn setting, a warning page displays for the end user to warn him/her that accessing the intended URL may be against established policies and to proceed at his/her own risk
- filter if a service port is given a filter setting, that port will use filter settings created for library categories (block or open settings) to determine whether users should be denied or allowed access to that port
- ignore if the filter segment detected on the network has a service port set up to be ignored, that service port will be bypassed

## Filtering Rules

**Individual User Profiles** - A user in an NT or LDAP domain can have only one individual profile set up per domain.

#### Filtering Levels Applied:

- 1. The global (default) filtering profile applies to any user under the following circumstances:
  - the user does not belong to a master IP group
  - the user has not been assigned a domain default profile from an NT or LDAP authentication domain
- If a minimum filtering level is defined, it applies to all master IP groups (and their members) and NT/LDAP groups who have been assigned filtering profiles after authenticating. The minimum filtering level combines with the user's profile to guarantee that categories blocked in the minimum filtering level are blocked in the user's profile.
- 3. For master IP group members:
  - a. A master IP group filtering profile takes precedence over the global profile.
  - b. A master IP group time profile takes precedence over the master IP group profile.
- 4. For IP sub-group members:
  - a. An IP sub-group filtering profile takes precedence over the master IP group's time profile.
  - b. An IP sub-group time profile takes precedence over the IP sub-group profile.
- 5. For individual IP members:
  - a. An individual IP member filtering profile takes precedence over the IP sub-group's time profile.
  - b. An individual IP member time profile takes precedence over the individual IP member profile.

- For NT/LDAP users, if a user is authenticated, settings for the user's group or individual profile from the NT/ LDAP domain are applied and take precedence over any IP profile.
  - a. If the user belongs to more than one group in an authentication domain, the profile for the user is determined by the order in which the groups are listed in the Group Priority list set by the global administrator. The user is assigned the profile for the group highest in the Group Priority list.
  - b. If a user has an individual profile set up, that profile supercedes all other profile levels for that user. The user can have only one individual profile in each domain.
  - c. On an LDAP domain, if a user belongs to a container, that profile takes precedence over the group profile for that user.
- 7. An override account profile takes precedence over an authentication profile. This account may override the minimum filtering level—if the override account was set up in the master IP group tree, and the global administrator allows override accounts to bypass the minimum filtering level, or if the override account was set up in the global group tree.



**NOTE**: An override account set up in the master IP group section of the R3000 console takes precedence over an override account set up in the global group section of the console.

8. A lock profile takes precedence over all filtering profiles. This profile is set up under Filter Options, by enabling the X Strikes Blocking feature.

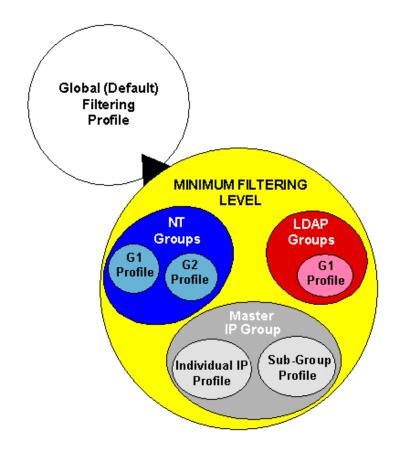


Fig. 1-4 Sample filtering hierarchy diagram

# **Authentication Solutions**

## **R3000 Authentication Protocols**

The R3000 supports two types of authentication protocols: Windows NT LAN Manager (NTLM), and Lightweight Directory Access Protocol (LDAP).

- NTLM authentication supports NTLM authentication running on any of the following servers: Windows NT 4.0, Windows 2000 Mixed Mode, and Windows 2003 Mixed Mode.
- LDAP authentication supports all versions of LDAP, such as Microsoft Active Directory, Novell eDirectory, Sun ONE, and OpenLDAP.

## R3000 Authentication Tiers and Options

#### **R3000** authentication tiers

The R3000 authentication architecture for NTLM and LDAP authentication protocols is comprised of three tiers. When using NT and/or LDAP authentication with the R3000, one of these three tiers is selected for use on the network, depending on the server(s) used on the network and the preferred authentication method(s) to be employed.

- Tier 1: Single sign-on, net use based authentication for NT or Active Directory domains.
- Tier 2: Time-based, Web authentication for NT and LDAP authentication methods.
- Tier 3: Session-based, Web authentication for NT or LDAP authentication method.

#### **R3000** authentication options

Depending on the setup of your network, any of the following authentication options can be enabled to ensure the end user is authenticated when logging into his/her workstation: 8e6 Authenticator, Active Directory Agent, and Novell eDirectory Agent.



**& NOTE**: See Appendix A: Authentication Operations for information on using Tier 1, Tier 2, and Tier 3 on the network, and configuring 8e6 Authenticator, Novell eDirectory Agent, and Active Directory Agent.

## Authentication Solution Compatibility

Below is a chart representing the authentication solution compatibility for a single user:

	Tier1 net use	Tier 2 time based	Tier 3 session based	8e6 Authen- ticator	eDirec- tory Agent	Active Directory Agent
Tier 1		Yes	Yes	N/R	N/A	N/R
Tier 2	Yes		N/A	Yes	Yes	Yes
Tier 3	Yes	N/A		Yes	Yes	Yes
8e6 Authen- ticator	N/R	Yes	Yes		N/R	N/R
eDirectory Agent	N/A	Yes	Yes	N/R		N/A
Active Directory Agent	N/R	Yes	Yes	N/R	N/A	

KEY:

- N/A = Not Applicable
- N/R = Not Recommended

## Authentication System Deployment Options

Below is a chart representing authentication system deployment options on a network:

Authentication System	Single Sign-On (SSO)	Force Authentication
SunOne OpenLDAP CommuniGate Pro (Stalker)	None	Tier 2 or Tier 3
Windows NT 4.0	Tier 1 "net use"	Tier 2 or Tier 3
Windows 2000/2003 Server (both Mixed and Native modes)	Tier 1 "net use" 8e6 Authenticator AD Agent	Tier 2 or Tier 3
Novell eDirectory	8e6 Authenticator Novell eDirectory Agent (for eDirectory server version 8.7 and higher)	Tier 2 or Tier 3
Windows 2000/2003 Server and Novell eDirectory Mixed environment	8e6 Authenticator Novell eDirectory Agent AD Agent	Tier 2 or Tier 3

## Ports for Authentication System Access

The following ports should be used for authentication system access:

Туре	No.	Function
TCP	8081	Used between the R3000's transmitting inter- face and the SSL block page for Tier 2 or Tier 3 authentication.
ТСР	836	Used between the R3000's Virtual IP address and Java applet for Tier 3 authentication.
ТСР	139	Used between the R3000 and workstations requiring Tier 1 or Tier 3 authentication.
TCP/ UDP	137	Used between the R3000 and workstations requiring Tier 1 authentication.
LDAP	389	Used for communicating with domain control- lers in order to bind with them so that user/ group information can be queried/accessed.
LDAPS	636	Used for communicating with domain control- lers in order to bind with them so that user/ group information can be queried/accessed.

## Configuring the R3000 for Authentication

#### **Configuration procedures**

When configuring the R3000 server for authentication, settings must be made in System and Group windows in the Administrator console.



**NOTES**: If the network has more than one domain, the first one you add should be the domain on which the R3000 resides.

The entries described in this section represent entries to be made on a typical network.

#### System section

The first settings for authentication must be made in the System section of the Administrator console in the following windows: Operation Mode, LAN Settings, Enable/Disable Authentication, Authentication Settings, Authentication SSL Certificate (if Web-based authentication will be used), and Block Page Authentication.

1. Select "Mode" from the navigation panel, and then select "Operation Mode" from the pop-up menu.

The entries made in the Operation Mode window will vary depending on whether you will be using the invisible mode, or the router or firewall mode.

In the Listening Device frame, set the Listening Device to "LAN1".

In the Block Page Device frame:

- · If using the invisible mode, select "LAN2".
- If using the router or firewall mode, select "LAN1".
- 2. Select "Network" from the navigation panel, and then select "LAN Settings" from the pop-up menu.

The entries made in this window will vary depending on whether you are using the invisible mode, or the router or firewall mode. The LAN1 and LAN2 IP addresses usually should be in a different subnet.

- If using the invisible mode: For the LAN1 IP address, select 255.255.255 for the subnet mask.
- If using the router or firewall mode: Specify the appropriate IP address and subnet mask in the applicable fields.
- 3. Select "Authentication" from the navigation panel, and then select Enable/Disable Authentication from the pop-up menu.

Enable authentication, and then select one of three tiers in the Web-based Authentication frame:

- Tier 1: Choose this option if you will only be using net use based authentication for NT or Active Directory servers.
- Tier 2: Choose this option if you wish to use timed Web-based authentication for NT and LDAP domains. This option gives the user a timed session for his/her Internet access. After the timed profile expires, the user will have to log in again if he/she wants to continue to have Internet access.
- Tier 3: Choose this option if you wish to use persistent Web-based authentication for NT and LDAP domains. This option gives the user a persistent network connection via a pop-up window that keeps the user's session open until the window is closed, so the user does not have to log in repeatedly.

If you wish to use the tier you specified as a fallback authentication solution, you have the option to enable any of the following authentication solutions as appropriate to your environment: 8e6 Authenticator, Active Directory Agent, Novell eDirectory Agent. 4. Select "Authentication" from the navigation panel, and then select "Authentication Settings" from the pop-up menu.

In the Settings frame, enter general configuration settings for the R3000 server such as IP address entries.

From the NIC Device to Use for Authentication pull-down menu:

- If using the invisible mode: Select "LAN2" as the device to send traffic on the network.
- · If using the router or firewall mode: Select "LAN1".

Information should only be entered in the NT Authentication Server Details frame if the R3000 will use the NT Authentication method to authenticate users.

5. Select "Authentication" from the navigation panel, and then select Authentication SSL Certificate from the popup menu. This option should be used if Web-based authentication will be deployed on the R3000 server.

Using this option, you create either a self-signed certificate or a Certificate Request (CSR) for use by the Secure Sockets Layer (SSL). The certificate should be placed on client machines so that these machines will recognize the R3000 as a valid server with which they can communicate.

6. Select "Control" from the navigation panel, and then select "Block Page Authentication" from the pop-up menu.

In the Block Page Authentication window, select the Reauthentication Options to be used. The items you select will be listed as options for re-authentication on the Options page, accessible from the standard block page. If the "Re-authentication" (NET USE) option is selected, enter the login script path to be used by the R3000 for reauthentication purposes.

#### **Group section**

In the Group section of the Administrator console, choose NT or LDAP, and then do the following:

1. Add a domain from the network to the list of domains that will have users authenticated by the R3000.



**NOTE**: If the network has more than one domain, the first one you add should be the domain on which the R3000 resides.

- 2. Create filtering profiles for each group within that domain.
- 3. Set the group priority by designating which group profile will be assigned to a user when he/she logs in. If a user is a member of multiple groups, the group that is positioned highest in the list is applied.
- 4. Create unique filtering profiles for individual users.

# CHAPTER 2: NETWORK SETUP

# **Environment Requirements**

## Workstation Requirements

#### Administrator

Minimum system requirements for the administrator include the following:

- Windows 98 or later operating system (not compatible with Windows server 2003)
- Internet Explorer (IE) 5.5 or later
- · JavaScript enabled
- Java Virtual Machine
- Java Plug-in (use the version specified for the R3000 software version)
- Java Runtime Environment, if using Tier 3 authentication

NOTE: R3000 administrators must be set up with software installation privileges in order to install Java used for accessing the interface.

#### End User

- Windows 98 or later operating system (not compatible with WIndows server 2003)
- Internet Explorer (IE) 5.5 or later
- · JavaScript enabled
- Java Runtime Environment, if using Tier 3 authentication
- Pop-up blocking software, if installed, must be disabled

## Network Requirements

- High speed connection from the R3000 server to the client workstations
- FTP or HTTPS connection to 8e6's software update server
- Internet connectivity for downloading Java Virtual Machine—and Java Runtime Environment, if necessary—if not already installed

# Set up the Network for Authentication

The first settings for authentication must be made in the System section of the console in the following windows: Operation Mode, LAN Settings, Enable/Disable Authentication, Authentication Settings, Authentication SSL Certificate (if Web-based authentication will be used), View Log File (for troubleshooting authentication setup), and Block Page Authentication. Entries for customizing the block page and/ or authentication request form are made in the Common Customization, Authentication Form Customization, and Block Page Customization windows.

## Specify the operation mode

Click Mode and select Operation Mode from the pop-up menu to display the Operation Mode window:

🚔 R3000 Enterprise Filter				
8e6 R3000	YSTEM GROUP LIBRARY	REPORTING	E	nterprise Filter
System     Control     Network     Administrator     Diagnostics     Alert     Patch     Synchronization     Mode     Backup/Restore     Reset     Reset     SNMP     Hardware Failure Detection     X Strikes Elocking     Customization	STEM     GROOP     ElBRARY       Operation Mode     System>Mode>Operation Mode       Mode     © Invisible     C Router     C Firewall       © Invisible     C Router     C Firewall     C       Listening Device     Device     Device     Device       Device     LANT     ■       Block Page Delivery Method     Protocol Methods:     © Send Block Page via ARP Table     © Sen       Block Page Note To:     © Default Gateway     C Alternate IP Address     IP       Current MAC Address     00:02:16:0A:52:0	Mobile Block Pag Device to set d Block to Specified He	<b>je Device</b> nd block page	LAN2
				Apply
Host Name: logo.com	IP: 200.10.100.75	Version: R3000 En	terprise Filter	1.10.10.5
Java Applet Window				

Fig. 2-1 Operation Mode window

The entries made in this window will vary depending on whether you will be using the invisible mode, or the router or firewall mode.

- 1. In the Mode frame, select the mode to be used: "Invisible", "Router", or "Firewall".
- 2. In the Listening Device frame, set the **Device** to "LAN1".

- 3. In the Block Page Device frame:
  - · If using the invisible mode, select "LAN2".
  - · If using the router or firewall mode, select "LAN1".

If using the invisible mode, the Block Page Delivery Method frame displays. Choose from either of the two **Protocol Methods**:

- "Send Block Page via ARP Table" this option uses the Address Resolution Protocol method to find the best possible destination MAC address of a specified host, usually the R3000 gateway.
- "Send Block to Specified Host MAC Address" using this preferred method, the block page will always be sent to the MAC address of a specified host, usually the R3000 gateway.

Choose from either of the two **Block Page Route To** selections:

- "Default Gateway" this option indicates that the default gateway on your network will be used for sending block pages.
- "Alternate IP Address" this option should be used if block pages are not being served.

Enter the **IP** address of the router or device that will serve block pages.

4. Click Apply.

## Specify the subnet mask, IP address(es)

Click Network and select LAN Settings from the pop-up menu to display the LAN Settings window:

🚖 R3000 Enterprise Filter						
	YSTEM	GROUP	LIBRARY	REPORTING	E HELP	nterprise Filter
System Control Administrator Administrator Diagnostics Alert Patch Synchronization Mode Backup/Restore Rest Rest Radius Authentication Setting SNMP Hardware Failure Detection X Strikes Elocking Customization Customization Host Name: logo.com	System> Host Nam	-		.20.75 / 25	5.255.255.25	Apply
Java Applet Window		1.		procession reduced an	icorprise r neer	
Java Applet window						

Fig. 2-2 LAN Settings window

The entries made in this window will vary depending on whether you are using the invisible mode, or the router or firewall mode.



**NOTE**: If the gateway IP address on the network changes, be sure to update the Gateway IP address in this window.

#### Invisible mode

For the **LAN1 IP** address, select *255.255.255.255* for the subnet mask, and click **Apply**.

#### Router or firewall mode

- 1. Enter the following information:
  - In the LAN1 IP field of the IP/Mask Setting frame, enter the IP address and specify the corresponding subnet of the "LAN1" network interface card to be used on the network.
  - In the LAN2 IP field, enter the IP address and specify the corresponding subnet of the "LAN2" network interface card to be used on the network.

**TIP**: The LAN1 and LAN2 IP addresses usually should be placed in different subnets.

- In the Primary IP field of the DNS frame, enter the IP address of the first DNS server to be used for resolving the IP address of the authentication server with the machine name of that server.
- In the **Secondary IP** field of the DNS frame, enter the IP address of the second DNS server to be used for resolving the IP address of the authentication server with the machine name of that server.
- In the Gateway IP field of the Gateway frame, enter the IP address of the default router to be used for the entire network segment.
- 2. Click **Apply** to apply your settings.

**NOTE**: Whenever modifications are made in this window, the server must be restarted in order for the changes to take effect.

## Enable authentication, specify criteria

- Click Authentication and select Enable/Disable Authentication from the pop-up menu to display the Enable/ Disable Authentication window:
- 2. Click Enable to enable authentication.
- 3. Select one of three tiers in the Web-based Authentication frame:

8e6 R3000						nterpris	and the second se
HOME S	YSTEM	GROUP	LIBRARY	REPORTING	HELP	QUIT	
System Control Network Administrator Diagnostics Alert Patch Synchronization Mode Sudhentication MC Mode Backup/Restore Reset Readius Authentication Setting SNMP Hardware Failure Detection X Strikes Blocking Warn Option Setting Customization	System>A Authentica Web-ba C Tier 1 C Tier 2 C Tier 3 Tier 2 & 3 authentic card insta 8 e6 Au C On ( R is highly AD Age C On (	uthentication ication sed Authent : Web-based A : Use time-base : Use persisten Note: In an or siton proces. ! leel. Please co leel. Please co thenticator > Orf orf	uthentication uthentication disa ed profiles, with thi t logins via a Java ganization with mo In this scenario, 8 In this scenario, 8 In this scenario, 8 that the Se6 Auth	e Authentication oled (Net Use enabled) ne-out (in minutes): 30 Applet re than 5000 users, slond for recommends using an	viness may b n R3000 Filter Dow Powed on at all b	r with an SSL mioad 8e6 Au imes.	accelerator
	Novell eDirectory Agent						
	Sendin ⓒ on (	<b>g Keep Aliv</b> 이 Off	e	Inactive ses	ssion lifetime	(in minutes):	20160
						l	Apply

Fig. 2-3 Enable/Disable Authentication window

**NOTES**: See information on the following pages for details about each of the tiers, and for steps that must be executed to enable your tier selection.

See Appendix A: Authentication Operations for more information about each tier and for configuring various authentication options.

- 4. Enable any of the following authentication options, as pertinent to your environment:
  - In the 8e6 Authenticator frame, be sure the 8e6 Authenticator is "On"—unless the Novell eDirectory Agent option will be used instead. When enabling the 8e6 Authenticator option, and then downloading and installing the 8e6 Authenticator (authenticat.exe) on a network share accessible by the domain controller or a Novell eDirectory server, the 8e6 Authenticator automatically authenticates the end user when he/she logs into his/her workstation.
  - If you have a Novell eDirectory server and the 8e6 Authenticator will not be used, turning "On" Novell eDirectory Agent will enable end user logon and logoff events to be logged. To use this option, the LDAP domain must be set up and activated in the Group tree.

WARNING: When enabling Novell eDirectory Agent, the agent will immediately begin scanning Novell eDirectory-based domain labels.

- If using a Windows 2000 or Windows 2003 server for authentication, the Active Directory Agent option can be used for capturing end user logon and logoff events and sending a session table to the R3000 so end users receive the correct filtering profile. To use this feature, turn "On" the AD Agent, and then specify settings for administrator computers authorized to configure the AD Agent via the Active Directory Agent console. Download and install the AD Agent (DCAgent.msi) on the administrator workstation.
- 5. If using Tier 1, in the Sending Keep Alive frame, click "On" to specify that keep alives should be sent on a connection to verify whether it is still active. Click "Off" to specify that the end user's session will be kept alive based on the number of minutes entered in the text box.
- 6. Click Apply.

#### Net use based authentication

**Tier 1: Web-based Authentication disabled (Net Use enabled)** – Choose this option if you will be using net use based authentication for NT or Active Directory.

- 1. Click "Tier 1".
- 2. In the Sending Keep Alive frame, click the radio button corresponding to the option to be used:
  - "On" This option specifies that keep alives should be sent on a connection to verify whether it is still active.
  - "Off" This option specifies that the end user's session will be kept alive based on the number of minutes entered in the text box.

In the **Inactive session lifetime (in minutes)** field, enter the number of minutes the end user's session will be kept alive.

3. Click **Apply** to open the alert box that confirms your selection.

#### Web-based authentication

Choose either Tier 2 or Tier 3 if Web-based authentication will be used.

**NOTE**: If selecting either Tier 2 or Tier 3, please be informed that in an organization with more than 5000 users, slowness may be experienced during the authentication process. In this scenario, 8e6 recommends using an R3000 Filter with an SSL accelerator card installed. Please contact 8e6 for more information.

**Tier 2: Use time-based profiles, with time-out (in minutes)** – Choose this option if using NT and/or LDAP authentication, and you want the user to have a time limit on his/her Internet connection. This option uses an authentication servlet that lets the user log into either domain with no persistent connection between the client PC and the R3000.

- 1. Click "Tier 2".
- 2. Enter a whole number for the duration of time the user will retain his/her Internet connection.
- 3. Click **Apply** to open the alert box that confirms your selection.

**Tier 3: Use persistent logins via a Java Applet** – Choose this option if using NT and/or LDAP authentication, and you want the user to maintain a persistent network connection.

This option—the preferred method for NT authentication opens a profile window that uses a Java applet:



Fig. 2-4 Java applet

The profile window must be kept open during the user's session in order for the user to have continued access to the Internet.

**NOTE**: Tier 3 Authentication requires a current version of Java Runtime Environment (JRE) on end-users' PCs. In some cases, a JRE will need to be downloaded and installed on workstations and the R3000 will allow the JRE download at the time of login. However some operating systems may require this action to be performed manually.

- 1. Click "Tier 3".
- 2. Click **Apply** to open the dialog box that informs you about the requirement of a current Java Runtime Environment (JRE) to be installed on each end user's workstation:

Message X
Tier 3 Authentication requires a current version of Java Runtime Environment (JRE) on end-users' PCs. In some cases, a JRE will need to be downloaded and installed on workstations and the R3000 will allow the JRE download at the time of login. However some operating systems may require this action to be performed manually.
To ensure that the end-users are using the most current version of JRE, choose the method for distributing the current version to their workstations:
C 8e6 automatically distributes JRE during user login
<ul> <li>Administrator manually distributes JRE to user workstations</li> </ul>
Continue Cancel
Java Applet Window

Fig. 2-5 Tier 3 dialog box

- To ensure that end-users are using the most current version of JRE, choose the method for distributing the current version to their workstations: "8e6 automatically distributes JRE during user login" or the default selection, "Administrator manually distributes JRE to user workstations".
- 4. Click **Continue** to open the alert box that confirms your selection.

## Enter network settings for authentication

 Click Authentication and select Authentication Settings from the pop-up menu to display the Authentication Settings window:

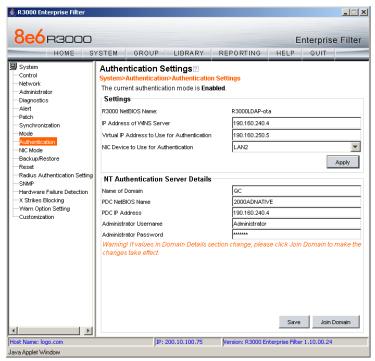


Fig. 2-6 Authentication Settings window

In the Settings frame, at the **R3000 NetBIOS Name** field the NetBIOS name of the R3000 displays. This information comes from the entry made in the Host Name field of the LAN Settings window.

2. In the **IP Address of WINS Server** field, if using a WINS server for name resolution, enter the IP address of each Windows DNS server to be filtered by this R3000, with a space between each IP address.

3. In the Virtual IP Address to Use for Authentication field, *1.2.3.5* displays by default. If using Tier 1 or Tier 3, enter the IP address that from now on will be used for communicating authentication information between the R3000 and the PDC. This must be an IP address that is not being used, on the same segment of the network as the R3000.



**WARNING**: If the IP address entered here is not in the same subnet as this R3000, the net use connection will fail.

- 4. From the **NIC Device to Use for Authentication** pulldown menu:
  - if using the invisible mode, select "LAN2" for sending traffic on the network—in particular, for transferring authentication data.
  - if using the router or firewall mode, select "LAN1".
- 5. Click Apply to apply your settings.

**NOTE**: If using the NT authentication method, you will later return to this window to join the domain. See the section on Join the NT domain in Chapter 3: NT Authentication Setup for information about these procedures.

### Create an SSL certificate

Authentication SSL Certificate should be used if Web-based authentication will be deployed on the R3000 server. Using this feature, a Secured Sockets Layer (SSL) self-signed certificate is created and placed on client machines so that the R3000 will be recognized as a valid server with which they can communicate.

Click Authentication and select Authentication SSL Certificate from the pop-up menu to display the Authentication SSL Certificate window:

8e6 R3000 Enterprise Filt
System Cortrol Network Advinistrator Diagnostics Alert Patch Synchronization Nick Mode Sufferification Nick Mode Configuration Configur
Host Name: logo.com IP: 200.10.100.75 Version: R3000 Enterprise Filter 1.10.00.24 Java Applet Window

Fig. 2-7 Authentication SSL Certificate window

This window is comprised of three tabs: Self Signed Certificate, Third Party Certificate, and Download/View/Delete Certificate. These tabs are used to create, view, and/or delete self-signed or third party SSL certificates.

#### Create, Download a Self-Signed Certificate

- 1. On the Self Signed Certificate tab, click **Create Self Signed Certificate** to generate the SSL certificate.
- 2. Click the Download/View/Delete Certificate tab:

R3000 Enterprise Filter							<u> </u>
8e6r3000					1	nterprise	Filter
	System> The R300 Authentid the R300 possibly a Self Sign Click Dow workstat workstat Click Dele DNS nam	Authenticati 10 uses a SSL c ation. After cr 0 should not be added to each ed Certificate ed Certificate ion. This will all ions. ete Certificate I e of the R3000 ificate or CSR 4	ertificate to secure eating a self-signed changed. If the Di client workstation's Third Party Certific rtificate to save a c ow you to obtain th co erase the R3000' has changed. Afte	n SSL Certificate Its communications will certificate or a Certifi Sonane changes, ar trusted certificate list ate Download/View opy of the R3000's cu e R3000's certificate s current SSL certificate r deleting the current workstation that w	HELP th clients for W icate Request new certificate //Delete Certific mrent SSL certi so you can dist te. This should certificate, yo	QUIT Veb-based (CSR), the DNS must be created ate ficate file to your ribute it to clien Use done ONLY u will need to cr	iname of dand ur it if the reate a
<b>4</b>							
Host Name: logo.com	,	IP	200.10.100.75	Version: R3000 I	Enterprise Filte	r 1.10.00.24	

Fig. 2-8 Download/View/Delete Certificate tab

 Click Download/View Certificate to open the File Download dialog box where you indicate whether you wish to Open and view the file, or open the Save As window so that you can Save the SSL certificate to a specified folder on your workstation.

**NOTE**: While the SSL certificate can be downloaded on a Macintosh computer, the best method to import the certificate is via the Authentication Request Form, when prompted by the Security Alert warning message to add the certificate to the trusted certificate store.

Once the certificate is saved to your workstation, it can be distributed to client workstations for users who need to be authenticated.



**TIP**: Click **Delete Certificate** to remove the certificate from the server.

#### Create, Upload a Third Party Certificate

#### **Create a Third Party Certificate**

1. Click the Third Party Certificate tab:



Fig. 2-9 Third Party Certificate tab



**NOTE**: If a third party certificate has not yet been created, the Create CSR button is the only button activated on this tab.

2. Click **Create CSR** to open the Create CSR pop-up window:

Create CSR	×
Common Name (Host Name)	R3000LDAP-ota
Email Address	pjohnson@logo.com
Organization	LOGO
Organization Unit	Inc.
Locality	Orange
State or Province	California
Country (2 character country code	e)US
Create	Cancel
Java Applet Window	

Fig. 2-10 Create CSR pop-up window

The **Common Name (Host Name)** field should automatically be populated with the host name. This field can be edited, if necessary.

- 3. Enter your Email Address.
- 4. Enter the name of your **Organization**, such as **8e6** *Technologies*.
- 5. Enter an **Organizational Unit** code set up on your server, such as *Corp*.
- 6. Enter **Locality** information such as the name of your city or principality.
- 7. Enter the **State or Province** name in its entirety, such as *California*.
- 8. Enter the two-character **Country** code, such as **US**.
- 9. Click Create to generate the Certificate Signing Request.

NOTE: Once the third party certificate has been created, the Create CSR button displays greyed-out and the Download/View CSR, Upload Certificate, Delete CSR buttons are now activated.

#### **Upload a Third Party Certificate**

1. Click **Upload Certificate** to open the Upload Signed SSL Certificate for R3000 pop-up window:

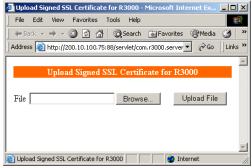


Fig. 2-11 Upload Signed SSL Certificate box

The Message dialog box also opens with the message: "Click OK when upload completes."



- TIP: Click Cancel in the dialog box to cancel the procedure.
- 2. In the Upload Signed SSL Certficate for R3000 pop-up window, click **Browse** to open the Choose file window.
- 3. Select the file to be uploaded.
- 4. Click Upload File to upload this file to the R3000.
- 5. Click **OK** in the Message dialog box to confirm the upload and to close the dialog box.

#### **Download a Third Party Certificate**

 In the Authentication SSL Certificate window, click Download/View CSR to open a pop-up window containing the contents of the certificate request:

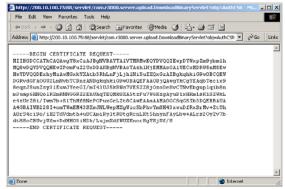


Fig. 2-12 Download CSR pop-up window

2. Click the "X" in the upper right corner of the window to close it.



TIP: Click Delete CSR to remove the certificate from the server.

## View log results

Use the View Log File window if you need to troubleshoot any problems with the authentication setup process.

1. Click Diagnostics and select View Log File from the popup menu to display the View Log File window:

駦 R3000 Enterprise Filter					
	YSTEM GROUP	LIBRARY	REPORTING	Enterpris	e Filter
System Control Hetwork Administrator Dismostics Alert Patch Synchronization Mode Authentication MIC Mode Backup/Restore Realus Authentication Setting SWMP Hardware Failure Detection X Strikes Blocking Customization	View Log File System>Diagnostic Log File Details Log File Last Number of Lines	S>View Log File Wbwatch Log (wbw 100 •			
Host Name: logo.com		IP: 200.10.100.75	Version: R3000 En	terprise Filter 1.10.00.24	
Java Applet Window					

Fig. 2-13 View Log File window

**NOTE**: In this user guide, only authentication-related options will be addressed. For information about all other options, see the View Log File window in the R3000 User Guide.

- 2. In the Log File Details frame, select the type of Log File to view:
  - "User Name Log (usage.log)" used for viewing the time and date a user logged on and off the network, along with the user's profile information.
  - "Wbwatch Log (wbwatch.log)" used for viewing messages on attempts to join the domain via the Authentication Settings window.
  - "Authentication Log (AuthenticationServer.log)" used for viewing information about the authentication process for users, including SEVERE and WARNING error messages.
  - "Admin GUI Server Log (AdminGUIServer.log)" used for viewing information on entries made by the administrator in the console.
  - "eDirectory Agent Debug Log (edirAgent.log)" used for viewing the debug log, if using eDirectory LDAP authentication.
  - "eDirectory Agent Event Log (edirEvent.log)" used for viewing the event log, if using eDirectory LDAP authentication.
  - "Authentication Module Log (authmodule.log)" used for viewing information about SEVERE error messages pertaining to LDAP authentication connection attempts.
- 3. Choose the **Last Number of Lines** to view (100-500) from that file.

4. Click **View** to display results in the Result pop-up window:

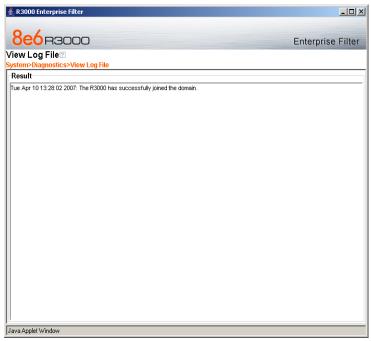


Fig. 2-14 View Log File Result pop-up window

5. Click the "X" in the upper right corner of the pop-up window to close it.

## Specify block page settings

Click Control and select Block Page Authentication from the pop-up menu to display the Block Page Authentication window:

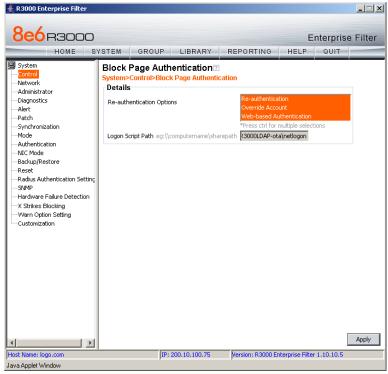


Fig. 2-15 Block Page Authentication window

#### **Block Page Authentication**

- 1. In the **Re-authentication Options** field of the Details frame, all block page options are selected by default, except for Web-based Authentication. Choose from the following options by clicking your selection:
  - Web-based Authentication select this option if using Web authentication with time-based profiles or persistent login connections for NT or LDAP authentication methods.
  - **Re-authentication** select this option for the reauthentication option. The user can restore his/her profile and NET USE connection by clicking an icon in a window to run a NET USE script.
  - Override Account select this option if any user has an Override Account, allowing him/her to access URLs set up to be blocked at the global or IP group level.

**TIP**: Multiple options can be selected by clicking each option while pressing the Ctrl key on your keyboard.



**NOTE**: See the R3000 User Guide for information about the Override Account feature.

- 2. If the "Re-authentication" option was selected, in the Logon Script Path field, \\PDCSHARE\scripts displays by default. In this field, enter the path of the logon script that the R3000 will use when re-authenticating users on the network, in the event that a user's machine loses its connection with the server, or if the server is rebooted. This format requires the entry of two backslashes, the authentication server's computer name (or computer IP address) in capital letters, a backslash, and name of the share path.
- 3. Click Apply to apply your settings.

### **Block page**

When a user attempts to access Internet content set up to be blocked, the block page displays on the user's screen:

🗿 8e6 R3000 - Microsoft Inl	ternet Explor	er					
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorite	es <u>T</u> ools <u>H</u> e	lp					
← Back • ⇒ • 🔕 👔	삶 🔍 Sear	ch 👔 Favorites	History	B- 🎒	<b>W</b> • E		
Address 🙋 w.coors.com/&IP-	=200.10.100.75	5:81&CAT=ALCO&	USER=LOGO\I	Domain%20Ad	mins\GLANG	→  ∂	Links
,						_	12
		ACCESS D	ENIED!			HE	LP
Internet access to		ed website has anization's Inte			on your use	er profile	
User/Machine: LO		nins\GLANG					
	0.10.101.140						
Category: Alc Requested URL: http://www.category.com/ Reguested URL: http://reguested/ Reguested URL: http://reguested/ Reguested URL: http://reguested/ Reguested URL: http://reguested/ Reguested URL: http://reguested/ Reguested URL: http://reguested/ Reguested URL: http://reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reguested/ Reg							
Requested on . This	J. // W W W COOLS	.com/					
	-	or further optior	a lisk borg				
To submit this bloc	ked site for r	eview, <u>click here</u>	. For assista	Ince, contact	-		
8e6 R3000 Inter	met filtering pro	vided by <u>8e6 Tech</u>	nologies. Copy	right 2003. Al	l rights reserv	ed.	

Fig. 2-16 Block page

**NOTES**: See Block Page Customization for information on adding free form text and a hyperlink at the top of the block page. Appendix C: Create a Custom Block Page from the R3000 User Guide for information on creating a customized block page using your own design.

#### **User/Machine frame**

By default, the following data displays in the User/Machine frame:

- **User/Machine** field The username displays for the NT/ LDAP user. This field is blank for the IP group user.
- IP field The user's IP address displays.
- **Category** field The name of the library category that blocked the user's access to the URL displays. If the content the user attempted to access is blocked by an Exception URL, "Exception" displays instead of the library category name.
- **Blocked URL** field The URL the user attempted to access displays.

#### Standard Links

By default, the following standard links are included in the block page:

- **HELP** Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** Clicking this link takes the user to 8e6's Web site.

### **Optional Links**

By default, these links are included in the block page under the following conditions:

- For further options, <u>click here</u>. This phrase and link is included if any option was selected at the Re-authentication Options field in the Block Page Authentication window. Clicking this link takes the user to the Options window, described in the Options page sub-section that follows.
- To submit this blocked site for review, <u>click here</u>. -This phrase and link is included if an email address was entered in the Submission Email Address field in the Common Customization window. Clicking this link launches the user's default email client. In the composition window, the email address from the Submission Email Address field populates the "To" field. The user's message is submitted to the global administrator.

#### **Options page**

The Options page displays when the user clicks the following link in the block page: **For further options**, <u>click</u> <u>here</u>.

🎒 8e6 R3000 - Microsoft Internet Explorer	_ 🗆 🗙
<u>File Edit Vi</u> ew F <u>a</u> vorites <u>I</u> ools <u>H</u> elp	1
🗢 Back 🔹 🤿 🗸 🔯 🖓 🕼 😡 Search 📓 Favorites 🖓 History 🛛 🖏 🚽 🗐 🗸 🗐	
Address 🕖 http://200.10.100.75:81/cgi/block.cgi 🗾 🧭	Go Links »
	<u> </u>
OPTIONS	HELP
User/Machine: LOGO/Domain Admins/GLANG IP: 200.10.101.140	
Category: Alcohol	
Requested URL: http://www.coors.com/	
Option 1: <u>Click here</u> for secure Web-based authentication.	
Option 2: If the above profile is incorrect or there has been an error, you can:	
Re-start your system and re-login or	
<ul> <li>Try re-authenticating your user profile</li> </ul>	
Option 3: If you have an override account, enter your username and password.	
Username:	
Password: Override	
Warning! The override account option will not function if anti-popup software is installed on	
your system.	
	~
Done	

Fig. 2-17 Options page

The following items previously described for the Block page display in the upper half of the Options page:

- BACK and HELP links
- User/Machine frame contents

The frame beneath the User/Machine frame includes information for options (1, 2, and/or 3) based on settings made in the Block Page Authentication window.

#### **Option 1**

Option 1 is included in the Options page if "Web-based Authentication" was selected at the Re-authentication Options field in the Block Page Authentication window. The following phrase/link displays:

Click here for secure Web-based authentication.

When the user clicks the link, the Authentication Request Form opens:

File Edit View Favorites	ation - Microsoft Internet Explorer		_1	
				ľ
	🖞 🖏 Search 😩 Favorites 🎯 History 🛛 🖓 🔤 📄		_	
Address (2) https://r3000a.gc.	local:8081/AuthenticationServer/AuthenticationForm.jsp?URL=192.168.20.10/index.htm8dP=192.1	168.20.008CAT-SPORTSBUSER-DEFAULT	• 6	>0
	WEB ACCESS AUTHENTICATION	HELP		
	Please log in to access the Internet.			
	Authentication Login			
	Username: tjones			
	Password: Annual			
	Domain Novell (LDAP)			
	Alias QC_Server			
	Log In			
	Be6 R3000 Internet filtering provided by Be6 Technologies, Copyright 2005. All right	ts reserved.		

Fig. 2-18 Authentication Request Form



**NOTE:** See Authentication Form Customization for information on adding free form text and a hyperlink at the top of the Authentication Request Form.

#### **Option 2**

The following phrase/link displays, based on options selected at the Re-authentication Options field in the Block Page Authentication window:

- **Re-start your system and re-login** This phrase displays for Option 1, whether or not either of the Reauthentication Options (Re-authentication, or Webbased Authentication) was selected in the Block Page Authentication window. If the user believes he/she was incorrectly blocked from a specified site or service, he/ she should re-start his/her machine and log back in.
- <u>Try re-authenticating your user profile</u> This link displays if "Re-authentication" was selected at the Reauthentication Options field, and an entry was made in the Logon Script Path field. When the user clicks this link, a window opens:

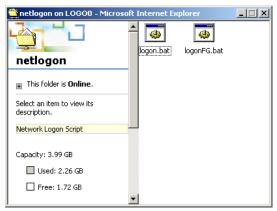


Fig. 2-19 Re-authentication option

The user should click the **logon.bat** icon to run a script that will re-authenticate his/her profile on the network.

#### **Option 3**

Option 3 is included in the Options page, if "Override Account" was selected at the Re-authentication Options field in the Block Page Authentication window.

This option is used by any user who has an override account set up for him/her by the global group administrator or the group administrator. An override account allows the user to access Internet content blocked at the global or IP sub-group level.

The user should enter his/her **Username** and **Password**, and then click **Override** to open the Profile Control window. This window must be left open throughout the user's session in order for the user to be able to access blocked Internet content.



**NOTES**: See Appendix F: Override Pop-up Blockers for information on how a user with an override account can authenticate if a pop-up blocker is installed on his/her workstation.

See the R3000 User Guide for information about the Override Account feature.

### **Common Customization**

Common Customization lets you specify elements to be included in block pages and/or the authentication request form end users will see.

Click Customization and then select Common Customization from the pop-up menu to display the Common Customization window:

	SYSTEM GROUP	LIBRARY	REPORTING	Enterpris	ie i niei
System Control Network Administrator	Common Custo System>Customizat Details	omization 2 ion>Common Cust			
Diagnostics Alert Patch	Username Display IP Address Display	⊙ On ⊙ On		C Off C Off	
Synchronization Mode Authentication	Category Display Blocked URL Display	© On ⊙ On		C off C off	
NIC Mode Backup/Restore Reset	Copyright Display Title Display	⊙ On ⊙ On		C off C off	
Radius Authentication Setting SNMP Hardware Failure Detection X Strikes Blocking	Help Display Help Link Text	⊙ On HELP		C off	
	Help Link URL Submission Review Di	splay 💿 On	www.8e6.com/techsupp Dcompany.com	O Off	nl

Fig. 2-20 Common Customization window

By default, in the Details frame all elements are selected to display in the HTML pages, the Help link points to the FAQs page on 8e6's public site that explains why access was denied, and a sample email address is included for administrator contact information. These details can be modified, as necessary.

### Enable, disable features

- 1. Click "On" or "Off" to enable or disable the following elements in the HTML pages, and make entries in fields to display customized text, if necessary:
  - Username Display if enabled, displays "User/ Machine" followed by the end user's username in block pages
  - IP Address Display if enabled, displays "IP" followed by the end user's IP address in block pages
  - Category Display if enabled, displays "Category" followed by the long name of the blocked category in block pages
  - Blocked URL Display if enabled, displays "Blocked URL" followed by the blocked URL in block pages
  - Copyright Display if enabled, displays 8e6 R3000 copyright information at the footer of block pages and the authentication request form
  - Title Display if enabled, displays the title of the page in the title bar of the block pages and the authentication request form
  - Help Display if enabled, displays the specified help link text in block pages and the authentication request form. The associated URL (specified in the Help Link URL field described below) is accessible to the end user by clicking the help link.



**NOTE**: If enabling the Help Display feature, both the Help Link Text and Help Link URL fields must be populated.

• Help Link Text - By default, *HELP* displays as the help link text. Enter the text to display for the help link.

- Help Link URL By default, http://www.8e6.com/techsupport/deniedresponse.html displays as the help link URL. Enter the URL to be used when the end user clicks the help link text (specified in the Help Link Text field).
- Submission Review Display if enabled, displays in block pages the email address of the administrator to receive requests for a review on sites the end users feel are incorrectly blocked. The associated email address (specified in the Submission Email Address field described below) is accessible to the end user by clicking the <u>click here</u> link.



**NOTE**: If enabling the Submission Review Display feature, an email address entry of the designated administrator in your organization must be made in the Submission Email Address field.

- Submission Email Address By default, admin @company.com displays in block pages as the email address of the administrator to receive feedback on content the end user feels has been incorrectly blocked. Enter the global administrator's email address.
- 2. Click Apply to save your entries.



TIP: Click Restore Default to revert to the default settings.

### **Authentication Form Customization**

To customize the Authentication Request Form, click Customization and select Authentication Form from the pop-up menu:

駦 R3000 Enterprise Filter				
	STEM GROU	JP LIBRARY	REPORTING H	Enterprise Filter
System Control Network dministrator	System>Customiz Details	n Form Customiz ation>Authentication I	Form Customization	
Diagnostics Alert Patch Synchronization Mode Authentication NIC Mode	Header Description		S AUTHENTICATION	
Backup/Restore     Backup/Restore     Reset     Radius Authentication Setting     SNMP     Hardware Failure Detection     X Strikes Blocking     Warn Option Setting     Oustomization	Link Text Link URL			
4			Restore Default	Preview Apply
Host Name: logo.com		IP: 200.10.100.75	Version: R3000 Enterpr	ise Filter 1.10.00.24
Java Applet Window				

Fig. 2-21 Authentication Form Customization window



**NOTE**: This window is activated only if Authentication is enabled via System > Authentication > Enable/Disable Authentication, and Web-based Authentication is specified.

**TIP**: An entry in any of the fields in this window is optional, but if an entry is made in the Link Text field, a corresponding entry must also be made in the Link URL field.

- 1. Make an entry in any of the following fields:
  - In the **Header** field, enter a static header to be displayed at the top of the Authentication Request Form.
  - In the **Description** field, enter a static text message to be displayed beneath the Authentication Request Form header.
  - In the Link Text field, enter text for the link's URL to be displayed beneath the Description in the Authentication Request Form, and in the Link URL field, enter the corresponding hyperlink in plain text using the http:// or https:// syntax.

Any entries made in these fields will display centered in the Authentication Request Form, using the Arial font type.

2. Click Apply.

**TIP**: Click **Restore Default** to revert to the default text in this window.

#### **Preview sample Authentication Request Form**

1. Click **Preview** to launch a separate browser window containing a sample Authentication Request Form, based on entries saved in this window and in the Common Customization window:

🚰 Web Access Authentication - Microsoft Internet Explorer	_ <b>_</b> _×
File Edit View Favorites Tools Help	
← Back - → - ③ Ø 🏠 🖓 Search 📾 Favorites 🥮 Media 🎯 🛃 - 🎒 📰 📃	
Address 🕘 https://200.10.100.75:8081/AuthenticationServer/PreviewAuthenticationForm.jsp	▼ 🖓 Go 🛛 Links »
	<u>^</u>
WEB ACCESS AUTHENTICATION HELP	
Please log in to access the Internet	
Authentication Login	
Username :	
Password :	
Domain LOGSYS (NT) 💌	
Alias Disabled	
Log In	
8e6 R3000 Internet filtering provided by 8e6 Technologies. Copyright 2005. All rights reserved.	
	_
Done	internet
	111

Fig. 2-22 Sample Customized Authentication Request Form

By default, the following data displays in the frame:

- Username field The username displays.
- Password field The user's IP address displays.
- **Domain** field All LDAP domain names set up on the R3000 display in the pull-down menu.
- Alias field (optional) All alias names associated with the LDAP domain specified in the field above display in the pull-down menu, if the account names were entered for that LDAP domain.

By default, the following standard links are included in the Authentication Request Form:

- **HELP** Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** Clicking this link takes the user to 8e6's Web site.
- 2. Click the "X" in the upper right corner of the window to close the sample Authentication Request Form.

TIP: If necessary, make edits in the Authentication Form Customization window or the Common Customization window, and then click Preview in this window again to view a sample Authentication Request Form.

### **Block Page Customization**

To customize the block page, click Customization and select Block Page from the pop-up menu:

≜ R3000 Enterprise Filter							<u>_   ×</u>
	YSTEM	GROUP	LIBRARY	REPORTING	E	nterprise I	Filter
HOME S System Control Network Administrator Diagnostics Alert Patch Synchronization Mode Authentication NIC Mode Backup/Restore Reset Reset Reset Hardware Failure Detection X Strikes Blocking Warn Option Setting Distinuzation	Block P	age Custo ustomization	Somization Source Page C ACCESS D	ustomization	website has b	een denied base	ed on
I I I I I I I I I I I I I I I I I I I				Restore Def	ault Pr	eview A	pply
Host Name: logo.com		IP: 2	00.10.100.75	Version: R3000 Er	nterprise Filter	1.10.10.5	
Java Applet Window							

Fig. 2-23 Block Page Customization window



**NOTE**: See Appendix C: Create a Custom Block Page from the R3000 User Guide for information on creating a customized block page using your own design.

**TIP**: An entry in any of the fields in this window is optional, but if an entry is made in the Link Text field, a corresponding entry must also be made in the Link URL field.

- 1. Make an entry in any of the following fields:
  - In the **Header** field, enter a static header to be displayed at the top of the block page.
  - In the **Description** field, enter a static text message to be displayed beneath the block page header.
  - In the Link Text field, enter text for the link's URL to be displayed beneath the Description in the block page, and in the Link URL field, enter the corresponding hyperlink in plain text using the http:// or https:// syntax.

Any entries made in these fields will display centered in the customized block page, using the Arial font type.

2. Click Apply.

**TIP**: Click **Restore Default** to revert to the default text in this window.

### Preview sample block page

1. Click **Preview** to launch a separate browser window containing a sample customized block page, based on entries saved in this window and in the Common Customization window:

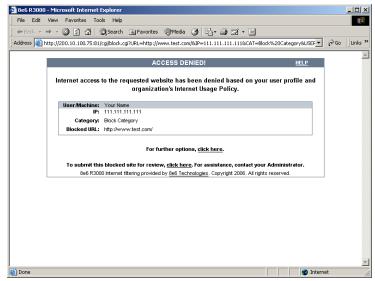


Fig. 2-24 Sample Customized Block Page

By default, the following data displays in the User/ Machine frame:

- User/Machine field The username displays for the NT/LDAP user. This field is blank for the IP group user.
- IP field The user's IP address displays.
- **Category** field The name of the library category that blocked the user's access to the URL displays. If the content the user attempted to access is blocked by an Exception URL, "Exception" displays instead of the library category name.
- **Blocked URL** field The URL the user attempted to access displays.

By default, the following standard links are included in the block page:

- **HELP** Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** Clicking this link takes the user to 8e6's Web site.

By default, these links are included in the block page under the following conditions:

- For further options, <u>click here</u>. This phrase and link is included if any option was selected at the Reauthentication Options field in the Block Page Authentication window. Clicking this link takes the user to the Options window, described in the Options page subsection.
- To submit this blocked site for review, <u>click here</u>. -This phrase and link is included if an email address was entered in the Submission Email Address field in the Common Customization window. Clicking this link launches the user's default email client. In the composition window, the email address from the Submission Email Address field populates the "To" field. The user's message is submitted to the global administrator.
- 2. Click the "X" in the upper right corner of the window to close the sample customized block page.

**TIP**: If necessary, make edits in the Block Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample block page.

# **CHAPTER 3: NT AUTHENTICATION SETUP**

**NOTE**: If you are running a Windows 2000 or Windows 2003 Server and are using the NTLM authentication protocol, then you need to make SMB Signing "not required." See Appendix B: Disable SMB Signing Requirements for steps on how to disable SMB Signing restrictions.

# Join the NT Domain

Click Authentication and select Authentication Settings from the pop-up menu to display the Authentication Settings window:

駦 R3000 Enterprise Filter							_ 🗆 🗙
	/STEM	GROUP LIBRARY	REPORT	ING HE		erprise QUIT	and the second se
HOME S	Authei System> The cur Setting R3000 N/ IP Addre: Virtual IP NIC Devic NIC Devic NIC Devic NIC Devic NIC Net PDC IP A Administr Administr	Authentication Settings Authentication>Authentication gs etBIOS Name: ss of WINS Server Address to Use for Authentication ce to Use for Authentication thentication Server Details Domain 300S Name	n Settings abled. 190.16 190.16 LAN2 QOOLA 2000.4 190.16 Admin ######	DAP-ota 30.240.4 30.250.5 DNATIVE 80.240.4 30.240.4 strator			Apply
Host Name: logo.com		IP: 200.10.100.75	Version: R	3000 Enterpris	Save	Join D	omain
Java Applet Window		,					

Fig. 3-1 Authentication Settings window

Information should only be entered in the NT Authentication Server Details frame if the R3000 will use the NT Authentication method to authenticate users.

٩

**NOTE**: The following Windows servers are supported by the current version of authentication: NT 4.0 SP4 or later, Mixed Mode 2000, and 2003. A Windows 2003 server may require changes to the default settings for SMB signing to allow communications.

The account that is provided for accessing the Windows server must have the administrative rights to add a machine account to the specified domain on the R3000. This requirement ensures the R3000 will be able to authenticate users from the Windows domain.

- 1. Enter the alphanumeric **Name of Domain** on which this server resides, using capital letters.
- 2. Using capital letters, enter up to 15 alphanumeric characters of the **PDC NetBIOS Name**, which is the computer name of the authentication server, or Primary Domain Controller.
- 3. Enter the **PDC IP Address**, which is the authentication server's IP address.
- 4. Enter the **Administrator Username** and **Administrator Password**. This account used for joining the domain must have administrator privileges.
- 5. Click **Join Domain** to save your entries and to submit a request for the R3000 to join the domain.

**TIP**: If entries in the NT Authentication Server Details frame are modified after joining the domain, you must join the domain again.

**NOTE**: Click **Save** if you are only pre-configuring the box. This option lets you save credentials without re-entering the information each time the domain is joined, or if the R3000 gets out of sync with the Primary Domain Controller.

# **Create an NT Domain**

After joining the domain, go to the Group section of the console and add an NT domain that contains entities to be authenticated.

### Add an NT domain

 Click NT in the navigation panel to open the pop-up menu, and select Add Domain to open the Create Domain Controller dialog box:

Create Domain Controller	×
Domain Name	QC
Domain Controller	2000adnative
IP Address	190.160.250.2
UserName	administrator
Password	*****
Confirm Password	*****
Apply	Cancel
Java Applet Window	

Fig. 3-2 Create Domain Controller

2. In the **Domain Name** field, enter the name of the domain on which the R3000 resides, using capital letters.



**NOTES**: The Domain Name must be the same name entered in the Authentication Settings window's Name of Domain field.

The alphanumeric NT domain name must be at least two characters but less than 64 characters in length, and can contain a hyphen (-) and underscore (\_), though the hyphen cannot be the first or last character of the name.

- 3. In the **Domain Controller** field, enter the name of the authentication server for the domain.
- 4. Enter the domain controller's IP Address.

- 5. In the **UserName** field, enter the username of the administrator.
- 6. Enter the password in the **Password** and **Confirm Password** fields.
- 7. Click **Apply** to add the domain to the tree.

### Refresh the NT branch

Click NT in the navigation panel to open the pop-up menu, and select **Refresh** whenever changes have been made in this branch of the tree.

### View or modify NT domain details

### **Domain Settings**

 Double-click NT in the navigation panel to open the NT branch of the Group tree. Select the NT domain you added, and choose Domain Details from the pop-up menu to display the default Settings tab of the NT Domain Details window:

駦 R3000 Enterprise Filter						<u>_</u> _×
8e6 R3000	YSTEM	GROUP	LIBRARY	REPORTING	E	nterprise Filter
Gorup ④ Gobal Group 원 교학 IP 금 용 NT ④ 공을 NOGSYS ④ 유 및 LOGSYS 문- 공을 LOAP	Settings Doma	Default Rule ) in Settings IT>QC>Domai Name er 255	2	QC 2000adnative 190.160.250 administrator	2	
	Passwor					Modify
Host Name: logo.com		IP:	200.10.100.75	Version: R3000 En	terprise Filte	r 1.10.00.24
Java Applet Window						

Fig. 3-3 NT Domain Details window, Settings tab

**NOTE**: To enter profile information for NT groups and users once domain settings are established, see Set up NT Domain Groups, Members.

- 2. For the Domain Settings:
  - The **Domain Name** entered in the Create Domain Controller dialog box displays greyed-out and cannot be modified.
  - The following fields can be modified: name of the domain Controller, IP Address, User Name, Password, and Confirm Password.

Whenever criteria on this tab is modified:

- a. The password from the Password field must be entered in the **Confirm Password** field for verification.
- b. Click Modify to apply your settings.

### **Default Rule**

1. Click the Default Rule tab to display the Default Rule settings of the NT Domain Details window:

駦 R3000 Enterprise Filter							_ 🗆 ×
8e6r3000	YSTEM	GROUP	LIBRARY	REPORTING	HELP	nterprise QUIT	e Filter
(2) Group - (2) Global Group 단 - 말 IP 	Defau	Default Rule     <b>t Rule</b>  2  T>QC>Default	Rule				
-	Default I Default I	Rule Redirect URL	6	le0 Minimum Filtering Default Block Page	Level	_	•
	Filter Op	tions		X Strikes Blocking Google/Yahoo! Safe Search Engine Keyw URL Keyword Filter	ord Filter Contro Control	bl	
Host Name: logo.com Java Applet Window		IP: 2	00.10.100.75	Version: R3000	Enterprise Filter	_	Modify

Fig. 3-4 NT Domain Details window, Default Rule tab

- 2. For the Default Rule:
  - "Rule0, the Minimum Filtering Level" displays by default as the **Default Rule**. If this rule is used, it will be applied to all groups and members in the NT domain without a filtering profile established.

- "Default Block Page" is selected by default as the Default Redirect URL. If the default block page is used, it will be applied to all groups and members in the NT domain without a filtering profile established. If "Custom URL" is selected, a URL must be entered in the corresponding text box.
- Filter Options that have been selected display check marks in corresponding checkboxes for "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".

Whenever criteria on this tab is modified, click **Modify** to apply your settings.

### Delete an NT domain

To delete a domain profile, choose Delete from the NT domain menu. This action removes the domain from the tree.

# Set up NT Domain Groups, Members

In the navigation panel, the NT domain branch of the tree menu includes options for setting up groups and/or members in the domain so that filtering profiles can later be created. The following options are used in this setup process: Select Group/Member from Domain, Set Group Priority, Manually Add Member, Manually Add Group, and Upload User/Group Profile.

### Add NT groups, members to the tree

Before you can create filtering profiles for groups and/or members in a domain, you must first add the groups and/or members to the tree list for that domain.

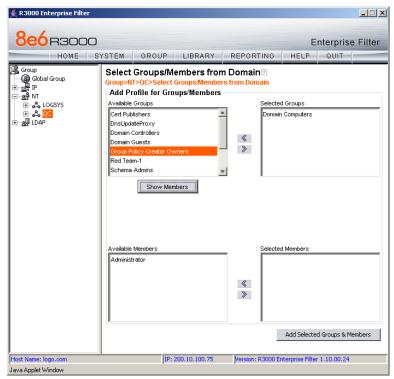


Fig. 3-5 Select Groups/Members from Domain window

Select the NT domain, and choose Select Group/Member from Domain from the pop-up menu to display the Select Groups/Members from Domain window (see Figure 3-5).

To add groups—that need filtering profiles—to the tree list:

- 1. Choose a group from the Available Groups list box.
- 2. Use the right arrow button (>) to move the group to the Selected Groups list box.

If necessary, select a group and use the left arrow button (<) to move the group back to the Available Groups list box.

To add group members—who need filtering profiles—to the tree list:

- 1. Choose the group from the Available Groups list box.
- 2. Click **Show Members** to display group members in the Available Members list box.
- 3. Choose a member from the Available Members list box, and use the right arrow button (>) to move the group to the Selected Members list box.

If necessary, select a member and use the left arrow button (<) to move the member back to the Available Members list box.

When all entities who need filtering profiles have been added to the selected Groups and/or Selected Members list box(es), click **Add Selected Groups & Members** to add them within the domain's section of the tree list.



**NOTE**: See Add or maintain an entity's profile under Create and Maintain NT Profiles for information on defining the filtering profile for the group. WARNING: When adding an NT group or member to the tree list, the group/member will be blocked from Internet access if the minimum filtering level has not been defined via the Minimum Filtering Level window. If you have just established the minimum filtering level, filter settings will not be effective until the group member/user logs off and back on the server. Refer to the R3000 User Guide for more information on the minimum filtering level.

# Specify a group's filtering profile priority

1. Select the NT domain, and choose Set Group Priority from the pop-up menu to display the Set Group Priority window:

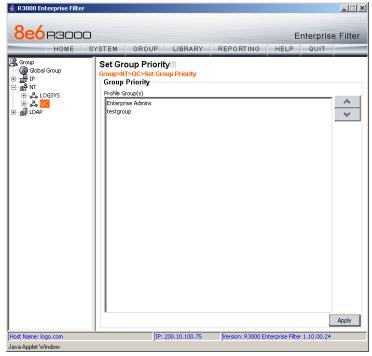


Fig. 3-6 Set Group Priority window

This window is used for designating which group profile will be assigned to a user when he/she logs in. If a user is a member of multiple groups, the one that is positioned highest in the list is applied.



**NOTES**: Groups automatically populate the Profile Group(s) list box, if these groups have one or more identical users and were added to the tree list via the Select Groups/Members from Domain window.

An entry for the Group Priority list is added to the end of the list when the group profile for that group is added to the R3000, and is removed automatically when you delete the profile.

- 2. To change the filtering priority of groups:
  - a. Select a group from the Profile Group(s) list box.
  - b. Use the up or down arrow button to move that group up or down in the list.
  - c. Click Apply to apply your settings.

### Manually add a user's name to the tree

1. Select the NT domain, and choose Manually Add Member from the pop-up menu to open the Manually Add Member dialog box:

Manually Add Member	×
Please enter the user name	_
OK Cancel	
Java Applet Window	

Fig. 3-7 Manually Add Member box

This dialog box is used for adding a username to the tree list, so that a filtering profile can be defined for that user.

2. Enter the username in the text box, up to 16 characters.

**TIP**: NT usernames should be entered without breaks or spaces. The first character must be a letter. The following ASCII characters can be used: "A-Z", "a-z", "0-9", "\_" (underscore), and "-" (hyphen).

Examples: TJONES JSmith Jane\_Doe Doe-John

- 3. Click **OK** to add the username to the domain's section of the tree.
- NOTE: See Add or maintain an entity's profile under Create and Maintain NT Profiles for information on defining the filtering profile for the user.

### Manually add a group's name to the tree

1. Select the NT domain, and choose Manually Add Group from the pop-up menu to open the Manually Add Group dialog box:

Manually Add Group	×
Please enter the group name	
OK Cancel	
Java Applet Window	

Fig. 3-8 Manually Add Group box

This dialog box is used for adding a group name to the tree list, so that a filtering profile can be defined for that group.

- 2. Enter the group's name in the text box.
- 3. Click **OK** to add the group name to the domain's section of the tree.



NOTE: See Add or maintain an entity's profile under Create and Maintain NT Profiles for information on defining the filtering profile for the group.

### Upload a file of filtering profiles to the tree

1. Select the NT domain, and choose Upload User/Group Profile from the pop-up menu to display the Upload User/ Group Profile window:



Fig. 3-9 Upload User/Group Profile window

This window is used for uploading a file to the tree with user or group names and their associated filtering profiles.

2. Click **Upload** to open the Upload Member Profile File pop-up window:

🚰 Upload Member Profile File - Microsoft Internet Explorer 📃 🔲
File Edit View Favorites Tools Help
🛛 🖛 Back 👻 🤿 🛛 🔯 🖄 🔯 Search 🕋 Favorites 🎯 Media 🥨
Address 🙆 http://200.10.100.75:88//R3000/servlet/com.r3000.se 💌 🔗 Go 🗍 Links
Upload Member Profile File
File Browse Upload File
🙋 Upload Member Profile File

Fig. 3-10 Upload Member Profile File window

- 3. Click Browse to open the Choose file window.
- 4. Select the file to be uploaded.

**WARNING**: Any file uploaded to the server will overwrite the existing user/group profile file.

Each user/group profile in the file uploaded to the server *must be* set up in a specified format in order for the profile to be activated on the server. This format differs depending on whether the profiles are user or group profiles. Based on the type of file format used, the file should have the following name:

- · ntuserprofile.conf if the file contains NT user profiles
- ntgroupprofile.conf if the file contains NT group profiles

1

**NOTE**: See Appendix E: User/Group File Format and Rules for examples of valid filtering profile formats to use when creating a list of profiles to be uploaded to the server.

∕

**WARNING**: When uploading a list of profiles to the tree list, the user will be blocked from Internet access if the minimum filtering level has not been defined via the Minimum Filtering Level window. If you have just established the minimum filtering level, filter settings will not be effective until the user logs off and back on the server. Refer to the R3000 User Guide for more information on the minimum filtering level.

- 5. Click **Upload File** to upload this file to the server. The Upload Successful pop-up window informs you to click Reload in order for these changes to be effective.
- 6. Click Reload.
- 7. Go to the NT branch of the tree, and choose **Refresh** from the NT group menu.

# **Create and Maintain NT Profiles**

Once an NT group or member has been added to the tree, a filtering profile can be created and maintained for that entity. For groups, the following options are available for filtering profile creation and maintenance: Group Member Details, Profile, and Remove. For members, the following options are available for filtering profile creation and maintenance: Profile, and Remove.

## Add an NT group, member to the tree list

Select the NT domain, and choose Group Member Details from the pop-up menu to display the Group/Member Details window:

🚖 R3000 Enterprise Filter							_ 🗆 🗙
8e6radoo	YSTEM	GROUP	LIBRARY	REPORTING	E	nterprise QUIT	e Filter
Group Gobal Group	Group>N Group Full Nat Domain Domain	Details me Type ember to Pr	orise Admins>Gr	oupMember Details			Add
Host Name: logo.com		IP	200.10.100.75	Version: R3000 Er	nterprise Filter	1.10.00.24	
Java Applet Window							

Fig. 3-11 Group/Member Details window

This window is used for viewing profile information about a group, and for adding members to a group.

In the Group Details frame, the following details display: **Group** name, **Domain** name, and **Domain Type**. Members that belong to the group display in the Members list box in the Add Member to Profile frame.

To add a member to the tree list so that a profile can be created for that member:

- 1. Select the entity from the Members list box.
- 2. Click Add.

### Add or maintain an entity's profile

Select the NT domain, and choose Profile from the pop-up menu to display the default Category tab of the Profile window:

8e6r3000	STEM GROUP LIBRARY REPORTI	NG	E HELP	nterpr	ise Filte
HUME S Group G Global Group G Global Group G Jar IP G ANT G A LOGSYS C A CC C	Category Redirect URL Filter Options Category Profile C Group>NT>QC>Enterprise Admins>Category Prof Group: Enterprise Admins Current Profile Minimum Filterin Available Filter Levels Rule0 Minimum Filtering Level	ile	Minim Child Po	rnograph	ering Leve / /t Content
	Category         Category Groups         Category Groups         Adult Content         Bandwidth         Disiness/investments         Courternit         Courternit         Courternit         Courternit         Courternit         Courternity/Organizations         Courternity         Courternity         Courternity         Courternity         Internet Productivity         Courternity         Courternity         Courternity         Courternity	Pass Pass P P P P P P P P P P P P P P P	Allow	Warn	Biock

Fig. 3-12 Group Profile window, Category tab

The Profile window is used for viewing/creating the filtering profile of the defined entity (group or member). Entries made in the Category, Redirect URL, and Filter Options tabs comprise the profile string for the entity.

#### **Category Profile**

Category Profile is used for creating the categories portion of the filtering profile for the entity.

**NOTE**: In order to use this tab, filtering rules should already have been set up via the Rules window, accessible from the Global Group options, and the minimum filtering level should already be established. The minimum filtering level is set up in the Minimum Filtering Level window, accessible from the Global Group options. See the R3000 User Guide for more information about these windows.

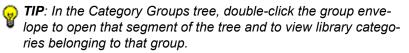
By default, "Rule0 Minimum Filtering Level" displays in the **Available Filter Levels** pull-down menu, and the Minimum Filtering Level box displays "Child Pornography" and Pornography/Adult Content". By default, **Uncategorized Sites** are allowed to Pass.



**NOTE**: By default, the Available Filter Levels pull-down menu also includes these three rule choices: Rule1 BYPASS", "Rule2 BLOCK Porn", "Rule3 Block IM and Porn", and "Rule4 8e6 CIPA Compliance".

To create the category portion of the entity's filtering profile:

 Select a filtering rule from the available choices in the Available Filter Levels pull-down menu. This action automatically populates the Pass, Allow, Warn, and/or Block columns in the Rule Details frame with filter settings for each category group/library category in the Category Groups tree.



**NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting.

- To change the filter setting for a category group/library category, double-click the column (Pass, Allow, Warn, Block) in the row corresponding to that category group/ library category to move the check mark to that column:
  - Pass URLs in this category will pass to the end user.
  - Allow URLs in this category will be added to the end user's white list.
  - Warn URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization's policies. The end user can view the URL after seeing a warning message and agreeing to its terms.
  - Block URLs in this category will be blocked.

**TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

- Click the "Pass" or "Block" radio button to specify whether all Uncategorized Sites should pass or be blocked.
- 4. Click **Apply** to apply your settings.

#### **Redirect URL**

Click the Redirect URL tab to display the Redirect URL page of the Profile window:

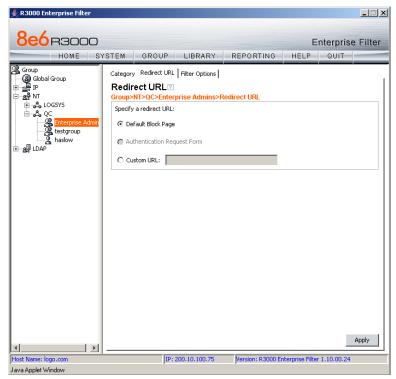


Fig. 3-13 Group Profile window, Redirect URL tab

Redirect URL is used for specifying the URL to be used for redirecting users who attempt to access a site or service set up to be blocked.

1. Specify the type of redirect URL to be used: "Default Block Page", or "Custom URL".

If "Custom URL" is selected, enter the redirect URL in the corresponding text box. Users will be redirected to the designated page at this URL instead of the block page.

2. Click **Apply** to apply your settings.

#### **Filter Options**

Click the Filter Options tab to display the Filter Options page of the Profile window:

👙 R3000 Enterprise Filter						
8e6r3000					E	nterprise Filter
HOME SY	STEM	GROUP	LIBRARY	REPORTING	HELP	QUIT
Group Goods Goods Group Goods Goods Group Goods Goods	Filter Group> Filter Sea Good Sea UR	Options trikes Blocking ogle/Yahoo! Safe arch Engine Keyw L Keyword Filter	Search Enforcem	ent		
						Apply
Host Name: logo.com		IP: 2	00.10.100.75	Version: R3000 E	nterprise Filter	1.10.00.24
Java Applet Window						

Fig. 3-14 Group Profile window, Filter Options tab

Filter Options is used for specifying which filter option(s) will be applied to the entity's filtering profile.

 Click the checkbox(es) corresponding to the option(s) to be applied to the filtering profile: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control". If URL Keyword Filter Control is selected, the "Extend URL Keyword Filter Control" option can be selected.



**NOTE**: See the R3000 User Guide for information about Filter Options.

2. Click Apply to apply your settings.

### Remove an entity's profile from the tree

To remove a group or member's profile from the tree, select the profile in order to open the pop-up menu, and choose Remove.

# **CHAPTER 4: LDAP AUTHENTICATION SETUP**

## **Create an LDAP Domain**

In the Group section of the console, add an LDAP domain that contains entities to be authenticated.

## Add the LDAP domain

 Click LDAP in the navigation panel to open the pop-up menu, and select Add Domain to open the Create LDAP Domain dialog box:

Create LDAP Domain	×
LDAP Server IP/Hostname	190.160.20.54
LDAP Server Port	389
LDAP Domain Label	TEST
Apply	Cancel
Java Applet Window	

Fig. 4-1 Create LDAP Domain box

- 2. In the **LDAP Server IP/Hostname** field, enter either the IP address or the hostname of the authentication server.
- 3. In the **LDAP Server Port** field, enter the LDAP server port number. By default, enter **389**.
- 4. In the **LDAP Domain Label** field, enter the name of the LDAP domain. This entry does not need to match the NetBIOS name.

٢

**NOTE**: The alphanumeric LDAP domain name must be at least two characters but less than 64 characters in length, and can contain a hyphen (-) and underscore (\_), though the hyphen cannot be the first or last character of the name. 5. Click **Apply** to add the domain to the tree. This action takes you directly to the LDAP domain window (see View, modify, enter LDAP domain details).

### Refresh the LDAP branch

Click LDAP in the navigation panel to open the pop-up menu, and select **Refresh** whenever changes have been made in this branch of the tree.

### View, modify, enter LDAP domain details

Double-click LDAP in the navigation panel to open the LDAP branch of the Group tree. Select the LDAP domain you added, and choose Domain Details from the pop-up menu to display the default Type tab of the LDAP Domain Details window:

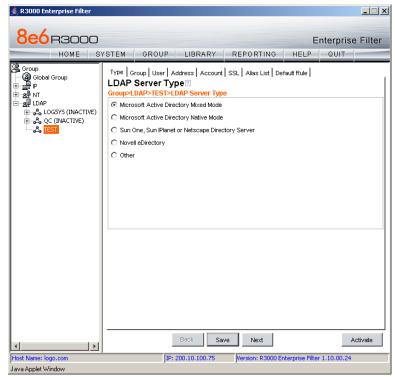


Fig. 4-2 Domain Details window, Type tab

The LDAP domain window is comprised of the following wizard tabs: Type, Group, User, Address, Account, SSL, Alias List, and Default Rule. By going through the entire wizard, domain details are established for the LDAP domain, preparing the LDAP domain for group and user filtering profile setup. After all entries are made on the wizard tabs, the domain can be activated.

WARNING: The instructions in this user guide have been documented based on standard default settings in LDAP for Microsoft Active Directory Services. The suggested entries and examples may not be applicable to all other server types, or if any changes have made to default settings on the LDAP Active Directory server.

#### LDAP Server Type

Based on the entries made when creating the LDAP domain, the R3000 will attempt to auto-detect the type of server being used, and if successfully detected, the appropriate LDAP Server Type radio button will be pre-selected on the Type tab.

 If making a selection on this tab, the following options are available: "Microsoft Active Directory Mixed Mode", "Microsoft Active Directory Native Mode", "Sun One, Sun IPlanet or Netscape Directory Server", "Novell eDirectory", and "Other". If the server type is not detected, "Other" will be selected.

The server type setting on this tab defines the content that displays on all other tabs of the wizard.



**NOTE**: If the server type is changed on this tab, object type settings will be overwritten with the new object type settings. User settings will not be modified.

- 2. If a selection was made on this tab, click **Save** to save your setting.
- 3. Click **Next** to go to the Group tab.

WARNING: The contents of the tabs for User and Group do not normally need to be changed. The settings on these tabs are made automatically when you select the server type at the beginning of the setup process. Unless you have made changes to the Schema of your LDAP server and are sure of the consequences of altering these settings, **do not** alter anything in these tabs. The only action you need to execute on these tabs is to confirm the settings by clicking the **Next** button at the bottom of the window, until you reach the Address tab.

#### **Group Objects**

The Group tab is used for including or excluding group objects in the LDAP domain.

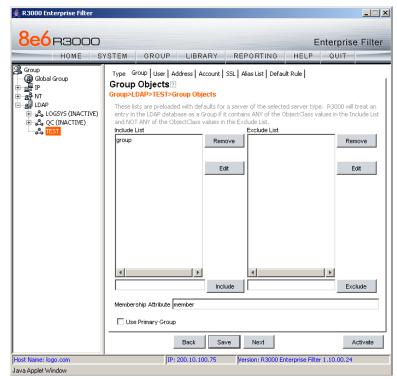


Fig. 4-3 Domain Details window, Group tab

By default, this tab is populated as follows:

- The **Include List** is populated with appropriate group objects, based on the server type.
- The **Membership Attribute** field is populated with the name of the LDAP attribute from the group record that identifies members of the group.
- 1. Generally, no action needs to be performed on this tab. However, under special circumstances, the following actions can be performed:
  - A group object can be added or excluded by making an entry in the appropriate field, and then clicking the **Include** or **Exclude** button.
  - A group object name can be edited by selecting the group object from the appropriate list box, editing the name in the field, and then clicking the **Edit** button.
  - A group object can be removed by selecting the group object and then clicking **Remove**.
- 2. Based on the selected server type, one of the following checkboxes is available for specifying a particular group profile assignment, if necessary:
  - If using Active Directory, the "Use Primary Group" checkbox displays on this tab. You may wish to check this box to indicate that profiles based on user groups should be assigned to users.
  - If using Novell eDirectory or Sun ONE, the "Use Dynamic Group" checkbox displays on this tab. You may wish to check this box to indicate that profiles based on dynamic groups should be assigned to users.
- 3. If any modifications were made on this tab, click **Save**.
- 4. Next to go to the User tab.

#### **User Objects**

The User tab is used for including or excluding user objects in the LDAP domain.

8e6r3000				Enter	prise Filter
HOME SY	STEM GR	OUP LIBRARY	REPORTING	HELP Q	UIT
Group - (응 Global Group) - 말 IP - 말 IDAP 태 - 소리 CGSYS (INACTIVE) 태 - 소리 CGSYS (INACTIVE) 태 - 소리 QC (INACTIVE)	User Objec Group>LDAP>T These lists are p entry in the LDA	ts TEST>User Objects preloaded with defaults f AP database as a User if f the ObjectClass values Re	t SSL Alias List Defau or a server of the selecte it contains ANY of the Ob in the Exclude List. Exclude List move Computer	ed server type, R30	
		Ir	ndude		Exclude
	Use Case-S	iensitive Comparison			
		Back	Save Next		Activate

Fig. 4-4 Domain Details window, User tab

By default, the Include List and Exclude List are populated with appropriate user objects, based on the server type.

- 1. Generally, no action needs to be performed on this tab. However, under special circumstances, the following actions can be performed:
  - A user object can be added or excluded by making an entry in the appropriate field, and then clicking the **Include** or **Exclude** button.

- A user object name can be edited by selecting the user object from the appropriate list box, editing the name in the field, and then clicking the **Edit** button.
- A user object can be removed by selecting the user object and then clicking **Remove**.
- If the user DN cannot be auto-detected during the profile setup process, click "Use Case-Sensitive Comparison" to perform a manual comparison check.
- 2. If any modifications were made on this tab, click **Save**.
- 3. Click **Next** to go to the Address tab.

#### Address Info

The LDAP domain address information populates the Address tab:

🚔 R3000 Enterprise Filter					<u>-</u> :×
8e6 R3000				E	nterprise Filter
HOME SY	STEM GROUP	LIBRARY	REPORTING	HELP	QUIT
응 Group - 영 Global Group 한 문화 IP 한 관화 NT - 소화 LOAP 한 국과 LOGSYS (INACTIVE) 한 국과 QC (INACTIVE)	Type Group User A Address Info Group>LDAP>TEST>A Server DNS Name			ault Rule	
	Server IP Address DNS Domain Name	190.160.20.54			
	NETBIOS Domain Name				
	Server LDAPS Port	636			
	Server LDAP Port	389			
	LDAP Query Base	DC=qc2domain,D	C=local		
		Back Sav	e Next		Activate
Host Name: logo.com	IP:	200.10.100.75	Version: R3000	Enterprise Filter	1.10.00.24
Java Applet Window					

Fig. 4-5 Domain Details window, Address tab

**NOTE**: If the DNS settings are not published in the LDAP directory, the Server DNS Name, DNS Domain Name, and LDAP Query Base fields will not be populated automatically. Functioning forward and reverse DNS name resolution is one of the requirements for LDAP authentication. Please ensure the correct DNS settings are set.

- 1. This tab includes the following fields, some pre-populated by default, and some that you may wish to edit:
  - The **Server DNS Name** field should contain the DNS name of the server. If this field is already populated, it may need to be edited if there is more than one DNS server available.

**NOTES**: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

If using a Novell server, be sure the Server DNS Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- The **Server IP Address** that displays by default is the one that was entered in the LDAP Server IP field of the Create LDAP Domain dialog box.
- The DNS Domain Name should be the DNS name of the LDAP domain, such as logo.com, and may need to be edited if the entire domain name does not display by default.

**NOTES**: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

If using a Novell server, be sure the DNS Domain Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- If necessary, the **NETBIOS Domain Name** can be entered.
- By default, 636 displays in the Server LDAPS Port field.
- By default, the value that was entered in the LDAP Server Port field of the Create LDAP Domain dialog box displays in the **Server LDAP Port** field.

 By default, the LDAP Query Base displays the root of the LDAP database to query using the LDAP Syntax, e.g. DC=domain,DC=com, or o=server-org. The entry in this field is case sensitive and should be edited, if necessary.

If this field is not populated, enter the LDAP query base.

- 2. If any modifications were made on this tab, click Save.
- 3. Click **Next** to go to the Account tab.

#### Account Info

The Account Info tab is used for specifying the account information needed for binding to the LDAP database.

駦 R3000 Enterprise Filter	
	Enterprise Filter
응 Group - 영 Global Group - 영 Global Group - 영 IVT - 월 UDAP - 응 LOGSYS (INACTIVE) - 응 QC (INACTIVE) - 응 TEST	Type   Group   User   Address Account   SSL   Alias List   Default Rule   Account Info [2] Group>LDAP>TEST>Account Info
	Use Anonymous Bind       LDAP Account Name     n=Users,dc=qc2domain,dc=local       Password     *******       Confirm Password     *******
	Distinguished Name Auto Discovery A "distinguished name" (e.g.: CN=administrator, CN=users,DC=xyz,DC=com) must be entered in the "DDAP Account Name" box above. To find the "distinguished name" for a user, please click on the "Find Distinguished Name" Find Distinguished Name
Host Name: logo.com Java Applet Window	Back         Save         Next         Activate           IP: 200.10.100.75         Version: R3000 Enterprise Filter 1.10.00.24

Fig. 4-6 Domain Details window, Account tab

- 1. Do one of the following:
  - If your LDAP database does not require a username to be provided in order to bind to the LDAP database, click the "Use Anonymous Bind" checkbox to grey out the fields and Find Distinguished Name button in this tab.

 If you know the authorized user's full LDAP Distinguished Name, enter it in the LDAP Account Name field. For example, enter the entire string in a format such as:

cn=Administrator,cn=Users,dc=qc2domain,dc=local

or

cn=admin,o=logo-org

Then enter the password in the **Password** and **Confirm Password** fields.

 If you do not know the authorized user's full LDAP Distinguished Name, click Find Distinguished Name in the Distinguished Name Auto Discovery frame to open the Distinguished Name Auto Discovery pop-up box:

Distinguished Nam	e Auto Discovery		X
User Name			
Domain Name			
Password			
Confirm Password			
Find D	Distinguished Name	Cancel	
Java Applet Window			

Fig. 4-7 Distinguished Name Auto Discovery box

Make entries in the following fields:

- a. **User Name** administrator's user name (e.g. *administrator*).
- b. **Domain Name** name of the domain (e.g. *logo.com*). This field displays greyed out if it was already included on the Address Info tab.
- c. Password and Confirm Password.

Click **Find Distinguished Name** to perform the search for the LDAP Distinguished Name. If the administrator's user name and password are successfully retrieved, the pop-up box closes and the fields on this tab become populated with appropriate data.

2. Click Save to save your entries.

**NOTE**: Once the Distinguished Name and password are successfully saved on this tab, Distinguished Name Auto Discovery frame will no longer display at the bottom of this tab.

3. Click **Next** to go to the SSL tab.

#### **SSL** Settings

SSL settings should be made if your network requires a secure connection from the R3000 to the LDAP server.



Fig. 4-8 Domain Details window, SSL tab

**NOTE**: See Appendix C: Obtain, Export an SSL Certificate for information on how to obtain a Sun ONE server's SSL certificate, or how to export an Active Directory or Novell server's SSL certificate to your desktop and then upload it to the R3000.

 If applicable, click in the "Enable Secure LDAP over SSL" checkbox. This action activates the Upload buttons in the Manually Upload SSL Certificate for LDAPS frame and the Automatically Upload SSL Certificate for LDAPS frame.

- 2. To automatically upload an SSL certificate, go to the Automatically Upload SSL Certificate for LDAPS frame and do the following:
  - a. In the **Wait \_\_\_\_\_seconds for certificate** field, by default 3 displays. Enter the number of seconds to wait before the certificate is automatically uploaded.
  - b. Click Upload to upload the certificate.

To manually upload an SSL certificate, go to the Manually Upload SSL Certificate for LDAPS frame and do the following:

a. Click the **Upload** button to open the Upload SSL Certificate for LDAPS pop-up window:



Fig. 4-9 Upload SSL Certificate for LDAPS

- b. Click **Browse** to open the Choose file window and select the R3000 server's SSL certificate.
- c. Click **Upload File** to upload the SSL certificate to the R3000 server.

WARNING: If using a Novell server, be sure the name on the SSL certificate (to be uploaded to the server) matches the Server DNS Name entered in the Address Info tab.

- 3. Click Save.
- 4. Click Next to go to the Alias List tab.

#### Alias List

The Alias List will be automatically populated if the Account Name was entered in the Account tab. This list includes all alias names for the domain that will be included in the Alias pull-down menu in the Authentication Request Form.

			Enterprise
HOME SY	STEM GROUP	P LIBRARY REPORTING HEL	.P QUIT
up ) Global Group I IP NT LDAP 	Type   Group   User   Alias List Group>LDAP>TEST	Address   Account   SSL   <mark>Alias List  </mark> Default Rule   <mark>&gt;Alias List</mark>	
🖧 QC (INACTIVE)	Alias Name	LDAP Container Name	Alias Enabled
🖧 TEST	Builtin	CN=Builtin, DC=gc2domain, DC=local	
	Idapgroup	OU=ldapgroup.DC=gc2domain.DC=local	
	OCcontainer1000 M	OU=OCcontainer1000,OU=MasterContainer,D	N N
	QCcontainer1001_M	OU=QCcontainer1001,OU=MasterContainer,D	
	QCcontainer1002_M	OU=QCcontainer1002,OU=MasterContainer,D	
	QCcontainer1003_M	OU=QCcontainer1003,OU=MasterContainer,D	
	QCcontainer1004_M	OU=QCcontainer1004,OU=MasterContainer,D	
	QCcontainer1005_M	OU=QCcontainer1005,OU=MasterContainer,D	
	OCcontainer1006 M	OU=OCcontainer1006,OU=MasterContainer,D	
	QCcontainer1007_M	OU=QCcontainer1007,OU=MasterContainer,D	
	QCcontainer1008_M	OU=QCcontainer1008,OU=MasterContainer,D	
	QCcontainer1009_M	OU=QCcontainer1009,OU=MasterContainer,D	
	QCcontainer100_Ma.	OU=QCcontainer100,OU=MasterContainer,DC	. 🔽
	QCcontainer1010_M	OU=QCcontainer1010,OU=MasterContainer,D	
	QCcontainer1011_M	OU=QCcontainer1011,OU=MasterContainer,D	
	QCcontainer1012_M	OU=QCcontainer1012,OU=MasterContainer,D	
	QCcontainer1013_M	OU=QCcontainer1013,OU=MasterContainer,D	
	QCcontainer1014_M	OU=QCcontainer1014,OU=MasterContainer,D	
	QCcontainer1015_M	OU=QCcontainer1015,OU=MasterContainer,D	
	QCcontainer1016_M	OU=QCcontainer1016,OU=MasterContainer,D	
	QCcontainer1017_M	OU=QCcontainer1017,OU=MasterContainer,D	
	Reload OU List		Enable/Disable All

Fig. 4-10 Domain Details window, Alias List tab

However, if there are many alias names to be loaded, the tab initially displays without any data and the Search in Progress box opens:

Search in Progress	×
The LDAP server is returning a substantial amount of data.	
Please wait while the search is in progress.	
Java Applet Window	
Fig. 4.11 Search in Progress box	

Fig. 4-11 Search in Progress box

After the search is completed, the Search in Progress box closes, and the list displays the Alias Name and the corresponding LDAP Container Name.



NOTE: If the alias list does not display, double-check the settings on the other tabs and verify that all of your settings are correct.

- The following actions can be performed on this tab:
  - An Alias Name can be edited by double-clicking the Alias Name in the designated row, and then making your modifications.
  - If an Organizational Unit (OU) has been deleted from the LDAP directory but has already been added to the alias list, the list can be reloaded by clicking the **Reload OU List** button. When clicking this button, the Search in Progress box opens and the domain becomes inactive and will need to be reactivated.
  - By default, all items are selected for inclusion in the alias list, as indicated by a check mark in the Alias Enabled checkbox. To deselect an item, click the checkbox to remove the check mark.
  - To select or deselect all items in the list, click the Enable/Disable All button. This button lets you toggle between these two operations.
- 2. If any modifications were made on this tab, click **Save**.
- 3. Click **Next** to go to the Default Rule tab.

#### **Default Rule**

The Default Rule applies to any authenticated user in the LDAP domain who does not have a filtering profile.

🚔 R3000 Enterprise Filter	
	Enterprise Filter
Group Global Group ⊕ ∰ IP ⊕ & Al IDAP ⊕ & LOAP ⊕ & LOASYS (INACTIVE) ⊕ & QC (INACTIVE) ⊕ & QC (INACTIVE) ⊕ & STET	Type   Group   User   Address   Account   SSL   Alias List   Default Rule           Default Rule  2         Group-LDAP>TEST>Default Rule         Select one of the following as the default rule:         Rule 0: Minimum Filtering Level         Specify a redirect URL:         If Default Block Page         C Custom URL:         Filter Options:         If X Strikes Blocking         Google/Vahool Safe Search Enforcement         If Search Engine Keyword Filter Control         If URL Keyword Filter Control         Extend URL Keyword Filter Control         Backup Server Configurations:         Add       Modify         Default Save
Host Name: logo.com Java Applet Window	IP: 200.10.100.75 Version: R3000 Enterprise Filter 1.10.00.24

Fig. 4-12 Domain Details window, Default Rule tab

- 1. This tab is comprised of the following components that can be modified:
  - By default, "Rule0" is the default rule. This rule can be changed by making another selection from the pull-down menu.
  - To specify the type of redirect URL to be used for users who do not have a filtering profile, click the radio button corresponding to "Default Block Page", or "Custom URL".

If Custom URL is selected, enter the redirect URL in the text box.

- Click the checkbox(es) corresponding to the option(s) to be applied to the filtering profile: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control". If URL Keyword Filter Control is selected, the "Extend URL Keyword Filter Control" option can be selected.
- To specify a backup server for use with this LDAP server in the event the primary server cannot be accessed, see the setup instructions in LDAP Backup Server Configuration.

**NOTE:** If "Novell eDirectory" was selected for the LDAP Server Type, and the Novell eDirectory Agent option was enabled in the Enable/Disable Authentication window in the System section of the console, Novell eDirectory Agent Settings displays above the Backup Server Configurations buttons.

- 2. If any modifications were made on this tab, click Save.
- 3. After all entries have been made in these wizard tabs, click **Activate** to activate the domain.

**TIP**: After the domain is activated, whenever subsequent modifications are made in any of these wizard tabs, Activate must be clicked again to re-activate the domain.



**NOTE**: To enter profile information for LDAP groups and users, see Create, Maintain LDAP Profiles.

#### LDAP Backup Server Configuration

#### Configure a backup server

To add a backup server's settings:

1. Click **Add** to open the Backup Server Configuration wizard pop-up window:

Address Account S Address Info? Group>LDAP>TEST>/		
oroup come rearry	1001 033 1110	
Server DNS Name		
Server IP Address		
DNS Domain Name	qc2domain.local	
NETBIOS Domain Name		
Server LDAPS Port	636	
Server LDAP Port	389	
LDAP Query Base	DC=qc2domain,DC=local	
	k Save Next Close	

Fig. 4-13 Backup Server Configuration, Address Info

**NOTE**: The **Back** and **Save** buttons can be clicked at any time during the wizard setup process. Click **Close** to close the wizard pop-up window.

- 2. Enter, edit, or verify the following criteria:
  - Server DNS Name DNS name of the LDAP server, such as server.logo.local

**NOTES**: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

Be sure the Server DNS Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- Server IP Address IP address of the server, such as 100.10.150.30
- **DNS Domain Name** DNS name of the LDAP domain, such as logo.local



**NOTES**: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.

Be sure the DNS Domain Name exactly matches the name on the SSL certificate that will be uploaded to the server.

- NETBIOS Domain Name an entry in this field is optional
- Server LDAPS Port by default, 636 displays in this field
- Server LDAP Port by default, the value that was entered in the LDAP Server Port field of the Create LDAP Domain dialog box displays in the field
- LDAP Query Base root of the LDAP database to query using the LDAP Syntax, e.g. DC=domain,DC=com or o=server-org.

**TIP**: The entry in this field is case sensitive.

- 3. Click Save.
- 4. Click Next to go to the Account tab:

Backup Server Configuration	×
Address Account SSL Account Info Group>LDAP>TEST>Account Info	1
🗆 Use Anonymous Bind	
LDAP Account Name	Ш
Password	Ш
Confirm Password	Ш
Distinguished Name Auto Discovery A "distinguished name" (e.g.: CN=administrator, CN=users, DC=uyz, DC=com) must be entered in the "LDAP Account Name" biox above. To find the "distinguished name" for a user, please click on the "Ind Distinguished Name" button and enter the username (e.g.: Administrator), domain name (if needed), and password. Find Distinguished Name	
Back Save Next Close	1
Java Applet Window	

Fig. 4-14 Backup Server Configuration, Account Info

- 5. Enter, edit, or verify the following criteria:
  - "Use Anonymous Bind" click this checkbox to grey out the fields in this tab, if your LDAP database does not require a username to be provided in order to bind to the LDAP database
  - If you know the authorized user's full LDAP Distinguished Name:
    - a. Enter the authorized user's full LDAP Distinguished Name in the **LDAP Account Name** field.

For example:

```
cn=Administrator,cn=Users,dc=qc2domain,
dc=local
```

or

cn=admin,o=logo-org

b. Enter the password in the **Password** and **Confirm Password** fields.

- If you do not know the authorized user's full LDAP Distinguished Name:
  - a. Click **Find Distinguished Name** in the Distinguished Name Auto Discovery frame to open the Distinguished Name Auto Discovery pop-up box (see Fig. 4-8).
  - b. Enter the administrator's **User Name** (e.g. *administrator*).
  - c. Enter the **Domain Name** (e.g. *logo.com*). This field displays greyed out if it was already included on the Address Info tab.
  - d. Enter the password in the **Password** and **Confirm Password** fields.
  - e. Click **Find Distinguished Name** to perform the search for the LDAP Distinguished Name. If the administrator's user name and password are successfully retrieved, the pop-up box closes and the fields on this tab become populated with appropriate data.
- 6. Click Save to save your entries.

NOTE: Once the Distinguished Name and password are successfully saved on this tab, Distinguished Name Auto Discovery frame will no longer display at the bottom of this tab.

7. Click Next to go to the SSL tab:

ackup Server Configuration	×
Address Account SSL	
SSL Settings	
Group>LDAP>TEST>SSL Settings	
Enable Secure LDAP over SSL	
Manually Upload SSL Certificate for LDAPS	
Enter the path to the SSL certificate for your LDAP server. This certificate is	
required to communicate with your LDAP server with secure encryption. The certificate should be a Base64 encoded .der or .cer format SSL Certificate.	
Upload	
Automatically Upload SSL Certificate for LDAPS	
R3000 can automatically generate and upload SSL certificate for your LDAP server. Make sure secure LDAP is properly set up and the hostname you specified for your LDAP server is correct. Depending on the network environment, the time it takes to fetch the certificate can vary. You may wait up to 15 seconds.	
Upload Wait 3 seconds for certificate	
Back Save Next Close	
va Applet Window	

Fig. 4-15 Backup Server Configuration, SSL Settings

SSL settings should be made if your network requires a secure connection from the R3000 to the LDAP server.

**NOTE**: See Appendix C: Obtain, Export an SSL Certificate for information on how to export a server's SSL certficate to your desktop and then upload it to the R3000.

- a. If applicable, click in the "Enable Secure LDAP over SSL" checkbox. This action activates the Upload buttons in the Manually Upload SSL Certificate for LDAPS frame and the Automatically Upload SSL Certificate for LDAPS frame.
- b. To automatically upload an SSL certificate, go to the Automatically Upload SSL Certificate for LDAPS frame and do the following:
  - In the Wait \_\_\_\_\_ seconds for certificate field, by default 3 displays. Enter the number of seconds to wait before the certificate is automatically uploaded.
  - Click **Upload** to upload the certificate.

To manually upload an SSL certificate, go to the Manually Upload SSL Certificate for LDAPS frame and do the following:

- Click the Upload button to open the Upload SSL Certificate for LDAPS pop-up window (see Fig. 4-9).
- Click **Browse** to open the Choose file window and select the R3000 server's SSL certificate.
- Click **Upload File** to upload the SSL certificate to the R3000 server.

**WARNING**: Be sure the name on the SSL certificate (to be uploaded to the server) matches the Server DNS Name entered in the Address Info tab.

- 8. After all entries are made using the wizard, click **Save**.
- 9. Click **Close** to close the wizard pop-up window.

#### Modify a backup server's configuration

- 1. On the Default Rule tab, click **Modify** to open the Backup Server Configuration wizard pop-up window.
- 2. Click the tab(s) in which to make edits for the backup server: Address, Account, SSL.
- 3. Make the necessary edits.
- 4. Click Save.
- 5. Click Close to close the wizard pop-up window.

#### Delete a backup server's configuration

On the Default Rule tab, click **Delete** to remove the backup server's configuration.

### Delete a domain

To delete a domain profile, choose Delete from the LDAP domain menu. This action removes the domain from the tree.

## Set up LDAP Domain Groups, Members

In the navigation panel, the LDAP domain branch of the tree menu includes options for setting up groups and/or members in the domain so that filtering profiles can later be created. The following options are used in this setup process: Select Group/Member from Domain, Set Group Priority, Manually Add Member, Manually Add Group, and Upload User/Group Profile.

### Add LDAP groups, users to the tree

Before you can create filtering profiles for groups and/or members in a domain, you must first add the groups and/or members to the tree list for that domain.



Fig. 4-16 LDAP User/Group/Container Browser window

Select the LDAP domain, and choose Select Group/ Member from Domain from the pop-up menu to display the LDAP User/Group/Container Browser window (see Figure 4-16).

This window is used for retrieving the names of groups, users, or containers from an LDAP domain so that a filtering profile can be assigned.



**NOTES**: If the "Use Dynamic Group" option was specified in the Group tab of Domain Details, "Dynamic Group Enabled" displays towards the bottom left of this window.

See Appendix D: LDAP Server Customizations if using an OpenLDAP server.

#### Perform a basic search

- 1. Specify the type of search by clicking the "User", "Group", or "Container" radio button.
- If "User" or "Group" was selected, choose either "cn=" (common name) or "uid=" (user ID) from the pull-down menu for the attribute type used in the LDAP directory. This menu displays greyed-out if "Container" was selected.
- 3. In the input field that follows the pull-down menu, type in the group name, username, or container name exactly as it was entered on the LDAP server, or enter a partial name followed by the asterisk (\*) wildcard.
- 4. Make a selection from the **In** pull-down menu to specify the section of the server to search.
- Click Search to display rows of results in the grid below. The following information is included for each entity: Type (USR, GRP, CTR), Name (as entered on the LDAP server), DN string, Profile (Rule number, if assigned), View button, and Mark checkbox.

#### **Options for search results**

The following actions can be performed on search results:

- To narrow the number of records returned by your initial query, click the "Within Results" checkbox, modify your search criteria in the input field, and then click **Search**.
- To query either the list of groups in which a user is a member, or the list of users who are members of a Group Record, click the **View** button in the Members column to display the results in the grid.
- To select or deselect all records in the grid, click Mark/ Unmark All.
- To select or deselect all highlighted records in the grid, click Mark/Unmark Selected. This feature works only if records are first selected in the grid by clicking on them.
  - Multiple records are selected by clicking one record, and then pressing the **Ctrl** key on your keyboard and clicking another record.
  - A block of multiple records is selected by clicking the first record in the block, then pressing the **Shift** key on your keyboard, and then clicking the last record in the block.

### Apply a filtering rule to a profile

To apply a filtering rule to an entity in the grid:

- 1. Go to the Mark column and click the checkbox for that entity.
- 2. Select a filtering rule from the drop-down menu.
- 3. Click **Add Rule** to display the selected Rule number in the Profile column.

When the LDAP branch of the tree is refreshed, all entities with rules applied to them appear in the tree.

#### Delete a rule

To delete a rule from a profile, the entity must currently display in the grid and have a rule assigned to the profile.

- 1. Click the Mark checkbox for the entity.
- 2. Click **Delete Rule** to remove the entity's profile from the tree.

# Specify a group's filtering profile priority

1. Select the LDAP domain, and choose Set Group Priority from the pop-up menu to display the Set Group Priority window:

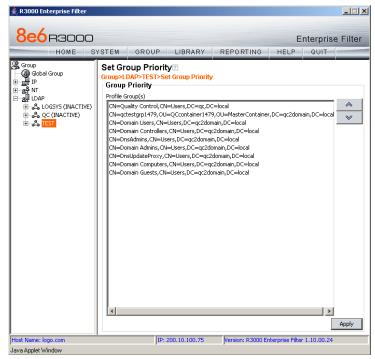


Fig. 4-17 Set Group Priority window

This window is used for designating which group profile will be assigned to a user when he/she logs in. If a user is a member of multiple groups, the one that is positioned highest in the list is applied. **NOTES**: Groups automatically populate the Profile Group(s) list box, if these groups have one or more identical users and were added to the tree list via the Select Groups/Members from Domain window.

An entry for the Group Priority list is added to the end of the list when the group profile for that group is added to the R3000, and is removed automatically when you delete the profile.

- 2. To change the order of groups in the list:
  - a. Select a group from the Profile Group(s) list box.
  - b. Use the up or down arrow button to move that group up or down in the list.
  - c. Click **Apply** to apply your settings.

#### Manually add a user's name to the tree

1. Select the LDAP domain, and choose Manually Add Member from the pop-up menu to open the Manually Add Member dialog box:

Manually Add Member	×
Please enter the user name	
OK Cancel	
Java Applet Window	

Fig. 4-18 Manually Add Member box

This dialog box is used for adding a username to the tree list, so that a filtering profile can be defined for that user.

2. Enter the username in the text box.



**TIP**: LDAP usernames should be input exactly as entered as entered for the LDAP Distinguished Name.

#### Examples:

CN=Jane Doe, CN=Users, DC=qc, DC=local CN=Public\, Joe Q., OU=Users, OU=Sales, DC=qc, DC=local CN=Doe\, John, CN=Users, DC=qc, DC=local cn=dyn-grp,ou=progrm,o=nwrd-org

3. Click **OK** to add the username to the domain's section of the tree.

**NOTE**: See Add or maintain an entity's profile under Create and Maintain LDAP Profiles for information on defining the filtering profile for the user.

### Manually add a group's name to the tree

1. Select the LDAP domain, and choose Manually Add Group from the pop-up menu to open the Manually Add Group dialog box:

Manually Add Group	×
Please enter the group name	
OK Cancel	
Java Applet Window	

Fig. 4-19 Manually Add Group box

This dialog box is used for adding a group name to the tree list, so that a filtering profile can be defined for that group.

- 2. Enter the group's name in the text box, using the entire Distinguished Name format.
- 3. Click **OK** to add the group name to the domain's section of the tree.

NOTE: See Add or maintain the entity's profile under Create and Maintain LDAP Profiles for information on defining the filtering profile for the group.

#### Upload a file of filtering profiles to the tree

 Select the LDAP domain, and choose Upload User/ Group Profile from the pop-up menu to open the Upload User/Group Profile window:

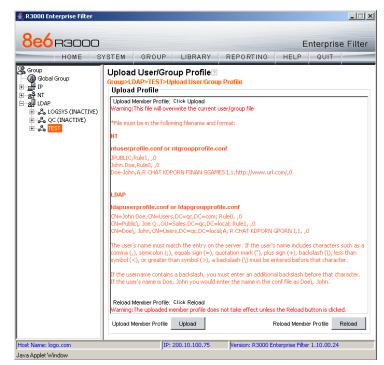


Fig. 4-20 Upload User/Group Profile window

This window is used for uploading a file to the tree with user or group names and their associated filtering profiles.

2. Click **Upload** to open the Upload Member Profile File pop-up window:

🖉 Upload Member Profile File - Microsoft Internet Explorer 📃 🔍
File Edit View Favorites Tools Help
← Back → → → 🙆 🛃 🚮 😡 Search 📾 Favorites 🎯 Media 🎯 👘 🎽
Address 🗃 http://200.10.100.75:88//R3000/servlet/com.r3000.se 💌 🄗 Go 🗍 Links »
Upload Member Profile File
File Browse Upload File
<u> </u>
🕲 Upload Member Profile File 🛛 👘 🔯 Internet 🏸

Fig. 4-21 Upload Member Profile File window

- 3. Click Browse to open the Choose file window.
- 4. Select the file to be uploaded.

**WARNING**: Any file uploaded to the server will overwrite the existing user/group profile file.

Each user/group profile in the file uploaded to the server *must be* set up in a specified format in order for the profile to be activated on the server. This format differs depending on whether the profiles are user or group profiles. Based on the type of file format used, the file should have the following name:

- Idapuserprofile.conf if the file contains LDAP user profiles
- Idapgroupprofile.conf if the file contains LDAP group profiles



**NOTE**: See Appendix E: User/Group File Format and Rules for examples of valid filtering profile formats to use when creating a list of profiles to be uploaded to the server.

WARNING: When uploading a list of profiles to the tree, the user will be blocked from Internet access if the minimum filtering level has not been defined via the Minimum Filtering Level window. If you have just established the minimum filtering level, filter settings will not be effective until the user logs off and back on the server.

- 5. Click **Upload File** to upload this file to the server. The Upload Successful pop-up window informs you to click Reload in order for these changes to be effective.
- 6. Click Reload.
- 7. Go to the LDAP branch of the tree, and choose **Refresh** from the LDAP group menu.

# **Create, Maintain LDAP Profiles**

Once an LDAP group, user member, or container has been added to the tree, a filtering profile can be created and maintained for that entity. For groups, the following options are available for filtering profile creation and maintenance: Group Member Details, Profile, and Remove. For users and containers, the following options are available for filtering profile creation and maintenance: Profile, and Remove.

# Add an LDAP group, member to the tree

Select the LDAP domain, and choose Group Member Details from the pop-up menu to display the Group/Member Details window:

👙 R3000 Enterprise Filter					_ 🗆 🗙
	YSTEM GRO	UP LIBRARY	REPORTING	E	nterprise Filter ฉบเา
Group Global Group B B B P B A A OC B Correst Correction	Group/Memb Group>NT>QC>EI Group Details Group Full Name Domain Domain Type Add Members Administrator	nterprise Admins>Gro	Enterprise Adr		Add
		10,000 10 100 75	Neurise - D2000 Fe	Lauranian Million	1 10 00 04
Host Name: logo.com Java Applet Window		IP: 200.10.100.75	Version: R3000 En	terprise Filter	1.10.00.24

Fig. 4-22 Group Member Details window

This window is used for viewing profile information about a group, and for adding members to a group.

In the Group Details frame, the following details display: **Group** name, **Full Name** (Distinguished Name) of the group, **Domain** name, and **Domain Type**. Members that belong to the group display in the Members list box in the Add Member to Profile frame.

To add a member to the tree list so that a profile can be created for that member:

- 1. Select the entity from the Members list box.
- 2. Click Add.

### Add or maintain an entity's profile

Select the LDAP domain, and choose Profile from the popup menu to display the default Category tab of the Profile window:

3e6 R3000					interpi	ise Fil
HOME S	YSTEM GROUP LIBRARY	REPORTIN	G	HELP	QUIT	
Group	Category Redirect URL Filter Options					
🚷 Global Group 💂 IP						
ଲୁଙ୍କ NT	Category Profile?	Cotoria Desella				
ar ⊞¦& LOGSYS	Group>NT>QC>Enterprise Admins> Group: Enterprise Admins Current Profil					
<u>⊨</u> & oc		e.wiiniinian riitening i	Level	Mission	um Eilte	ering Le
Enterprise Admin	Available Filter Levels				rnography	
🖓 testgroup	Rule0 Minimum Filtering Level 🔻				rnograpny aphy/Adu	
haslow				Fornogr	арпулчии	iii Coniterii
LDAP	Bule Details			·		
				-		
	Category		Pass	Allow	Warn	Block
	Category Groups					
	Adult Content					
	Bandwidth     Business/Investments		8			
	Community/Organizations		8			
	Contrainty/organizations     Custom Categories		ă			
	Education		Ø			
	🕀 🧰 Entertainment		$\overline{\mathbf{Q}}$			
	🗄 🚞 Government/Law/Politics					
	🕀 💼 Health/Fitness		$\odot$			
	Illegal/Questionable		8			
	Information Technology      Information Technology		8			
	Internet Communication      Internet Productivity		8			
	Internet/Intranet Misc.		ä			
			X			
	Uncategorized Sites	Block				

Fig. 4-23 Group Profile window, Category tab

The Profile option is used for viewing/creating the filtering profile of the defined entity (static or dynamic group, user member, or container). Entries made in the Category, Redirect URL, and Filter Options tabs comprise the profile string for the entity.

#### **Category Profile**

Category Profile is used for creating the categories portion of the filtering profile for the entity.



**NOTE**: In order to use this tab, filtering rules should already have been set up via the Rules window, accessible from the Global Group options, and the minimum filtering level should already be established. The minimum filtering level is set up in the Minimum Filtering Level window, accessible from the Global Group options.

By default, "Rule0 Minimum Filtering Level" displays in the **Available Filter Levels** pull-down menu, and the Minimum Filtering Level box displays "Child Pornography" and "Pornography/Adult Content". By default, **Uncategorized Sites** are allowed to Pass.



**NOTE**: By default, the Available Filter Levels pull-down menu also includes these three rule choices: Rule1 BYPASS", "Rule2 BLOCK Porn", "Rule3 Block IM and Porn", and "Rule4 8e6 CIPA Compliance".

To create the category portion of the entity's filtering profile:

 Select a filtering rule from the available choices in the Available Filter Levels pull-down menu. This action automatically populates the Pass, Allow, Warn, and/or Block columns in the Rule Details frame with filter settings for each category group/library category in the Category Groups tree.

**TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.

**NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting, since all library categories do not have the same filter setting.

- 2. To change the filter setting for a category group/library category, double-click the column (Pass, Allow, Warn, Block) in the row corresponding to that category group/ library category to move the check mark to that column:
  - Pass URLs in this category will pass to the end user.
  - Allow URLs in this category will be added to the end user's white list.
  - Warn URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization's policies. The end user can view the URL after seeing a warning message and agreeing to its terms.
  - Block URLs in this category will be blocked.

**TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

- Click the "Pass" or "Block" radio button to specify whether all Uncategorized Sites should pass or be blocked.
- 4. Click **Apply** to apply your settings at the entity's filtering level.

#### **Redirect URL**

Click the Redirect URL tab to display the Redirect URL page of the Profile window:

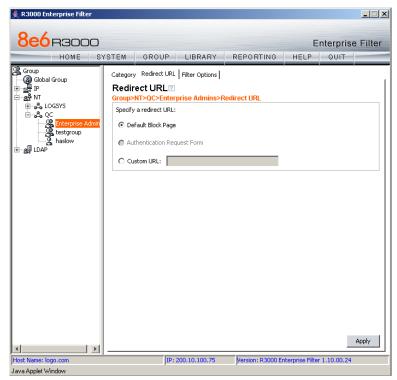


Fig. 4-24 Group Profile window, Redirect URL tab

Redirect URL is used for specifying the URL to be used for redirecting users who attempt to access a site or service set up to be blocked.

1. Specify the type of redirect URL to be used: "Default Block Page", or "Custom URL".

If "Custom URL" is selected, enter the redirect URL in the corresponding text box. Users will be redirected to the designated page at this URL instead of the block page.

2. Click **Apply** to apply your settings.

#### **Filter Options**

Click the Filter Options tab to display the Filter Options page of the Profile window:

🚖 R3000 Enterprise Filter							
8e6r3000					Er	terprise Filt	er
	STEM	GROUP	LIBRARY	REPORTING	HELP	QUIT	_
Group     Gobal Group	Filter Group> Filter Sea Good Sea UR	Options ? NT>QC>Enter Options trikes Blocking ogle/Yahoo! Safe arch Engine Keyw L Keyword Filter	Filter Options	ent		Apply	
				h	t to prote		
Host Name: logo.com Java Applet Window		JIP: 3	200.10.100.75	Version: R3000 Er	nterprise Hilter	1.10.00.24	

Fig. 4-25 Group Profile window, Filter Options tab

Filter Options is used for specifying which filter option(s) will be applied to the entity's filtering profile.

 Click the checkbox(es) corresponding to the option(s) to be applied to the filtering profile: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control". **NOTE**: See the R3000 User Guide for information about Filter Options.

2. Click **Apply** to apply your settings.

#### Remove an entity's profile from the tree

To remove a group, container, or user member's profile from the tree, select the profile in order to open the pop-up menu, and choose Remove.

# CHAPTER 5: AUTHENTICATION DEPLOYMENT

This final step of the authentication setup process includes testing authentication settings and activating authentication on the network.

# **Test Authentication Settings**

Before deploying authentication on the network, you should test your settings to be sure the Authentication Request Form login page can be accessed. If properly set up, the Authentication Request Form opens on a user's workstation if the user has been blocked from accessing specified Internet content. This form allows the user to authenticate him/herself in order to access Web content permitted by his/ her filtering profile.

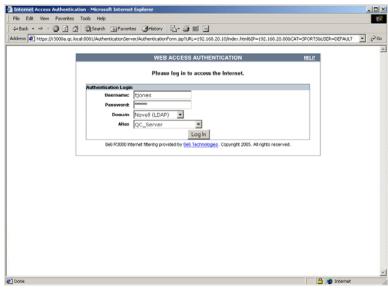


Fig. 5-1 Authentication Request Form

1

**NOTE**: In order to complete the test process, you should be sure you have your own filtering profile set up.

To verify that authentication is working, do either of the following, based on the Tier you selected:

 If Tier 2 or Tier 3 Web-based authentication will be used: Go to the Test Web-based authentication settings sub-section for instructions on testing the Authentication Request Form login page from a single workstation. For this test, you will create an IP profile for the test machine's IP address, and set the Redirect URL for the profile to access the Authentication Request Form.

**NOTE**: Before testing Web-based authentication settings, be sure the SSL certificate you created via the System > Authentication > Authentication SSL Certificate window (in Chapter 2) is placed on all workstations of users who will be authenticated. This ensures that users will not receive the Security Alert warning message from the server.

• If Tier 1 net use based authentication will be used: Go to the Test net use authentication settings sub-section for instructions on testing the net use based login command to see if you can access the assigned profile.

If you (the administrator) can be successfully authenticated in the domains that were set up, the test process is complete, and you are ready to activate authentication on the network (see Activate Authentication on the Network).



**NOTE**: The Usage Graphs window can be used for viewing and analyzing the number of end users who have been authenticated, and their usage of the Internet. See Usage Graphs from the Reporting screen section of the R3000 User Guide for more information about this reporting tool.

#### Test Web-based authentication settings

To verify that authentication is working properly, make the following settings in the Group section of the console:

#### Step 1: Create an IP Group, "test"

- 1. Click the IP branch of the tree.
- 2. Select Add Group from the pop-up menu to open the Create New Group dialog box:

≰ Create New Group 🛛 🗙						
Group Name	test					
Password	*****					
Confirm Password	*****					
ок	Cancel					
Java Applet Window						

Fig. 5-2 Create New Group box

- 3. Enter *test* as the Group Name.
- 4. Enter the password in the **Password** and **Confirm Password** fields.
- 5. Click **OK** to add the group to the tree.

#### Step 2: Create a Sub-Group, "workstation"

- 1. Select the IP Group from the tree.
- 2. Click Add Sub Group in the pop-up menu to open the Create Sub Group dialog box:

🚔 Create Sub Group	×
Group Name workstation	
OK Cancel	
Java Applet Window	

Fig. 5-3 Create Sub Group box

- 3. Enter *workstation* as the Group Name.
- 4. Click **OK** to add the Sub-Group to the IP Group.

#### Step 3: Set up "test" with a 32-bit net mask

- 1. Select the IP Group named "test" from the tree.
- 2. Click Members in the pop-up menu to display the Members window:

駦 R3000 Enterprise Filter						<u>_                                    </u>
	STEM	GROUP	LIBRARY	REPORTING	E	nterprise Filter
Group Gobal Group P P admin P P tech P P websuth P P websuth P P P websuth P P P websuth P P P websuth P P P P P P P P P P P P P P P P P P P	Add mod IP/MAC When usin frame can be cre Currer 190.160 New N © So © So	Content of the second sec	P     Subo	on the network, the II tered in the Range to I g the IP address and n ulate IP ranges withou d then clicking Add. Or	Detect global etmask or IP t t overlaps. A cce a member	proup window. A start and IP end, and member MAC is added in is added, a sub-group Remove
Host Name: logo.com Java Applet Window		JIP:	200.10.100.75	Version: R3000 Er	nterprise Filter	r 1.10.00.24

Fig. 5-4 Group Members window

- 3. Click the radio button corresponding to "Source IP".
- 4. Enter the **Source IP** address of the workstation, and select *255.255.255.255* as the subnet mask.
- 5. Click **Add** to include the IP address in the Current Members list box.

#### Step 4: Give "workstation" a 32-bit net mask

- 1. Select the IP Sub-Group "workstation" from the tree.
- 2. Click Members in the pop-up menu to display the Members window:

🚖 R3000 Enterprise Filter		
	STEM GROUP LIBRARY REPORTING HELP	Enterprise Filter
Group Global Global Group Global Global Group Global Gl	Members C Group>IP>tests workstation>Members Add members by  P © SubGroup Modify Sub Group Member To add or modify a member IP, enter the IP address and netmask or IP range the Calculator to calculate IP ranges without any overlaps. To add member MA address(se) from the "Available MAC(s)" is a row. To remove highlight the MAC address(es) and click the iright arrow. To save changes, click IP Address © Member IP 190.160.20.80 / 255.255.255.255 © Member IP Start End MAC Address Member MAC(s) Available MAC(s) Wember MAC(s)	in the Member fields. Use C(s), highlight the MAC e member MAC(s),
Host Name: logo.com Java Applet Window	IP: 200.10.100.75 Version: R3000 Enterprise Filt	ter 1.10.00.24

Fig. 5-5 Sub Group Members window

- 3. Click the radio button corresponding to "Member IP".
- 4. In the **Member IP** fields, enter the IP address of the workstation, and select 255.255.255.255 as the subnet mask.
- 5. Click Modify.

#### Step 5: Block everything for the Sub-Group

- 1. Select the IP Sub-Group "workstation" from the tree.
- 2. Click Sub Group Profile in the pop-up menu to display the Sub Group Profile window:

8e6 R3000				1	rise Filt
HOME	YSTEM GROUP LIBRARY R	EPORTING	HELP	QUI	r
Group 응 Gobal Group 문 IP 은 또한 dothin 은 또한 tech 은 또한 workstation 문 문 Workstation 문 문 Workstation 문 문 Under	Category Redirect URL Filter Options Category Profile C Group-IP-test-workstation-Category P Group: workstation Current Profile: Custom Pro Available Filter Levels Custom Profile Rule Details Category Groups Aduit Content Category Groups Aduit Content Category Groups Category Group		Child Po	rnograph	Block Block Content Block Co Co Co Co Co Co Co Co Co Co

Fig. 5-6 Sub Group Profile window, Category tab

3. In the Category Profile page, move all group categories to the Block column.

**TIP**: Blocks of category groups can be moved by clicking the first category group, and then pressing the Shift key on your keyboard while clicking the last category group, and then clicking in the Block column.

- 4. For Uncategorized Sites, click "Block".
- 5. Click Apply.

# Step 6: Use Authentication Request Page for redirect URL

1. Click the Redirect URL tab to display the Redirect URL page:

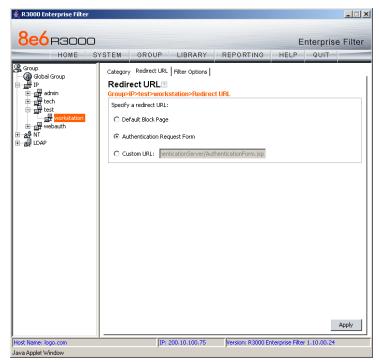


Fig. 5-7 Sub Group Profile window, Redirect URL tab

2. Select "Authentication Request Form".

**NOTE**: The host name of the R3000 will be used in the redirect URL of the Authentication Request Form, not the IP address. Be sure a forward/reverse DNS entry for the R3000 is made on the DNS server.

3. Click Apply.

#### Step 7: Disable filter options

1. Click the Filter Options tab to display the Filter options page:

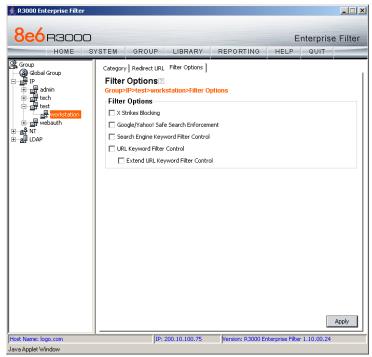
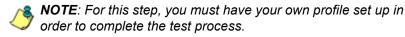


Fig. 5-8 Sub Group Profile window, Filter Options tab

- Uncheck all the checkboxes: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".
- 3. Click Apply.

#### Step 8: Attempt to access Web content



1. Launch Internet Explorer:



Fig. 5-9 Internet Explorer browser

2. Enter a URL in the Address field of the browser window.



**NOTE**: The URL should be one that begins with "http"—**not** "https".

3. After clicking **Go**, the Authentication Request Form should open:

Internet Access	Authentication - Microsoft Internet	t Explorer	5	. [D] ×
	Favorites Tools Help			
	🎯 🔄 슈님 @Search 🖻 Favoriti		_	
Address Address //	r3000a.gc.local:8081/AuthenticationServ	er/AuthenticationForm.jsp?URL=192.168.20.10/index.htmlbJP=192.168.20.808cAT=SPORTSbUSER=DEFAULT	-	200
				-
		WEB ACCESS AUTHENTICATION HELP		
		Please log in to access the Internet.		
	Authentication Login			
	Username:	tjones		
	Password:	Annen		
	Domain	Novell (LDAP)		
	Alias	QC_Server		
		Log In		
	8e6 R3000 Int	ernet filtering provided by <u>Be6 Technologies</u> . Copyright 2005. All rights reserved.		
Done Done		🔒 🍅 Internet		

Fig. 5-10 Authentication Request Form

- 4. Enter the following information:
  - Username
  - Password

If the Domain and Alias fields display, select the following information:

- Domain you are using
- Alias name for that domain (unless "Disabled" displays and the field is greyed-out)
- 5. Click **Log In** to authenticate or re-authenticate yourself on the network.

The test process has been completed successfully if you are now able to access the content for the URL you entered at step 2 in this section.

#### Test net use based authentication settings

1. From the test workstation, go to the NET USE command line and enter the NET USE command using the following format: **NET USE \\virtualip\R3000\$** 

For example: NET USE \\192.168.0.20\R3000\$

The entry you make should initiate a connection with Tier 1.

**TIP**: The virtual IP address should be the same as the one entered in the Virtual IP Address to Use for Authentication field in the Authentication Settings window (see Chapter 2: Network Setup, Enter network settings for authentication).

2. Make a Web request to a site you can access, based on your filtering profile.

The test process has been completed successfully if you are now able to access the content for the URL you entered at step 2 in this section.

# **Activate Authentication on the Network**

After successfully testing authentication settings, you are now ready to activate authentication on the network.

To verify that authentication is ready to be activated on the network, do either of the following, based on the Tier you selected:

• If Tier 2 or Tier 3 Web-based authentication will be used: There are two options for Web-based authentication: IP Group authentication, and Global Group Profile authentication. Select the option you wish to use on your network. Go to the Activate Web-based authentication for an IP Group sub-section for instructions on setting up an IP Group profile for authentication. Go to the Activate Web-based authentication for the Global Group subsection for instructions on setting up the Global Group Profile for authentication.



**NOTE**: An accelerator card is recommended if using Web-based authentication.

• If Tier 1 net use based authentication will be used: Go to the Activate net use based authentication sub-section for instructions on testing the login script and modifying the Global Group Profile for authenticating users.

# Activate Web-based authentication for an IP Group

IP Group authentication is the preferred selection for Webbased authentication—over the Global Group Profile authentication option—as it decreases the load on the R3000.

#### Step 1: Create a new IP Group, "webauth"

- 1. Click the IP branch of the tree.
- 2. Select Add Group from the pop-up menu to open the Create New Group dialog box:

Create New Group		
Group Name	webauth	
Password	*****	
Confirm Password	*****	
ок	Cancel	
Java Applet Window		

Fig. 5-11 Create New Group box

- 3. Enter *webauth* as the Group Name.
- 4. Enter the password in the **Password** and **Confirm Password** fields.
- 5. Click **OK** to add the group to the tree.

#### Step 2: Set "webauth" to cover users in range

- 1. Select the IP group "webauth" from the tree.
- 2. Click Members in the pop-up menu to display the Members window:

≜ R3000 Enterprise Filter						
	STEM	GROUP	LIBRARY	REPORTING	E	nterprise Filter
Group Global Group P P P P P P P P P P P P P P P P P P P	Member Group-IP>4 Add mer IP/MAC I When using for the designmenter IP is then clicking this frame bo can be creal Current 10.10.20.5 New Me © Sour	S 2 webauth>Me hbers by Members	embers IP Sub( to identify groups r must first be ent frame by entering Calculator to calci MAC address, an	Group on the network, the II cread in the Range to D g the IP address and n late IP ranges withou	<sup>2</sup> address and betect global etmask or IP to verlaps. A cice a member	i netmask or IP range group window. A
Host Name: logo.com Java Applet Window		IP: 2	200.10.100.75	Version: R3000 Er	nterprise Filte	r 1.10.00.24

Fig. 5-12 Members window

- 3. Click the radio button corresponding to "Source IP".
- 4. Enter the **Source IP** address of the workstation and specify the subnet mask for the range of user IP addresses of users to be authenticated.
- 5. Click **Add** to include the IP address range in the Current Members list box.

#### Step 3: Create an IP Sub-Group

- 1. Select the IP Group "webauth" from the tree.
- 2. Click Add Sub Group in the pop-up menu to open the Create Sub Group dialog box:

Create Sub Group	×
Group Name testsub	
OK Cancel	
Java Applet Window	

Fig. 5-13 Create Sub Group box

- 3. Enter the Group Name of your choice.
- 4. Click **OK** to add the Sub-Group to the IP Group.
- 5. Select the IP Sub-Group from the tree.
- 6. Click Members in the pop-up menu to display the Members window:

	Enterprise Filter
HUME S	Wembers         Add members by       P         Oroup>IP>webauth>testsub>Members         Add members by       P         Stadiation       P         Stadiation       P         Address(es) from the "Available MAC(s) is pointing the Mac(s), highlight the MAC address(es) from the "Available MAC(s), highlight the MAC address(es) from the "Available MAC(s) is the right arrow. To save changes, click Modify.         IP Address       (         C       Member IP       10.10.20.5       /       255.255.255.0       Calculator         MAC Address       Member MAC(s)       Available MAC(s)       Calculator         MAC Address       Member MAC(s)       Available MAC(s)       Modify

Fig. 5-14 Sub Group Members window

- 7. Click the radio button corresponding to "Member IP".
- 8. In the **Member IP** fields, enter the IP address range for members of the Sub-Group, and specify the subnet mask.
- 9. Click Modify.

#### Step 4: Block everything for the Sub-Group

- 1. Select the IP Sub-Group from the tree.
- 2. Click Sub Group Profile in the pop-up menu to display the Sub Group Profile window:

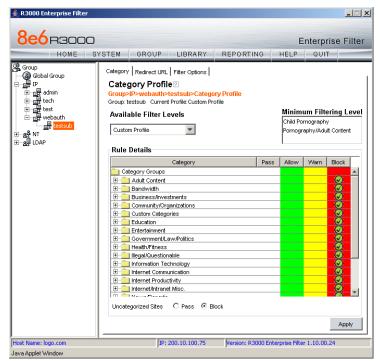


Fig. 5-15 Sub Group Profile window, Category tab

3. In the Category Profile page, move all group categories to the Block column.

**TIP**: Blocks of category groups can be moved by clicking the first category group, and then pressing the Shift key on your keyboard while clicking the last category group, and then clicking in the Block column.

- 4. For Uncategorized Sites, click "Block".
- 5. Click Apply.

# Step 5: Use Authentication Request Page for redirect URL

1. Click the Redirect URL tab to display the Redirect URL page:

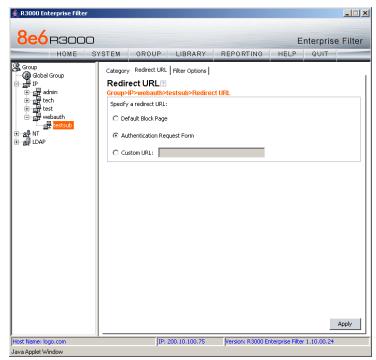
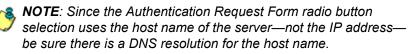


Fig. 5-16 Sub Group Profile window, Redirect URL tab

2. Select "Authentication Request Form".



#### 3. Click Apply.

As a result of these entries, Web-based authentication takes effect immediately, and any user in this Sub-Group will be sent to the Authentication Request Form if he/she attempts to access content on the Internet. After filling out this form and being authenticated, the user will be able to access Internet content based on his/her filtering profile.

#### Step 6: Disable filter options

1. Click the Filter Options tab to display the Filter options page:

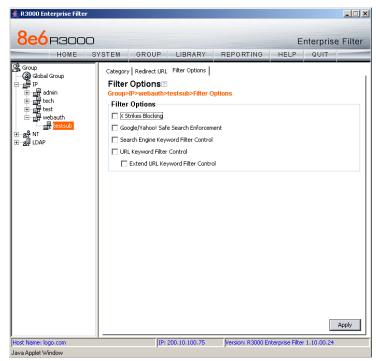


Fig. 5-17 Sub Group Profile window, Filter Options tab

- Uncheck all the checkboxes: "X Strikes Blocking", "Google/Yahoo! Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".
- 3. Click Apply.

# Step 7: Set Global Group to filter unknown traffic

- 1. Click Global Group in the tree to open the pop-up menu.
- 2. Select Global Group Profile to display the Category tab of the Profile window:

8e6 R3000					E	interpris	e Filte
HOME S	rstem	GROUP LIBRAR	REPORTIN	1G	HELP	QUIT	
을 Group 	Categ Group: Group: ( Availa Custo	/ Port   Default Redirect URL gory Profile ? Global Group>Category Pr Global Group Current Profile: able Filter Levels m Profile *	ofile		Child Por	u <b>m Filteri</b> nography aphy/Adult C	
	Rule	Details		-	[		
		Category		Pass	Allow	Warn	Block
		tegory Groups					<u>^</u>
		Adult Content Bandwidth		$\bigcirc$		_	
		Business/Investments		8			
		Community/Organizations		-8			
		Custom Categories		3			
		Education		-8			
		Entertainment		-8			
		Government/Law/Politics		-8			
		Health/Fitness		-8			
		Illegal/Questionable		-8			
	÷	Information Technology		-8			
		Internet Communication		-8			
		Internet Productivity		8			
		Internet/Intranet Misc.		ð			
	1	N		Ä			•
	Uncate	egorized Sites 💿 Pass 🤇	Block				
		-					
							Apply

Fig. 5-18 Global Group Profile window, Category tab

- a. In the Category Profile page, select categories to block, pass, white list, or assign a warn setting, and indicate whether uncategorized sites should pass or be blocked.
- b. Click Apply.
- 3. Click the Port tab to display the Port page:

🚖 R3000 Enterprise Filter						_ 🗆 🗙
	STEM	GROUP LIBRARY	REPORTING	Er	nterprise	Filter
Group Gobal Group B gr P S ag IDAP	Category Port?	Port   Default Redirect URL   F Global Group>Port Port(s)				Apply
Java Applet Window		,	·			

Fig. 5-19 Global Group Profile window, Port tab

- a. In the Port page, enter the **Port** number to be blocked.
- b. Click **Add** to include the port number in the Block Port(s) list box.
- c. After entering all port numbers to be blocked, click **Apply**.

4. Click the Default Redirect URL tab to display the Default Redirect URL page:

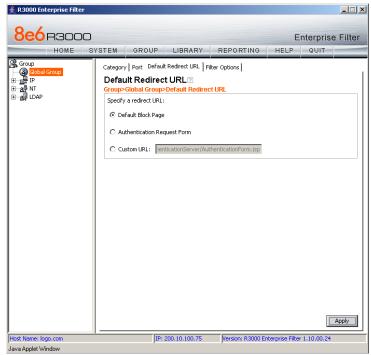


Fig. 5-20 Global Group Profile window, Default Redirect URL tab

- a. Select "Default Block Page".
- b. Click Apply.

5. Click the Filter Options tab to display the Filter Options page:

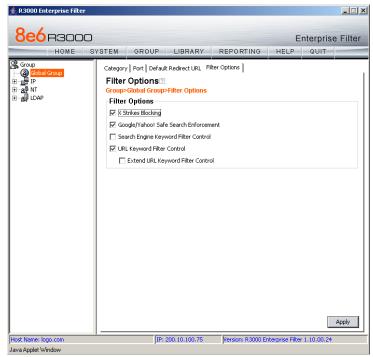


Fig. 5-21 Global Group Profile window, Filter Options tab

- a. Select filter options to be enabled.
- b. Click **Apply**.

As a result of these entries, the standard block page will display—instead of the Authentication Request Form when any user in this Sub-Group is blocked from accessing Internet content.

🖉 8e6 R3000 - Microsoft Internet Explorer 📃 🗖	l ×
Eile Edit View Favorites Tools Help	
Address 🛃 w.coors.com/&IP=200.10.100.75:81 &CAT=ALCO&USER=LOGO\Domain%20Admins\GLANG 💌 🔗 Go 🛛 Lin	ks »
ACCESS DENIED! HELP	
Internet access to the requested website has been denied based on your user profile and organization's Internet Usage Policy.	
User/Machine: LOGO/Domain Admins\GLANG	
IP: 200.10.101.140	
Category: Alcohol Reguested URL: http://www.coors.com/	
Requested on. http://www.coors.com/	
For further options, <u>click here</u> .	
To submit this blocked site for review, <u>click here</u> . For assistance, contact your Administrator.	
8e6 R3000 Internet filtering provided by <u>8e6 Technologies</u> . Copyright 2003. All rights reserved.	
	Ψ.
🖉 🛛 🖉 Internet	_//

Fig. 5-22 Default Block Page

# Activate Web-based authentication for the Global Group

This selection of Web-based authentication creates more of a load on the R3000 than the IP Group selection, and should only be used as an alternative to IP Group authentication.

### Step 1: Exclude filtering critical equipment

This step involves the identification of equipment—such as backup servers—you wish to be excluded from being served the Authentication Request Form page.

For this step, you must choose one of two options:

- Block Web access only Select this option if you do not want to log traffic for a machine that you set up to be excluded from filtering on the network. Using this option, you exclude the IP address of a machine via the Range to Detect window. If you select this option, go to Step 1A.
- Block Web access and log traffic Select this option if you wish to log traffic for a machine that you set up to be excluded from filtering on the network. Using this option, you create an IP profile for the machine via the Sub Group Profile window. If you select this option, go to Step 1B.

# Step 1A: Block Web access, logging via Range to Detect

**NOTE**: Segments of network traffic should not be defined if using the firewall mode.

#### **Range to Detect Settings**

- 1. Click Global Group in the tree to open the pop-up menu.
- 2. Select Range to Detect to display the Range to Detect Settings window:

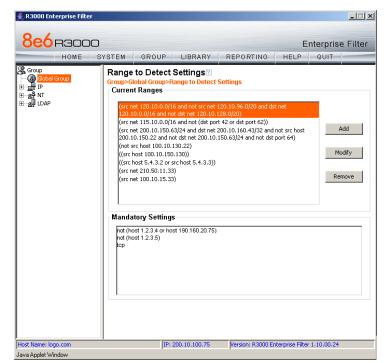


Fig. 5-23 Range to Detect Settings window, main window

3. In the Current Ranges frame, click **Add** to go to the next Settings page:



Fig. 5-24 Range to Detect Settings window, main window

4. Click **Start the Setup Wizard** to display Step 1 of the Range to Detect Setup Wizard:

#### Range to Detect Setup Wizard

8e6 R3000	Enterprise Filter
	STEM GROUP LIBRARY REPORTING HELP QUIT
Group - (③ <mark>Global Group</mark> 	Range to Detect Setup Wizard Group>Global Group>Range to Detect Setup Wizard Step 1 - Source IPs to Detect
B-SU LDAP	Welcome to the R3000 Range to Detect Setup Wizard. This wizard will help guide you through the steps needed to establish a filtering rule that the R3000 will use when filtering traffic. Note that any entries entered here will automatically be included as entries in Step 4 as Destination IPs that should be excluded from filtering.
	Use the text fields below in order to enter the Source IP(s) that the R3000 should filter
	Source IP
	10.10.10.0/24 Modify Remove
	IP / Netmask / Add Calculator
	Individual IP Add
	Next Cancel

Fig. 5-25 Range to Detect Setup Wizard, Step 1

- 1. Enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address of the source IP address(es) to be filtered.
- 2. Click Next to go to Step 2 of the Wizard:

8e6r300	SYSTEM GROUP LIBRARY REPORTING HELP QUIT
Group Gobel Group ⇒ Lat IP ⇒ a≩ NT ⇒ a≩ LDAP	Range to Detect Setup Wizard         Group>Global Group>Range to Detect Setup Wizard         Step 2 - Destination IPs to Include for Detection         Use the text fields below in order to enter the Destination IP(s) that the R3000 should filter. Enter your proxy IP(s) here.         Example Input:         5.5.5.30         5.5.5.18/28         5.5.5.90
	Destination IP  10.10.10.43/32  Modify  Remove  IP / Netmask
	Individual IP Add

Fig. 5-26 Range to Detect Setup Wizard, Step 2

- An entry for this step of the Wizard is optional. If there are destination IP address(es) to be filtered, enter the IP address and specify the Netmask, or enter the Individual IP address.
- 4. Click Next to go to Step 3 of the Wizard:

8e6r3000	YSTEM GRO	UP LIBRARY	REPORTING	HELP	nterprise QUIT	
Group Group Brite Br	Range to Def Group>Global Gro Step 3 - Sourc	tect Setup Wiza oup>Range to Detect te IPs to Exclude fi Ids below in order to Itering.	rd? Setup Wizard rom Detection	s) that the R3		×
	IP / Netmask	1	Add	i culator	Remove	Cancel
		IP: 200.10.100.75	Version: R3000 Er		at	Lancer

Fig. 5-27 Range to Detect Setup Wizard, Step 3

- An entry for this step of the Wizard is optional. If there are source IP address(es) to be ignored, enter the IP address and specify the Netmask, or enter the Individual IP address.
- 6. Click Next to go to Step 4 of the Wizard:

8e6 R3000		orise Filter
	STEM GROUP LIBRARY REPORTING HELP QU	IT
Group Global Group Global Group Global Group Global Group Global Group Global Group Global Group Global Group	Range to Detect Setup Wizard Group>Global Group>Range to Detect Setup Wizard Step 4 - Destination IPs to Exclude from Detection	
	Use the text fields below in order to enter the Destination IP(s) that the R30 should exclude from filtering. Note that any entries added in Step 1 are automatically entered here.	00
	Example Input: 5.5.5.5/30 5.5.5.16/29 5.5.5.16/29	•
	Destination IP	
	10.10.10.0/24 Modify	/
		_
	Remov	e
	IP / Netmask / 255.255.255.0 V Add	
	Calculator	
	Individual IP Add	
	Back Next	Cancel

Fig. 5-28 Range to Detect Setup Wizard, Step 4

- An entry for this step of the Wizard is optional. If there are destination IP address(es) to be ignored, enter the IP address and specify the Netmask, or enter the Individual IP address.
- 8. Click Next to go to Step 5 of the Wizard:

HOME	
Soup 	SYSTEM GROUP LIBRARY REPORTING HELP QUIT Range to Detect Setup Wizard Group>Global Group>Range to Detect Setup Wizard Step 5 - Destination Ports to Exclude from Detection
⊞– <b>2</b>	Use the text fields below in order to enter the Destination Port(s) that the R3000 should exclude from filtering. Example Input: 22 80 8462
	Individual Port Add Back Next Cancel

Fig. 5-29 Range to Detect Setup Wizard, Step 5

- 9. An entry for this step of the Wizard is optional. If there are ports to be excluded from filtering, enter each port number in the **Individual Port** field, and click **Add**.
- 10. Click **Next** to go to the final step of the Wizard:

8e6 R3000	C Enterprise Filter SYSTEM GROUP LIBRARY REPORTING HELP QUIT
HOME	
aroup @ <mark>Global Group</mark> ∃ <mark>-</mark> g⊉ IP ∃g⊉ NT	Range to Detect Setup Wizard         Group>Global Group>Range to Detect Setup Wizard         Step 6 - Recap
LDAP	Below is a recap of the entered information. Review for accuracy and click the "Finish" button to accept the entered information.
	Source IP
	Include IP Exclude IP 10.10.10.0/24 Machin. 10.10.10.34 Machin.
	10.10.10.0/24 Modify 10.10.10.34 Modify
	Destination IP Include IP Exclude IP
	10.10.10.43/32 Modify 10.10.10.0/24 Modify
	Destination Port Exclude Port
	64 Modify IP / Netmask // 255.255.50 V Calculator
	Back Finish Cancel

Fig. 5-30 Range to Detect Setup Wizard, Step 6

11. After review the contents in all list boxes, click **Finish** to accept all your entries.

As a result of these entries, the IP address(es) specified to be excluded will not be logged or filtered on the network.

Bypass Step 1B and go on to Step 2 to complete this process.

# Step 1B: Block Web access via IP Sub-Group profile

**NOTE**: This step assumes that the IP Group and Sub-Group have already been created.

- 1. Select the IP Sub-Group from the tree.
- 2. Click Sub Group Profile in the pop-up menu to display the Sub Group Profile window:

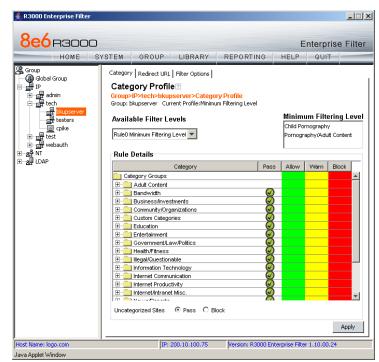


Fig. 5-31 Sub Group Profile window, Category tab

- 3. In the Category Profile page, create a custom profile by selecting categories to block, pass, white list, or assign a warn setting, and indicating whether uncategorized sites should pass or be blocked.
- 4. Click Apply.

5. Click the Redirect URL tab to display the Redirect URL page:

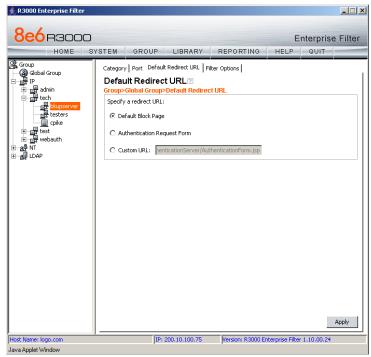


Fig. 5-32 Sub Group Profile window, Redirect URL tab

6. Select "Default Block Page", and then click Apply.

7. Click the Filter Options tab to display the Filter Options page:

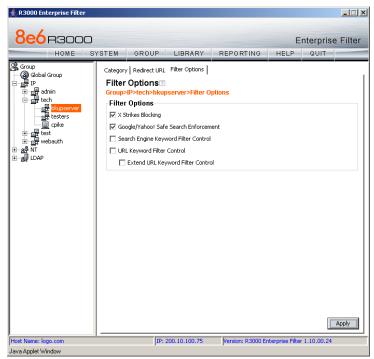


Fig. 5-33 Sub Group Profile window, Filter Options tab

8. Select filter options to be enabled, and click Apply.

As a result of these entries, the machine will not be served the Authentication Request Form, and will use the default block page instead.

Go on to Step 2 to complete this process.

#### Step 2: Modify the Global Group Profile

- 1. Click Global Group in the tree to open the pop-up menu.
- 2. Select Global Group Profile to display the Category tab of the Profile window:

8e6 R300				~ 1			rise Filt
HOME Group IP 관 관 지 고 신 고 아	Catego Group: C Availa Custor Rule	GROUP LIBRARY GROUP LIBRARY Global Group-Category Pr Global Group-Category Global Globa	Filter Options	Pass	Allow	VVern Vern VVern	Block

Fig. 5-34 Global Group Profile window, Category tab

- a. Block all categories and specify that uncategorized sites should be blocked.
- b. Click Apply.

3. Click the Port tab to display the Port page:

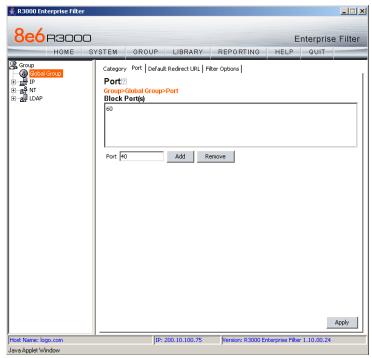


Fig. 5-35 Global Group Profile window, Port tab

- a. Enter the **Port** number to be blocked, and then click **Add** to include the port number in the Block Port(s) list box.
- b. After entering all port numbers to be blocked, click **Apply**.

4. Click the Default Redirect URL tab to display the Default Redirect URL page:

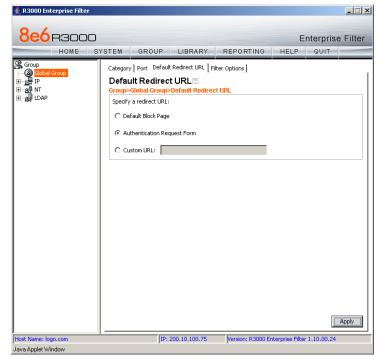


Fig. 5-36 Global Group Profile window, Redirect URL tab

a. Select "Authentication Request Form".

**NOTE**: Since the Authentication Request Form radio button selection uses the host name of the server—not the IP address— be sure there is a DNS resolution for the host name.

b. Click Apply.

5. Click the Filter Options tab to display the Filter Options page:

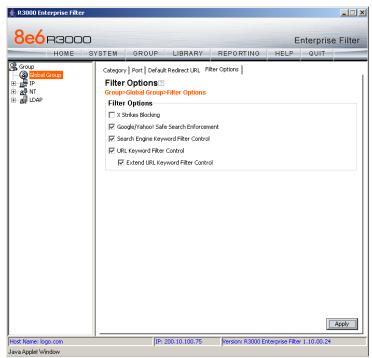


Fig. 5-37 Global Group Profile window, Filter Options tab

- a. Select filter options to be enabled.
- b. Click Apply.

As a result of these entries, a user who does not have a filtering profile will be served the Authentication Request Form so he/she can be authenticated.

## Activate NT authentication

After testing the NET USE command, the next step is to add the NET USE command to users' login scripts. We recommend that you add the 3-try login script to the existing domain login script.

The 3-try login script is used for attempting to log in the user to the authentication server in three separate attempts, in case of a login failure.

### Step 1: Modify the 3-try login script

Place a copy of the 3-try login script in the netlogon folder on your Domain Controller. Note that this sample script should be modified to use your own Virtual IP address instead of the IP address (192.168.0.20) in the sample script. This script lets users be re-authenticated from the block page without re-running the whole domain login script.

The script is as follows:

echo off :start cls net use \\192.168.0.20\r3000\$ /delete

:try1 echo "Running net use..." net use \\192.168.0.20\r3000\$ if errorlevel 1 goto :try2 if errorlevel 0 echo code 0: Success goto :end

:try2 echo Running net use... net use \\192.168.0.20\r3000\$ if errorlevel 1 goto :try3 if errorlevel 0 echo code 0: Success goto :end

:try3 echo Running net use... net use \\192.168.0.20\r3000\$ if errorlevel 1 goto :error if errorlevel 0 echo code 0: Success goto :end

:error if errorlevel 1 echo code 1: Failed!

:end

Once this updated login script has been added to the domain, each time users log in to Windows they will also log in to the R3000. Users will be blocked according to the profiles set up on the domain.

#### Step 2: Modify the Global Group Profile

The last step of the activation process is to adjust the Global Group Profile to set the policy for members of an IP-based profile, or for users who are not authenticated.

If you set a restrictive profile, unauthenticated users will not be able to obtain access until they are successfully authenticated.

If you set up a less restrictive profile to allow access, a user can still be authenticated, but won't be prompted to authenticate him/herself unless attempting to access a site that is blocked. Since the login script will automatically run when the user logs in, a less restrictive profile might be used to allow logging with the user's name without forced blocking.

- 1. Click Global Group in the tree to open the pop-up menu.
- 2. Select Global Group Profile to display the Category tab of the Profile window.
- 3. In the Category Profile page, select categories to block, pass, white list, or assign a warn setting, and indicate whether uncategorized sites should pass or be blocked.
- 4. Click Apply.
- 5. Click the Port tab to display the Port page.
- 6. Enter the Port number to be blocked, and then click **Add** to include the port number in the Block Port(s) list box.
- 7. After entering all port numbers to be blocked, click **Apply**.
- 8. Click the Default Redirect URL tab to display the Default Redirect URL page. Your options on this tab will vary, based on whether your network will be using net use based authentication only, or both Web-based and net use based authentication.
- 9. Click the Filter Options tab to display the Filter Options page. If necessary, select appropriate filter options to be enabled, and click **Apply**.

# **CHAPTER 6: TECHNICAL SUPPORT**

For technical support, visit 8e6 Technologies's Technical Support Web page at http://www.8e6.com/support.html, or contact us by phone, by e-mail, or in writing.

## Hours

Regular office hours are from Monday through Friday, 8 a.m. to 5 p.m. PST.

After hours support is available for emergency issues only. Requests for assistance are routed to a senior-level technician through our forwarding service.

## **Contact Information**

## Domestic (United States)

- 1. Call **1-888-786-7999**
- 2. Select option 2

## International

- 1. Call +1-714-282-6111
- 2. Select option 2

## E-Mail

For non-emergency assistance, e-mail us at **support@8e6.com** 

## Office Locations and Phone Numbers

#### 8e6 Corporate Headquarters (USA)

828 West Taft Avenue Orange, CA 92865-4232 USA

Local	:	714.282.6111
Fax	:	714.282.6116
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

#### 8e6 Taiwan

RM B2, 13F, No. 49, Sec. 3, Minsheng E. Rd. Taipei 104 Taiwan, R.O.C.

Taipei Local	:	2501-5285
Fax	:	2501-5316
Domestic Taiwan	:	02-2501-5285
International	:	886-2-2501-5285

## **Support Procedures**

When you contact our technical support department:

- You will be greeted by a technical professional who will request the details of the problem and attempt to resolve the issue directly.
- If your issue needs to be escalated, you will be given a ticket number for reference, and a senior-level technician will contact you to resolve the issue.
- If your issue requires immediate attention, such as your network traffic being affected or all blocked sites being passed, you will be contacted by a senior-level technician within one hour.
- Your trouble ticket will not be closed until your permission is confirmed.

## **APPENDIX A: AUTHENTICATION OPERATIONS**

When enabling authentication in the interface, there are three tiers from which to select based on the type of server(s) used on the network, and various authentication options can be used with each of these tiers.

## **Authentication Tier Selections**

R3000 authentication is designed to support the following server types for the specified tier(s):

## Tier 1: Net use based authentication



**NOTE**: Login scripts must be used for net use based authentication.

Using SMB/NetBIOS:

- Windows NT 4.0, SP4 or later
- Windows 2000 or 2003 Server in mixed/legacy mode



**NOTE**: SMB Signing must not be required.

Using LDAP:

- Microsoft Active Directory Mixed Mode
- Microsoft Active Directory Native Mode

## Tier 2, Tier 3: Web-based authentication

Using an NT authentication domain:

- Windows NT 4.0, SP4 or later
- Windows 2000 or 2003 Server in mixed/legacy mode



**NOTE**: SMB Signing must not be required.

Using an LDAP domain:

- Windows Active Directory 2002 and 2003
- Novell eDirectory
- SunONE directory server

## **Tier 1: Single Sign-On Authentication**

## Net use based authentication process

The following diagram and steps describe the operations of the net use based user authentication process:

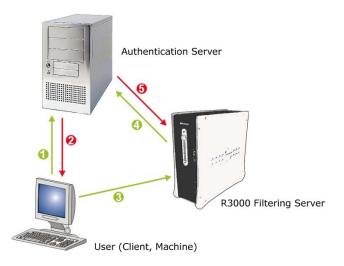


Fig. A-1 Net use based authentication module diagram

- 1. The user logs on the network from a Windows workstation (also known as "client" or "machine").
- 2. The authentication server on the network sends the user's workstation a login script containing a net use command.
- The execution of this net use command causes the Windows workstation to create an "IPC share" (command exchange) with the R3000 filter box as a shared network device.

**NOTE**: When the IPC share is created, no drives are mapped in this share.

- 4. Upon creating the IPC share, the software in the R3000 queries the network authentication server with the user's login name and password sent by the workstation.
- 5. Once the user is successfully authenticated, the R3000 matches the user's login name or group name with a stored list of profile settings in the R3000. As a result of this process, the user is assigned the appropriate level of filtering.
- The matched profile is set for the user's IP address. The IPC connection is completed and maintained with periodic "keep-alives."
- 7. When the user logs off, changes IP addresses, loses the network connection, or in any way causes the IPC connection to be altered or deactivated, the R3000 senses this change and returns the IP address to the configured global filtering level.

WARNING: Authentication will fail if a Network Address Translation (NAT) device is set up between the authentication server and end user clients. Authentication may also fail if network connections are overloaded, causing a severe delay in the transportation of SMB traffic. This can be a problem in any network, but is most prevalent in WAN links, or in trunk links that are overloaded.

#### **Re-authentication process**

- 1. The user loses his/her user profile after one of the following incidences occurs:
  - the server is rebooted, or
  - the connection from the user's machine to the server is dropped (as with a faulty network cable)
- 2. A block page displays for the user.
- 3. In order to re-access the Internet, the user must reauthenticate him/herself by clicking a link in the block page to generate a login script that re-authenticates the user's profile.

## Tier 1 authentication methods

Tier 1 supports two server authentication methods: Server Message Block (SMB) and LDAP.

### SMB protocol

SMB is a client/server protocol that requires the client to send a request to the server and receive an authentication response from the server, in order for the client to access resources on the network.

As the default protocol for NT 4.0 and earlier operating systems, SMB is supported by Windows 2000 and later OS versions.

#### **SMB Signing**

SMB Signing is a Windows security feature that prevents an active network session between a client and server from being tapped. While Microsoft has made this feature available since Windows NT 4.0, it was not a default setting. However, in Windows 2003, this feature is enabled by default.

Since SMB Signing is not currently supported by the R3000, 8e6 recommends disabling the requirement for this feature. This does not disable SMB Signing for machines that support it, but allows devices that do not support SMB Signing to connect. To disable the default setting that requires SMB Signing for all connections, follow the instructions in Appendix B: Disable SMB Signing Requirements.

Alternately, if you have an available Windows 2000 Server—or an earlier Windows NT 4.0 Server—and are willing to establish the necessary trust relationships with the Windows 2003 Server, this earlier Windows server can be used as the primary authentication server for the R3000 instead of the Windows 2003 Server.



**NOTE**: For information on SMB Signing compatibility with the R3000, refer to the chart in Appendix B: Disable SMB Signing Requirements.

## LDAP protocol

LDAP is a directory service protocol that stores entries (Distinguished Names) in a domain's directory using a hierarchical tree structure. The LDAP directory service is based on a client/server model protocol to give the client access to resources on the network.

When a client connects to a server and asks it a question, the server responds with an answer and/or with a pointer to the server that stores the requested information (typically, another LDAP server). No matter which LDAP server the client accesses, the same view of the directory is "seen."

The LDAP specification defines both the communication protocol and the structure, or schema, to a lesser degree. There is an Internet Assigned Network Authority (IANA) standard set that all LDAP directories should contain. Novell and Microsoft both have additional schema definitions that extend the default setups. Most server operating systems now support some implementations of LDAP authentication. The Microsoft Active Directory LDAP-based model became available with the release of Windows 2000.

## Name resolution methods

The name resolution process occurs when the R3000 attempts to resolve the IP address of the authentication server with the machine name of that server. This continuous and regulated automated procedure ensures the connection between the two servers is maintained.

When using an NT server with SMB, the name resolution process occurs when a valid Windows Internet Name Service (WINS) Server IP address is entered or a broadcast query is made.

When using an LDAP server, the name resolution process occurs when a Domain Name Service (DNS) entry is made. In order to accommodate this request, the LDAP server must have a valid DNS entry or the IP address must be added to the R3000 hosts file.



NOTE: If LDAP is used, client machines will still use the SMB authentication method to communicate with the R3000 server for Tier 1 authentication. LDAP communication only occurs between the R3000 server and the LDAP server.

## Configuring the authentication server

When configuring authentication, you must first go to the authentication server and make all necessary entries before configuring the R3000.

The following authentication components must be set up or entered on the console of the authentication server:

- domain name
- usernames and passwords
- user groups
- login scripts

#### Login scripts

Login (or logon) scripts are used by the R3000 server for reauthenticating users on the network.

The following syntax must be entered in the appropriate directory on the authentication server console:

#### Enter net use syntax in the login script

The virtual IP address is used by the R3000 to communicate with all users who log on to that server. This address must be in the same subnet as the one used by the transmitting interface of the R3000.

• For testing, user information can be specified on the command line as follows:

#### NET USE \\virtualip\R3000\$ /user:DOMAIN-NAME\username password

Example: NET USE \\192.168.0.20\R3000\$/ user:LOGO\jsmith xyz579

 The command to disconnect a session is: NET USE \\virtualip\R3000\$ /delete

#### View login script on the server console

The login script can be viewed on the authentication server console. This script resides in a different location on the server, depending on the version of the server:

#### Windows 2000 or Windows 2003 Server

\\servername.suffix\sysvol\domainname.suffix\
policies\{guid}\user\scripts\logon

c:\winnt\sysvol\sysvol\domainname.suffix\scripts

c:\winnt\sysvol\domainname\scripts

#### • Windows NT 4.0 Server

\\servername\netlogon

\\ipaddress\netlogon

c:\winnt\system32\repl\import\scripts

The login script must be specified either in the user's domain account or in the Active Directory Group Policy Object so that it runs when the user logs into the domain.

#### Block page authentication login scripts

In addition to the use of login scripts in the console of the authentication server, a login script path must be entered in the Block Page window of the R3000 Administrator console. This script is used for reauthenticating users on the network.

The following syntax must be used:

#### \\SERVERNAME\netlogon

or

#### \\IPaddress\netlogon



**NOTE**: See Block Page Authentication for more information about these entries.

## LDAP server setup rules

WARNING: The instructions in this user guide have been documented based on standard default settings in LDAP for Microsoft Active Directory Services. The use of other server types, or any changes made to these default settings, must be considered when configuring the R3000 server for authentication.

If LDAP will be used, the following items should be considered:

- The administrator in charge of the LDAP server should create a user for the R3000 in order to give that user full read access to the groups and users in the directory.
- Since the LDAP directory is structured as a tree, data needs to be retrieved the same way. Additionally, the order of the syntax is reversed compared to how it appears in normal file system folders. The deepest layer is listed first, in a similar manner as a DNS domain name: e.g. "engineering.company.net". In LDAP, a directory entry would look like this: "cn=engineering,dc=company, dc=net".
- Make sure all network configuration settings are correct (such as DNS, IP, etc.) before configuring LDAP settings.

1

NOTE: All filtering profiles are stored on the R3000 server.

# Tier 2: Time-based, Web Authentication

The following diagram and steps describe the operations of the time-based authentication process:

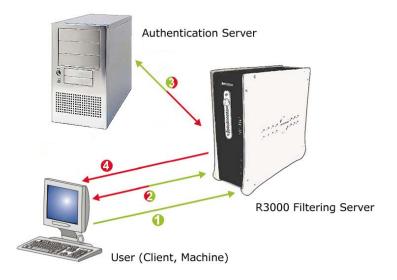


Fig. A-2 Web-based authentication module diagram

- 1. The user makes a Web request by entering a URL in his/ her browser window.
- 2. The R3000 intercepts this request and sends the user the Authentication Request Form, requesting the user to log in with his/her login ID and password.
- 3. The R3000 verifies the user's information with the authentication server (Domain Controller, Active Directory, LDAP, etc.).
- 4. The authenticated user is allowed to access the requested URL for the time period specified by the administrator.

# Tier 2 implementation in an environment

In an environment where Tier 2 time-based profiles have been implemented, end users receive filtering profiles after correctly entering their credentials into a Web-based Authentication Request Form. A profile remains active for a configurable amount of time even if the user logs out of the workstation, changes IP addresses, etc.

Tier 2 time-based profiles do not call for the R3000 to maintain a connection with the client machine, so the R3000 cannot detect when the user logs off of a workstation. In order to remove the end user's profile, one of two scripts detailed in this sub-section should be inserted into the network's login and/or logoff script.

The Tier 2 Script should be used if Tier 2 is the only tier implemented in an environment. The Tier 1 and Tier 2 Script should be used if Tier 2 is implemented along with Tier 1 in an environment. Since both sets of scripts use the NET USE command, the client machine must already have the ability to connect to the R3000 via NET USE in order for the profile to be removed in either environment.

### **Tier 2 Script**

If using Tier 2 only, this script should be inserted into the network's login script. If the network also uses a logoff script, 8e6's script should be inserted there as well. The inclusion of this script ensures that the previous end user's profile is completely removed, in the event the end user did not log out successfully.

echo off :start cls net use \\10.10.10.10\LOGOFF\$ /delete :try1 NET USE \\10.10.10.10\LOGOFF\$ if errorlevel 1 goto :try2 if errorlevel 0 echo code 0: Success goto :end

:try2 NET USE \\10.10.10.10\LOGOFF\$ if errorlevel 1 goto :try3 if errorlevel 0 echo code 0: Success goto :end

:try3 NET USE \\10.10.10.10\LOGOFF\$ if errorlevel 1 goto :error if errorlevel 0 echo code 0: Success goto :end

:error if errorlevel 1 echo code 1: Failed!

:end net use \\10.10.10.10\LOGOFF\$ /delete

### **Tier 1 and Tier 2 Script**

In an environment in which both Tier 1 and Tier 2 are used, this version of 8e6's script should be inserted into the network's login script. 8e6's script attempts to remove the previous end user's profile, and then lets the new user log in with his/her assigned profile.

echo off :startremove cls NET USE \\10.10.10.10\LOGOFF\$ /delete

:tryremove1 NET USE \\10.10.10.10\LOGOFF\$ if errorlevel 1 goto :tryremove2 if errorlevel 0 echo code 0: Success goto :endremove

:tryremove2 NET USE \\10.10.10.10\LOGOFF\$ if errorlevel 1 goto :tryremove3 if errorlevel 0 echo code 0: Success goto :endremove

:tryremove3 NET USE \\10.10.10.10\LOGOFF\$ if errorlevel 1 goto :removalerror if errorlevel 0 echo code 0: Success goto :endremove

:removalerror if errorlevel 1 echo code 1: Failed to send removal request!

:endremove net use \\10.10.10.10\LOGOFF\$ /delete :try1 NET USE \\10.10.10.10\R3000\$ if errorlevel 1 goto :try2 if errorlevel 0 echo code 0: Success goto :end

:try2 NET USE \\10.10.10.10\R3000\$ if errorlevel 1 goto :try3 if errorlevel 0 echo code 0: Success goto :end

:try3 NET USE \\10.10.10.10\R3000\$ if errorlevel 1 goto :error if errorlevel 0 echo code 0: Success goto :end

:error if errorlevel 1 echo code 1: Failed!

:end

in environments that use both Tier 1 and Tier 2, if a logoff script is used on the network, the Tier 2 Script should be inserted into the network's logoff script.

# **Tier 3: Session-based, Web Authentication**

The diagram on the previous page (Fig. A-2) and steps below describe the operations of the session-based authentication process:

- 1. The user makes a Web request by entering a URL in his/ her browser window.
- 2. The R3000 intercepts this request and sends the user the Authentication Request Form, requesting the user to log in with his/her login ID and password.
- 3. The R3000 verifies the user's information with the authentication server (Domain Controller, Active Directory, LDAP, etc.).
- 4. A pop-up window opens on the user's workstation while the original window loads the requested URL. The user will continue to be authenticated as long as the pop-up window remains open.

# 8e6 Authenticator

The 8e6 Authenticator ensures the end user is authenticated on his/her workstation, via an executable file that launches during the login process. To use this option, the 8e6 Authenticator client (authenticat.exe) should be placed in a network share accessible by the domain controller or a Novell eDirectory server such as NetWare eDirectory server 6.5.

**NOTE**: The 8e6 Authenticator client (authenticat.exe) can be downloaded from the Enable/Disable Authentication window. (See the Enable authentication, specify criteria sub-section in Chapter 2: Network Setup.)

# Environment requirements

### Minimum system requirements

The following minimum server components are required when using NetWare eDirectory server 6.5:

- · Server-class PC with a Pentium II or AMD K7 processor
- 512 MB of RAM
- Super VGA display adapter
- DOS partition of at least 200 MB and 200 MB available space
- 2 GB of available, unpartitioned disk space outside the DOS partition for volume sys:
- One network board
- CD drive

#### **Recommended system requirements**

The following server components are recommended for optimal performance when using NetWare eDirectory server 6.5:

- Server-class PC with two-way Pentium III, IV, or Xeon 700 MHz or higher processors
- 1 GB of RAM
- VESA compliant 1.2 or higher display adapter
- DOS partition with 1 GB of available space
- 4 GB of available, unpartitioned disk space outside the DOS partition for volume sys:
- One or more network boards
- Bootable CD drive that supports the EI Torito specification
- USB or PS/2\* mouse

## Workstation requirements

The 8e6 Authenticator client works with the following operating systems:

- Windows XP Pro SP1 and 2
- Windows 2000 Pro SP4
- Windows XP and Windows 2000 with Novell client v4.91

**NOTE**: Any non-domain supported Windows operating system, such as ME or XP Home Edition, will not work with the 8e6 Authenticator unless the Novell eDirectory client is installed for login and deployment of the 8e6 Authenticator client using a Novell server.

# Work flow in a Windows environment

- 1. The administrator stores the 8e6 Authenticator client (authenticat.exe) in a network-shared location that a login script can access.
- 2. Using a Windows machine, an end user logs on the domain, or logs on the eDirectory tree via a Novell client.
- 3. The end user's login script evokes authenticat.exe.
- 4. The 8e6 Authenticator client determines the authentication environment by examining the Windows registry, then retrieves the username and domain name using either Windows or Novell APIs, and sends this information (LOGON event) to the R3000.
- 5. The R3000 looks up the groups to which the end user belongs (Windows AD, PDC, or eDirectory through LDAP or NTLM/Samba), and determines the profile assignment.
- 6. The R3000 sets the profile for the end user with username (including the group name, if it is available) and IP.
- 7. The 8e6 Authenticator client continually sends a "heartbeat" to the R3000—with a specified interval of seconds between each "heartbeat"—until the end user logs off.
- 8. The end user logs off, and the 8e6 Authenticator client sends a LOGOFF event to the R3000. The R3000 removes the user's profile.



**NOTE**: The 8e6 Authenticator can handle up to 20 logons per second.

### 8e6 Authenticator configuration priority

The source and order in which parameters are received and override one another are described below.



**NOTE**: Any parameter set at the end of the list will override any parameter that was previously set.

- 1. **Compiled Defaults**: Given no parameters at all, the client will try to execute using the default compilation.
- Configuration File (optional): The default location of the configuration file is the same path/name as the authenticat.exe client, but with a ".cfg" extension instead of ".exe". The full path/name can be specified on the command line with the CF[] parameter. Review the ++ comment following Table 1 for more information.
- 3. **Command Line** (optional): Options on the command line will override compiled defaults and the configuration file. The command line can be left blank.
- 4. **R3000 Configuration Packet** (optional): The R3000 may send a configuration packet that will override all other settings, including the command line. If the R3000 changes the IP address or port used by authenticat.exe, then when authenticat.exe reconnects, authenticat.exe will use the new IP address and port.



**NOTE**: The R3000 can force authenticat.exe to reconnect with a re-logon event packet.

#### 8e6 Authenticator configuration syntax

All configuration parameters, regardless of their source, will use the following format/syntax:

#### wAA[B]w{C}w

{Parameter 'AA' with Data 'B', and Comment 'C' ignored.}

#### w;DD[E]w{C}w

{The semicolon causes 'DD[E]' to be ignored, 'C' is also ignored.}

Whereas '**AA**' is a two-letter, case-insensitive parameter name, '**B**' is the value for this parameter wrapped in brackets ([]), and '**w**' is zero or more white spaces (space, tab, carriage return, line feed). '**C**' is completely ignored, and anything wrapped in braces ({}) is considered a comment. A ';' immediately preceding a parameter will cause that parameter and its data to be ignored, which is convenient for temporarily reverting a parameter to default values during testing.

#### Sample command line parameters

authenticat.exe LF[c:\] ra[192.168.0.43]Rr[40000]

#### Sample configuration file

RA[100.10.101.30] { R3000 Virtual IP address } RP[139] { R3000 Port } RH[30000] { Heartbeat timer (30 seconds) } RR[30000] { Reconnect time (before connecting again) } RC[10000] { Connect Timeout (how long to wait for a connection response) } LE[0] LF[\\100.10.101.117\publogs\] { Where to put logs }

#### Sample R3000 configuration update packet 'PCFG'

After decryption, with protocol headers removed:

RH[30000]RC[1000]LE[1]

You only need to change the options you do not wish to remain as default. Often the IP address of the R3000 (RA) and the log file (LF) are the most desired options to change. Note that full network paths are allowed.

### **Table of parameters**

The following table contains the different parameters, their meanings, and possible values.

Param ID	Parameter Meaning	Values	Dbg Default	Release Default
UT+	User's Logon Environment	1-256 (0 = Win32, 1 = Nov- ell)	255 (auto)	255 (auto)
RA # *	R3000 Virtual IP Address	255.255.255.255:PORT;	0.0.0.0	0.0.0.0
RV #	R3000 VPN Sup- port Table	(IP-IP;IP:PORT;),		
RP	R3000 Port	1-65535	139	139
RH	R3000 Heartbeat Timer MS	1-4 billion (milliseconds)	30000	30000 (30 sec)
RR	R3000 Reconnect Time MS	1-4 billion (milliseconds)	30000	30000 (30 sec)
RC	R3000 Connect Timeout MS	1-4 billion (milliseconds)	10000	10000 (10 sec)
LE	Log using Event Viewer	1 or 0 (event view or log file)	0 (log file)	1 (event view)
LD	Logging Detail	1, 2, 3, or 4	1 (light)	0 (errors only)
LF *	Path-ONLY to out- put log file	1-1000 alphanum	C:\	C:\
CF ++	Full path/name of Configuration File	1-1000 alphanum	_	_

- If UT[0] is set, then the Novell environment will be ignored, if present, and only the Windows environment information will be retrieved and sent to the R3000. If UT[1] is set and the Novell environment is invalid or the user is not authenticated with its Novell server, then the results sent to the R3000 are invalid (probably empty values). The default UT[255] auto detects Novell vs. Win32 and will automatically favor Novell authentication over Windows, if possible.
- \* Special Interest. Values most likely to change during testing, configuration, and production implementation.
- ++ Alternate configuration file is only valid when specified on the command line. It will be ignored in any other context. If the configuration file cannot be loaded from the alternate location, an error will be logged and an attempt will be made to load the default configuration file. If the alternate configuration file is specified and is blank (CF[]), the 8e6 Authenticator will not attempt to load any configuration file; this can minimally speed up execution time. The compiled default value of CF[-] causes the default configuration file loading to be attempted, which has the same full path and filename of the current, loaded 8e6 Authenticator executable, but with an extension of ".cfg" instead of ".exe". That is, if the 8e6 Authenticator client is "\\example\authenticat.exe", the search for the default configuration file would be "\\example\authenticat.cfg". It is not an error if the default configuration file does not exist. It is an error if the default configuration file exists but cannot be read or parsed correctly. Unknown parameters are ignored. Format/syntax errors will abort the reading and report an error, but the 8e6 Authenticator will attempt to continue running.
- For each IP address where ":PORT" is omitted from the address, the RP[] port value is used. For example, if RA[1.1.1.1:5555] is set, the RP[] parameter is ignored.

RP[] affects port-less addresses specified in the RV[] command as well.

- For RA[], each IP address is separated by a semi-colon ';' and the first IP address will be tried for each new connection attempt. When the main IP address fails to respond, the next IP address in the list will be tried, and so on, if it fails. After the last IP address is tried, the logic will continue from the first IP address again. A retry attempt on the main IP address is subject to the RR[] Reconnect time. After any disconnection, the logic will always begin with the main IP address as its first attempt.
- For RV[], sets of R3000 addresses are specified based on an IP range that matches the client's IP address; multiple destination R3000 addresses may be used in each set and will have the same functionality as multiple destinations specified in the RA[] parameter. Each set is surrounded by parentheses '()'s, and sets are separated by commas ','. Any local client IP address that does not match any set will use the RA[] address. Sample format:

RV[(102.108.1.0-102.108.1.255;1.1.1.1;2.2.2.2),(102.108.2.0-102.108.2.255;3.3.3:222)]

In this example, a client with an IP address of 102.108.1.5 would try to connect to 1.1.1.1 using the RP[] port (2.2.2.2 as the backup). A client with 192.168.2.15 would try to connect to 3.3.3.3 port 222, which has no backup.

 Any local address that would end up connecting to 0.0.0.0 will not be observed by the 8e6 Authenticator. This allows RV[] to allow only specified ranges of IP addresses to be observed by the 8e6 Authenticator.

# **Novell eDirectory Agent**

Novell eDirectory Agent provides Single Sign-On (SSO) authentication for an R3000 set up in a Novell eDirectory environment. Using Novell eDirectory Agent, the R3000 is notified by the eDirectory server when an end user logs on or off the network, and adds/removes his/her network IP address, thus setting the end user's filtering profile accordingly.

# Environment requirements

### **Novell eDirectory servers**

The following eDirectory versions 8.7 or higher with Master, Read/Write, Read replicas have been tested:

- eDirectory 8.7 in RedHat Linux 9.0
- eDirectory 8.7 in NetWare 6.5 SP5



**NOTE**: See 8e6 Authenticator: Environment requirements for Minimum and Recommended system requirements. These requirements also apply to eDirectory 8.7 in RedHat Linux 9.0.

#### **Client workstations**

To use this option, all end users must log in the network. The following OS have been tested:

- Windows 2000 Professional
- Windows XP
- Macintosh

### **Novell clients**

The following Novell clients have been tested:

- Windows: Version 4.91 SP2
- Macintosh: Prosoft NetWare client Version 2.0

# Novell eDirectory setup

The eDirectory Agent uses the LDAP eDirectory domain configuration setup in the R3000 Administrator console. The eDirectory Agent receives notification from the eDirectory server regarding logon and logoff events by end users. The Novell client must be installed on each end user's workstation in order to handle logons to the eDirectory network. In this setup, the Novell client replaces the Windows logon application.

# R3000 setup and event logs

When using a Novell eDirectory server and choosing to use the Novell eDirectory Agent option in the R3000:

• Enable Novell eDirectory Agent in the Enable/Disable Authentication window.



**NOTES**: If using an SSO authentication solution, Tier 2 or Tier 3 should be selected as a fallback authentication operation.

When choosing the Novell eDirectory Agent option, the 8e6 Authenticator option must be disabled.

• If applicable, a back up server can be specified in the LDAP domain setup wizard, in the event of a connection failure to the primary Novell eDirectory server. Email alerts are sent to the administrator in such events.



**NOTE**: Back up server settings are made in the Default Rule tab of the LDAP Domain Details window, described in Chapter 4: LDAP Authentication Setup.

 Once the Novell eDirectory Agent option is set up, the View Log File window can be used to view end user logon/logoff events and the debug log.



**NOTE**: After the Novell eDirectory Agent is enabled, an individual's username will not display in the event log until he/she logs in again. Until that time, the user will be logged by his/her current filtering profile, which most likely would be IPGROUP or DEFAULT user.

# **Active Directory Agent**

Active Directory Agent is a Windows service that provides transparent user identification for Windows Active Directorybased networks. The Active Directory Agent (also called "AD Agent") collects information from several sources simultaneously and populates a single session table that identifies the current user for each active workstation on the network. This session table is forwarded to the R3000 so the end user is given the appropriate filtering profile.

The AD Agent can be installed on any Windows 2000 or 2003 server on the domain, and does not have to be installed on a domain controller.

In large networks, multiple AD Agent hosts can cooperate as a "team" to deal with issues of security partitioning, network bandwidth, and administrative responsibility boundaries.

# Product feature overview

- Provides Single Sign-On (SSO) transparent authentication
- · Supports Mixed or Native Windows environments
- · Supports LDAP and LDAPS protocols
- · Auto-detects domains and domain controllers
- Works with an existing Tier 2/Tier 3 authentication configuration

#### Windows server requirements

- · Windows 2000 or Windows 2003 server
- · Latest Microsoft patches/service packs applied
- At least 512 MB RAM
- 100 MB disk space
- Special domain user account for the service with permissions to read AD Agent event logs

#### Work flow in a Windows environment

- 1. AD Agent is installed in either a domain controller or on a separate Windows server that can talk to the domain controller via Windows APIs.
- 2. End users log on/off the network, and the event is logged in the event viewer.
- 3. AD Agent queries the event log or probes workstations to obtain log on/log off event information (login name, domain name, IP address of machine).
- 4. AD Agent sends information with the event indicator to the R3000 Authentication Module.
- 5. R3000 assigns or removes a profile based on the user information and event indicator.

# Set up AD Agent

### Step 1: AD Agent settings on the R3000

To set up Active Directory Agent on the R3000, go to System > Authentication > Enable/Disable Authentication window in the R3000 interface, and specify the following criteria:

R3000 Enterprise Filter	× II
8e6r3000	Enterprise Filter
System Control Network Administrator Diagnostics Alert	Enable/Disable Authentication  System-Authentication>Enable/Disable Authentication Authentication Authentication mode: Enabled Disable Disable
Patch Synchronization Mode Authentication Nic Mode Backup/Restore Reset Reset Shillp	Web-based Authentication         C       Tier 1: Web-based Authentication disabled (Net Use enabled)         Image: Tier 2: Use time-based profiles, with time-out (in minutes):       30         C       Tier 3: Use persistent logins via a Java Applet         Ter 2 & 3 Note: In an organization with more than 5000 users, slowness may be experienced during the
<ul> <li>─Hardware Failure Detection</li> <li>─X Strikes Blocking</li> <li>─Warn Option Setting</li> <li>─Customization</li> </ul>	authentication process. In this scenario, 866 recommends using an R3000 Filter with an SSL accelerator card installed. Please contact 866 for more information. 866 Authenticator © On O Off Download 866 Authenticator It is highly recommended that the 866 Authenticator option be turned on at all times. AD Agent
	© On C Off     Download 8e6 AD Agent Installer     Settings       Novell eDirectory Agent     C On © Off       Sending Keep Alive
Host Name: logo.com	IP: 200.10.100.75         Version: R3000 Enterprise Filter 1.10.00.24

Fig. A-3 Enable/Disable Authentication window, AD Agent frame

- 1. In the AD Agent frame, click "On".
- 2. Click **Settings** to open to the AD Agent Settings pop-up window, used for entering criteria to permit the primary AD Agent to send data to the R3000:

) Agent Settings					×
Settings					
Computer Name	e:	F	assphrase:		Í
ADSERVER1		*****			
JSMITH23		****			
				Datata	ı.
				Delete	
Computer Name:					]
Passphrase:					1
Confirm:					
			Add	Modify	
	Click Appl	y in parent wind	ow for change	es take effec	t
va Applet Window					

Fig. A-4 AD Agent Settings pop-up window

- 3. In the **Computer Name** field, enter the name of the primary AD Agent machine.
- 4. Enter from seven to 20 alphanumeric characters in the **Passphrase** field, and enter the same characters again in the **Confirm** field.
- 5. Click **Add** to include a row to the list above, showing the Computer Name in all upper-case letters, and asterisks for the Passphrase.

**NOTES**: To modify any of the criteria for an existing Computer Name entry, select the Computer Name from the list, and then modify the fields below. Be sure to make entries in the Passphrase and the Confirm fields before clicking Modify.

To delete a Computer Name from the list, select the Computer Name and then click Delete.

- 6. After making your entries, click the "X" in the upper right corner of the pop-up window to close it.
- 7. Click **Apply** in the Enable/Disable Authentication window to save your settings.

#### Step 2: Configure the domain, service account

- 1. Create a new group on the domain named dcagent\_services.
- 2. Create a new domain user account named **dcagent\_service** and make it a member of the dcagent\_services group.

**TIP**: Be sure to record the password for this domain account; you will be prompted for it during the configuration wizard process (see Step 3C: Run AD Agent configuration wizard).

3. Add the Administrator account to the dcagent\_services group.



**NOTE**: Any users in the dcagent\_services group have permission to manage the AD Agent.

- 4. Open the Domain Security Policy console, and do the following:
  - a. Expand the Local Policies > Audit Policy node of the Security Settings tree.
  - b. Double-click the Audit account logon events policy.
  - c. Check the "Define these policy settings" checkbox.
  - d. Check the "Success" checkbox.

Make the same settings in the Audit logon events policy.

- 5. Close the Domain Security Policy console.
- 6. Open the Domain Controller Security Policy console, and do the following:
  - a. Expand the Local Policies > User Rights Assignment node of the tree.
  - b. Double-click the Manage auditing and security log policy.
  - c. Check the "Define these policy settings" checkbox.

d. Add the dcagent\_services and Domain Admins groups to the list of permitted users.

If installing the AD Agent on a domain controller only:

- Double-click the "Allow Logon Locally" setting.
- Add the dcagent\_service account to the list of permitted users.
- 7. Close the Domain Controller Security Policy console.

### Step 3: AD Agent installation on Windows server

The steps in this section provide instructions for setting up and running AD Agent on a simple, single-domain network.

#### Step 3A: Download DCAgent.msi

- 1. In the R3000 interface, go to System > Authentication > Enable/Disable Authentication window.
- 2. In the AD Agent frame, click **Download 8e6 AD Agent Installer** to download the AD Agent (DCAgent.msi) to the administrator's machine.

#### Step 3B: Run AD Agent installation setup

1. Launch DCAgent.msi:



Fig. A-5 Run DCAgent.msi

NOTE: If prompted, install Microsoft .Net Framework 2.0. Framework may require updating other Windows components before installing the AD Agent.

2. Click **Run** to open the End User License Agreement (EULA) in the 8e6 AD Agent installation setup wizard:



Fig. A-6 AD Agent EULA

3. After reading the EULA, click **Accept** to proceed with the AD Agent installation setup process:

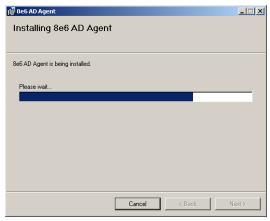


Fig. A-7 AD Agent installation

4. When the AD Agent installation setup process has successfully finished, completion information displays:

🗬 8e6 AD Agent	<u> </u>
Installation Complete	
8e6 AD Agent has been successfully installed.	
Click "Close" to exit.	
Please use Windows Update to check for any critical updates to the .NET Framework.	
Cancel < Back.	Close

Fig. A-8 Installation Complete

Click **Close** to close the installation setup window and to open the AD Agent configuration wizard window (see Fig. A-9). The configuration wizard can be completed now or at a later point in time.

#### Step 3C: Run AD Agent configuration wizard

The AD Agent configuration wizard should be run when setting up AD Agent for the first time, and if the role of the AD Agent on the current machine changes (from primary to satellite, or vice versa).

**TIP**: To access the configuration wizard after the initial setup process, go to Start on the Windows machine, and from the 8e6 AD Agent menu select Quick-Configuration Wizard.

1. Review the contents of the first wizard page that explains how to configure the domain and service account, as described in Step 2:

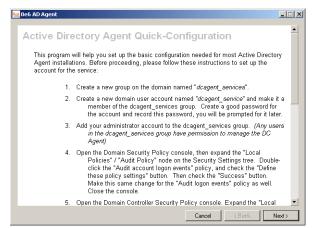


Fig. A-9 AD Agent configuration wizard, preliminary instructions

Click Next to go to the account and password page:

🛀 8e6 AD Agent	
Enter the dcagent_service account name and password below. If you he created the dcagent_services account or the dcagent_services group, cl follow the instructions for account setup.	ave not yet lick "Back" and
Account: LOGO \dcagent_service Password Confirm password:	
C Do not update service account	t settings.
Cancel	<pre>Back Next&gt;</pre>

Fig. A-10 Account and password information

- 2. By default, the Account field is populated with the path of the dcagent\_service account.
  - a. Enter the **Password** for this account, specified during Step 2.
  - b. Enter this same password again in the **Confirm password** field.

**NOTE**: If modifying an existing AD Agent installation and no changes need to be made to the account path or password, click the "Do not update service account settings" checkbox to bypass this option.

c. Click **Next** to display the page that lets you specify the role of AD Agent on this machine being configured:

🔤 8e6 AD Agent	_ 🗆 X
Select an agent role for this computer. A Primary agent can operate independently, or it can be the central control station for a team of agents. A Satellite agent can only operate as a subordinate member of a team, reporting its results to a Primary agent. Click Help for additional information about agent roles. If you're uncettain, or this is the first agent installed. the recommended estection is Primary.	
Help	
Role: Primary	
If this computer is to be a Satellite agent, provide the name of the Primary agent computer to which it will report.	
Primary agent computer name:	
Cancel < Back	Next >

Fig. A-11 Specify role of AD Agent on current machine

- 3. By default, the **Role** of the AD Agent on the current machine being configured is "Primary"—indicating that this is either the only machine running AD Agent, or this is the central machine among a team comprised of one or more "Satellite" machines running AD Agent.
  - If the role of this AD Agent is "Primary" Do the following:
    - a. Make sure "Primary" is selected.
    - b. Click **Next** to display the page for specifying R3000 criteria (see Fig. A-12).
  - If the role of this AD Agent is "Satellite" Do the following:
    - a. Select "Satellite".

- b. Enter the **Primary agent computer name** that will delegate to this machine the areas of the network to scan for end user logon/logoff events. This satellite machine running the AD Agent will send its logon/logoff event data to the primary machine running the AD Agent.
- c. Click **Next** to display the confirmation page (see Fig. A-13).
- 4. If configuring a primary AD Agent, make the following entries in the appropriate fields:

🛀 8e6 AD Agenl	t			
	This information is used when the AD 8e6 filter appliance.	Agent transmits user sessio	n information to the	
	Enable transmissions to	this appliance.	Help	
	Appliance address:	200.10.100.23		
	Port	26267		
	Appliance passphrase:	REPRESENT		
	(Repeat passphrase):	жиник		
	Descriptive name:	Filter #1		
	Normally the AD Agent sends small up only new user sessions. In some cas on the filter appliance), it can be usefi	es (such as when maintena		
		Cano	el < Back	Next >

Fig. A-12 R3000 criteria

- a. Enable transmissions to this appliance Click this checkbox to enable the AD Agent configured on the current machine to send information to the R3000 specified in this page.
- b. **Appliance address** Enter the IP address of the R3000 that will receive AD Agent logon/logoff event information.
- c. **Port** By default, "26267" displays for the R3000's port. This port number should only be changed if the R3000 is using a different port number.

- d. **Appliance passphrase** Enter the passphrase that was entered in the Passphrase field in the AD Agent Settings pop-up window (accessible via the Enable/ Disable Authentication window).
- e. (**Repeat passphrase**) Re-enter the passphrase entered in the previous field.
- f. **Descriptive name** By default "Filter #1" displays. A descriptive name for the R3000 can be entered in this field.
- After configuring the AD Agent in either a primary or satellite role, click **Next** to display the confirmation page, indicating whether the AD Agent started up successfully:

🔤 8e6 AD Agent	_ 🗆 X
The AD Agent service started successfully.	
When you click Close, the AD Agent control panel will open. You can make advanced configuration changes with the control panel if needed.	
OS Version is Microsoft Windows NT 5.1.2600 Service Pack 2 Reading Active Directory domain tree Skipping service account changes	
Skipping service account changes Granting Ulic ontrol to doagent_services for directory C:\Program Files\9e6 Technologies\8e6 DC Agen Directory recursion completed, 17 directories updated. Granting access to HKLM\SOFTWARE\9e6DCAgent for dcagent_services group ACL adjustment completed Saving configuration file C:\Program Files\9e6 Technologies\8e6 DC Agent\bin\dcagent.config Enabling doba work allocation	it and
E nating gobierrow and and and Stating service Service started successfully, configuration completed.	
	•
Copy to Clipboard	
Cancel < Back	Close

Fig. A-13 Confirmation information

**TIP**: Any errors during the configuration wizard process display in red text. If errors are present, or if any instructions are marked "MANUAL ACTION REQUIRED," use the Copy to Clipboard button to capture the log for reference by 8e6 Technical Support.

 After the configuration wizard has successfully completed, click Close to close the AD Agent configuration wizard and to launch the Active Directory Agent console, displaying today's Activity log (see Fig. A-14). **NOTE**: Information about how to view and use the Activity log is explained in the Activity tab section of Use the Active Directory Agent console.

## Use the Active Directory Agent console

The Active Directory Agent console is used for displaying results of workstation probe searches, for running or stopping the AD Agent service, and for configuring a primary AD Agent or Agent team.

**TIP**: To access the Active Directory Agent console after the initial setup process, go to Start on the Windows machine, and from the 8e6 AD Agent menu select AD Agent Control Panel.

#### Activity tab

Activity displays by default at the end of the configuration wizard process or if the AD Agent was configured as a satellite, and also whenever the Activity tab is clicked in the Active Directory Agent console of a primary AD Agent:

essions				- <u>6666</u> ,666
	Activity			
			_	
				11
onngurao	on 📑 View	as text 🏢	View as sprea	dsheet
				Loaded 5000 activity log records for today.
ime	Application	Level	Channel	Message
2:18:59	NetScan	App	Netsca	printSession Fwd_to_collector @ISE.1.13 200.10.101.101 RAP-SERVER1 Administrator LOGOD Y Unknown 2007-01-26 20
2.19.00	NetScan	Module	Netsca	Host 200.10.101.136 error #5 in NefW/kstaUserEnum
2:19:00	NetScan	Module	Netsca	NwkstaProbe 236 Error probing 200.10.101.136, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
2:19:00	NetScan	Module	Netsca	Host 200.10.101.00 error #5 in Nefw/kstaUserEnum
2:19:00	NetScan	Module	Netsca	Host 200.10.100.241 error #5 in Nefw/kstaUserEnum
219:00	NetScan	Module	Netsca	NwkstaProbe 71 Error probing 200.10.101.80, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
2.19.00	NelScan	Module	Netsca	NwkstaProbe 307 Error probing 200.10.100.241, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
2:19:01	NetScan	Detail	Netsca	NwkstaProbe 130 User login re-confirmed for logoo\tspuna at 200.103.103.154
2:19:01	NetScan	App	Netsca	printSession Fwd_to_collector @4SE.1.13 200.10.101.136 ED.AC-RCHRISTIAS N Unknown 2007-01-26 20:19:00 Z 0001-
2:19:01	NetScan NetScan	App App	Netsca	printSession Fwd_to_collector @/SE.1.13 200.10.100.241 ADMIN-AMILLAR_N_Urknown 2007-01-26 20:19:00.2_0001-01- printSession Fwd_to_collector @/SE.1.13 200.10.101.80 QC/wCHAUNA_N_Urknown 2007-01-26 20:19:00.2_0001-01-01
219:01	NelScan	App App	Netsca	printSession Fwd_to_collector @YSE.1.13.200.103.143.154 SALES-TSPAN tspuna L0G00 Y Interactive 2007-01-26.20
219.02	NetScan	Detail	Netsca	NwkstaProbe 284 User login re-confirmed for logicol-administrator at 200.10.101.84
2:19:02	NetScan	App	Netsca	printSession Fwd. to: collector @4SE.1.13 200.10.101.84 RAP-SERVER2 Administrator L0G00 Y Unknown 2007-01-26 20:
2:19:02	Transmit	App	TxSocket	
219:02	NetScan	Module	Netana	Host 200.10.101.79 error #5 in Nefwikstal JaerEnum
219.02	NelScan	Module	Netsca	NwkstaProbe 174 Enor probing 200.10.101.79, enor is E455 / E. NwsklaWorkstationProbe. Access/Denied
2.19.02	NetScan	App	Netsca	printSession Find to collector @4SE.1.13 200.10.101.79 QC-RNAGANA N Unknown 2007-01-26 20.19.02 Z 0001-01-01 0
2:19:03	NetScan	Module	Netsca	Host 200.10.101.142 error #5 in NefWkstaUserEnum
2:19:03	NetScan	Module	Netsca	NwkstaProbe 161 Error probing 200.10.101.142, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
2:19:03	NetScan	App	Netsca	printSession Fwd_to_collector @ISE.1.13 200.10.101.142 EDAC/AFANA N Unknown 2007-01-26 20:19:03 Z 0001-01-01
2:19:03	NetScan	Module	Netsca	Host 200.10.101.181 error #5 in NefwikstaUserEnum
2.19.03	NetScan	Module	Netsca	NwkstaProbe 152 Error probing 200.10.101.181, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
2.19.03	NetScan	App	Netsca	printSession Fwd_to_collector @4SE.1.13 200.10.101.181 EDAC-FAAI N Unknown 2007-01-26 20.19.03 Z 0001-01-01 00
2:19:04	NetScan	Module	Netsca	Host 200.10.101.81 error #5 in NefWkstaUserEnum
2:19:04	NetScan	Module	Netsca	NwkstaProbe 244 Error probing 200.10.101.81, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
2:19:04	NetScan	App	Netsca	printSession Fwd_to_collector @ISE.1.13 200.10.101.81 QCAAIA2 N Unknown 2007/01/26 20.19:04/2 0001-01-01 00:00
219:04	Transmit	App	TxSocket	[200.10.100.235:4494>200.10.101.174.26267] Connected.
219.04	Transmit	Detail	TxResp	CONNECT SUCCESS 200.10.101.174/26267

Fig. A-14 Primary AD Agent console, Activity tab

In this tab the activity log displays, comprised of rows of records for the most recent activity on the current machine running the AD Agent. The most recent activity displays at the bottom of the log.

**TIP**: To stop the activity log from automatically scrolling, rightclick in the table and de-select the "Auto-scroll" checkbox. Click this checkbox again to enable automatic scrolling.

For each row in this table, information is included in the following columns:

- Time time the activity was logged (in local military time, using the HH:MM:SS format).
- Application program in AD Agent that produced the record (e.g. Netscan, Transmit, Monitor, Collector, Logscan).
- Level severity of the filter used by the application (e.g. App, Error, Detail, Module).
- Channel type of information that was logged for the record, as defined by the application and its configuration file contents (e.g. NetscanWorkstationProbe, Transmit-Control, CollectorIntake, EventLogParsing).
- Message detailed information about activity for that record.

**NOTE**: Any record that displays in red text indicates an error on the server. All errors reported in this log will be sent in a daily email message to the designated administrator (see the Notifications page Active Directory Agent Configuration window ). The following actions can be performed via the Activity tab:

- View/download the activity log in the text file format -Click the **View as text** button to launch a Notepad file containing the contents of the activity log.
- View/download the activity log in the Excel spreadsheet format - Click the View as spreadsheet button to launch a spreadsheet in Microsoft Excel containing the contents of the activity log.
- View/modify primary AD Agent configuration, stop/start AD Agent service - Click the **Configuration** button to open a pop-up window containing AD Agent configuration tools and configured settings (see Active Directory Agent Configuration window).

#### Sessions tab

Sessions displays by default when the Active Directory Agent console is launched on a machine running the AD Agent in the primary role, or whenever the Sessions tab is clicked in the console of a primary AD Agent:

session:         Activity           configuration	CO ACCIV	e Directory	Agent	in the	0		
Importion         Importes	Activity	1					 
166.284.07.15         GCDAA         0/01 0000         0/23 00.20           101         191.060.010         GCCFARB         0/01 00000         0/23 1050           2 domininutor         2001.001.015         RAP-SERVP11         0/22 00.42         L00000         0/23 1050           2 domininutor         2001.001.015         RAP-SERVP11         0/22 00.42         L00000         0/25 00.20           2 domininutor         2001.001.0105         RAP-SERVP11         0/22 00.42         L00000         0/25 00.20           2 domininutor         2001.001.0105         RAP-SERVP11         0/25 00.23         L00000         0/25 00.23           2 domininutor         2001.001.0105         RALES-M6RD         0/75 00.23         L06000         0/25 00.23           2 domininutor         0001.001.1013         SALES-M6RD         0/1/25 00.23         L06000         0/1/25 00.23           2 domininutor         0001.001.1013         SALES-M6RD         0/1/25 00.23         L06000         0/1/25 00.23           2 domininutari         L000.001.1014         E00C D1A'         0/1/10.000         0/1/25 00.23         L0600         0/1/25 00.23           2 domininutari         L000.001.1014         SALES-M0LL         0/1/25 00.23         L0600         0/1/25 00.23         L0600         <			obe workstation 🗮 Vie	w as spreadsheet			
193         163         101         C_CEFARP         0/01         0000         0/22         1500           Administrator         2001         031025         FAP-SEFWR1         01/23         082         01/25         082.00           Administrator         2001         031025         FAP-SEFWR1         01/23         084         L0600         01/25         082.00           Administrator         2001         0310305         ACT 3VH         01/10         000         01/25         082.00           Into         2001         0310305         ACT 3VH         01/10         000         01/25         082.00           Into         2001         03103136         MARKET ANIDX         01/01         000         01/25         082.00           Into         2001         03103136         MARKET ANIDX         01/10         000         01/25         082.00           Into         2001         03103136         MARKET ANIDX         01/10         000         01/25         082.00           Into         2001         03103142         SALES-FROID         01/25         082.00         01/25         082.00           Into         2001         03103142         SALES-FROID         01/25	ser	IP Address	Workstation	Login	Error Domain	Ventied	
Administrative         200.103.1035         RAP-SERVP11         01/23.0042         L0000         01/25.0023           Administrative         200.103.1038         RAP-SERVP31         01/23.0044         L05000         01/25.0023           Imb         200.103.1038         RAP-SERVP32         01/23.0044         L05000         01/25.0023           Imb         200.103.1038         RADELSVP3         01/01.000         01/25.0023         L05000           Imb         200.103.103.15         MARESERINGK         01/01.00.00         01/25.0023         L05000         01/25.0023           Imd         200.103.103.15         GARLES-FINDCK         01/01.00.00         01/25.0023         L05000         01/25.0023           Imd         200.103.103.114         ED0CD1AV         01/01.00.00         01/25.0023         L05000         01/25.0023           Imd         200.103.103.114         ED0CD1AV         01/01.00.00         01/25.0023         L0500         01/25.0023           Imd         200.103.103.14         ED0CD1AV         01/25.0023         L0500         01/25.0023           Imd         200.103.103.15         SALES-FABUL         01/25.0023         L0500         01/25.0023           Imda         200.103.103.15         SALES-FABUL         01/25.0023 </td <td></td> <td>166.254.97.15</td> <td>QC-DAR</td> <td>01/01 00:00</td> <td></td> <td>01/25 08:29</td> <td></td>		166.254.97.15	QC-DAR	01/01 00:00		01/25 08:29	
Administrative         2001 103 1038         RAP SERVR2         01/23 108 41         L0G00         01/25 108 28           pto         2001 103 1038         AGETSVF         01/10 1000         01/25 108 29           pto         2001 103 1038         AGETSVF         01/10 1000         01/25 108 29           pto         2001 103 1038         AGESVF         01/10 1000         01/25 108 29           red         2001 103 1038         AGESVF         01/10 1000         01/25 108 29           administration         2001 103 1038         AGESVF         01/10 1000         01/25 108 29           administration         2001 103 1038         AGESVF         01/10 1000         01/25 108 29           administration         2001 103 1038         AGESVF         01/10 1000         01/25 108 29           administration         2001 103 1038         AGESVF         01/10 1000         01/25 108 29           administration         2001 103 1142         SALES FOLUE         01/25 108 29         L0G00         01/25 108 29           administration         2001 103 1142         SALES FOLUE         01/25 108 28         L0G00         01/25 108 29           administration         2001 103 1151         SALES FOLUE         01/25 108 28         L0G00         01/25 108 29	1	199.168.30.10	QC-EFARR	01/01 00:00		01/23 15:09	
200         001 <td></td> <td>200.103.103.5</td> <td>RAP-SERVR1</td> <td>01/23 08:42</td> <td>LOGOO</td> <td>01/25 08:28</td> <td></td>		200.103.103.5	RAP-SERVR1	01/23 08:42	LOGOO	01/25 08:28	
Jub         200.003.013.11         SALES-VAIGN         01/25 08.29         L0G00         01/25 08.29           Incd         200.103.103.13         SALES-AVIGN         01/25 08.29         L0G00         01/25 08.29           Incd         200.103.103.16         GAGAPTOP         01/01 00.00         01/25 08.29           200.103.103.10         GAGAPTOP         01/01 00.00         01/25 08.29           200.103.103.10         GAGAPTOP         01/01 00.00         01/25 08.29           200.103.103.11         SALES-FRADU         01/01 00.00         01/25 08.29           200.03.103.114         SALES-COUS         01/01 00.00         01/25 08.29           200.03.103.114         SALES-FRADU         01/01 00.00         01/25 08.29           200.03.103.114         SALES-FRADU         01/01 00.00         01/25 08.29           200.03.103.114         SALES-FRADU         01/25 08.23         L0G00         01/25 08.29           200.03.103.115         SALES-FRADU         01/25 08.23         L0G00         01/25 08.29           201.03.103.115         SALES-FRADU         01/01 00.00         01/25 08.29           200.03.103.115         SALES-FRADU         01/01 00.00         01/25 08.29           200.03.103.115         SALES-FRADU         01/01 00.00		200.103.103.6	RAP-SERVR2	01/23 08:41	LOGOO	01/25 08:28	
1         200.003.138         MARKET SNICK         07/07.00.00         07/25.08.29           1         200.003.003.03         SALES-ARDO         07/25.09.29         LOGOO         07/25.09.29           1         200.003.03.09         BARLS-ARDO         07/01.00.00         07/25.09.29           1         200.003.03.09         BARLS-ARDO         07/01.00.00         07/25.09.29           1         200.003.03.03.14         BALES-CREAD         07/25.09.29         LOGOO         07/25.09.29           1         200.03.103.14         SALES-CREAD         07/25.09.29         LOGOO         07/25.09.29           1         200.103.103.15         SALES-CRUE         07/25.09.29         LOGOO         07/25.09.29           1         200.103.103.15         SALES-ARUL         07/25.09.29         07/25.09.29 <td></td> <td>200.103.103.66</td> <td>ACCT-SVR</td> <td>01/01 00:00</td> <td></td> <td>01/25 08:29</td> <td></td>		200.103.103.66	ACCT-SVR	01/01 00:00		01/25 08:29	
mod         200.033.013.17         SALES-ARDOD         01/25.00.23         LOGOD         01/25.00.23           200.033.003.101         60ALPTOP         01/01.000         01/25.00.23         01/25.00.23           200.033.003.101         EDDC.DTA/         01/01.000         01/25.00.23         01/25.00.23           200.033.003.101         EDDC.DTA/         01/01.000         01/25.00.23         01/25.00.23           200.033.003.101         EDDC.DTA/         01/01.000         01/25.00.23         01/25.00.23           200.033.003.104         SALES-ACDUE         01/25.00.23         LOGOD         01/25.00.23           obag         200.033.03.104         SALES-ACDUE         01/25.00.23         LOGOD         01/25.00.23           yade         200.033.03.104         SALES-ACDUE         01/25.00.23         LOGOD         01/25.00.23           yade         200.033.03.15         SALES-ACAU         01/25.00.23         LOGOD         01/25.00.23           yade         200.033.03.15         SALES-ACAU         01/25.00.23         LOGOD         01/25.00.23           yade         200.033.03.15         SALES-ACAU         01/01.00.00         01/25.00.23           yade         200.033.03.15         SALES-ACAU         01/01.00.00         01/25.00.23		200.103.103.131	SALES-JVIGN	01/25 08:29	LOGOO	01/25 08:29	
200.103.103         0.662.AFTOP         01/01.000         01/25.06.25           200.103.103.104         0.660.AFTOP         01/01.000         01/25.06.25           200.003.103.142         0.600.CTAX         01/01.000         01/25.06.25           200.103.103.142         0.610.FTM6.576         0.1/01.000         01/25.06.25           200.103.103.142         0.610.FTM6.576         0.1/01.000         01/25.06.25           200.103.103.151         SALES-CDUB         01/25.06.25         LIGGOD         01/25.06.25           200.103.103.151         SALES-ARLL         01/25.06.25         LIGGOD         01/25.06.25           200.103.103.151         SALES-ARLL         01/25.06.25         LIGGOD         01/25.06.25           200.103.103.151         SALES-ARLL         01/25.06.25         LIGGOD         01/25.06.25           200.103.103.153         MAINETAKE         01/01.00.00         01/25.06.25         LIGGOD         01/25.06.25           200.103.103.154         SALES-ARLL         01/25.06.25         LIGGOD         01/25.06.25         LIGGOD         01/25.06.26           200.103.103.154         SALES-ARLL         01/25.06.25         LIGGOD         01/25.06.26         LIGGOD         01/25.06.26           200.103.103.155         HR-HICK         0.01/10.0	1	200.103.103.136	MARKET-SNICK	01/01 00.00		01/25 08:29	
200.033103141         EDDC DTA'         01/10 00,0         01/25 08,25           cbox         200.033103142         SALES-CRERO         01/25 08,25         L/0600         01/25 08,23           cobx         200.033103144         SALES-CRERO         01/25 08,23         L/0600         01/25 08,23           cobx         200.033103145         SALES-ACUUS         01/25 08,23         L/0600         01/25 08,23           rgabr         200.03310315         SALES-ACUUS         01/25 08,23         L/0600         01/25 08,23           abl         200.03310315         SALES-ACUUS         01/25 08,23         L/0600         01/25 08,23           abl         200.0310315         SALES-ACUUS         01/25 08,23         L/0600         01/25 08,23           abl         200.0310315         SALES-ACUUS         01/25 08,28         L/0600         01/25 08,23           bipum         200.03103154         SALES-AFRINN         01/25 08,28         L/0600         01/25 08,23           pade         200.03103154         SALES-AFRINN         01/17 08/07         L/0600         01/25 08,23           pade         200.03103157         SALES-AFRINN         01/17 08/07         L/0600         01/25 08,23           pade         200.03103157         SALES-AFRINN </td <td>bom</td> <td>200.103.103.137</td> <td>SALES-RROD</td> <td>01/25 00:29</td> <td>L0600</td> <td>01/25 08:29</td> <td></td>	bom	200.103.103.137	SALES-RROD	01/25 00:29	L0600	01/25 08:29	
Internet         2001 033 1034 / 2         SALES-CRERD         01/25 0828         LIGGD0         01/25 0828           Internet         0001 033 1034 / 4         SALES-CRUIS         07/25 0828         LIGGD0         01/25 0828           Internet         0001 033 1034 / 4         SALES-ROLUS         07/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 4         SALES-ROLUS         07/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 5         SALES-RALL         01/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 5         SALES-RALL         01/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 5         HR-HICK         01/01 000         01/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 5         HR-HICK         01/01 000         01/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 5         HR-HICK         01/01 000         01/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 5         HR-HICK         01/01 000         01/25 0828         LIGGD0         01/25 0828           Ingular         2001 033 1031 / 5		200.103.103.138	BAGLAPTOP	01/01 00:00		01/25 08:29	
2001103103144         ACCTING SYS         07/17 00:00         07/25 08:20           rodup         2001103103145         SALES-CDUG         07/25 08:23         L0GO0         07/25 08:23           radi         20011031031051         SALES-AGULL         07/25 08:23         L0GO0         07/25 08:23           radi         2001103103155         SALES-AGULL         07/25 08:23         L0GO0         07/25 08:23           radi         200110310315         SALES-AGULL         07/25 08:23         L0GO0         07/25 08:23           radi         200110310315         MARKETAKE         07/25 08:28         L0GO0         07/25 08:28           rbipun         2001103103154         SALES-STEINN         07/25 08:28         L0GO0         07/25 08:20           rbipun         2001103103154         SALES-STEINN         07/07 08:27         L0GO0         07/25 08:20           rbipun         2001103103156         TECH-STEINN         07/07 08:27         L0GO0         07/25 08:20           rbipun         2001103103156         SALES-SMD0B8         07/07 08:21         L0GO0         07/25 08:23           rbipun         2001103103161         SALES-SMD0B8         07/07 06:20         07/25 08:23         07/25 08:23           padeb         2001103103161		200.103.103.141	EDOC/DTAY	01/01 00:00		01/25 08:29	
Jokg         200103103149         SALES-FOLUE         01/25 0823         L0G00         01/25 0823           Judie         200103103165         SALES-FADLL         01/25 0823         L0G00         01/25 0823           Judie         200103103165         SALES-FADLL         01/25 0823         L0G00         01/25 0823           Judie         200103103151         SALES-FADLL         01/25 0823         L0G00         01/25 0823           Judie         200103103151         SALES-FAPL         01/25 0828         L0G00         01/25 0828           Jumin         200103103154         HR-HICK         01/01 000         01/25 0828         01/25 0828           Jumin         200103103155         HR-HICK         01/01 000         01/25 0828         01/25 0828           Jumin         200103103155         HR-HICK         01/01 000         01/25 0828         01/25 0828           Jumin         200103103155         HR-HICK         01/01 000         01/25 0828         01/25 0828           Judie         200103103157         SALES-FORD         01/01 70827         L0G00         01/25 0828           Judie         200103103157         SALES-FORD         01/01 70725         L0G00         01/25 0828           Judie         200103103161	cbro	200.103.103.142	SALES-CBR0	01/25 08:29	L0G00	01/25 08:29	
yguin         200.103.101.00         SALES-RADALL         01/25.00.23         LOGOD         01/25.00.23           aui         200.103.103.15         SALES-AAL         01/25.00.23         LOGOD         01/25.00.23           aui         200.103.103.15         SALES-AAL         01/25.00.23         LOGOD         01/25.00.23           truum         200.103.103.15         SALES-FRINN         01/25.00.23         LOGOD         01/25.00.23           1         200.103.103.154         SALES-TRINN         01/25.00.23         LOGOD         01/25.00.23           1         200.103.103.154         HAUHICK         01/01.00.00         01/25.00.23         01/25.00.23           1         200.103.103.154         HSLHICK         01/01.00.00         01/25.00.23         01/25.00.23           1         200.103.103.156         TECH-JEDIN         01/01.00.00         01/25.00.23         01/25.00.23           1         200.103.103.156         SALES-FOEL         01/01.00.00         01/25.00.23         01/25.00.23           2         200.103.103.161         SALES-FOED         01/01.00.00         01/25.00.23         01/25.00.23           2         200.103.103.161         SALES-FOED         01/01.00.00         01/25.00.23         01/25.00.23         01/25.00.23	1	200.103.103.144	ACCTING-SY8	01/01 00.00		01/25 08:30	
Juit         200103103151         SALES-AAL         01/25 0023         LOGGO         01/25 0023           1         200103103153         MARETAKE         01/01 0000         E455         01/23 1010           1         200103103154         SALES 15FUN         01/25 0028         LOGGO         01/25 0028           1         200103103154         SALES 15FUN         01/25 0028         LOGGO         01/25 0028           1         200103103154         FE0-AGIN         01/27 0807         LOGGO         01/25 0828           1         200103103154         FE0-AGIN         01/77 0827         LOGGO         01/25 0828           1         200103103154         SALES-500B         01/17 0827         LOGGO         01/25 0828           2         200103103154         SALES-500B         01/01 707.25         LOGGO         01/25 0828           2         200103103161         SALES-500B         01/17 077.25         LOGGO         01/25 0828           2         200103103161         SALES-500B         01/17 077.25         LOGGO         01/25 0828           2         200103103161         SALES-500B         01/17 077.25         LOGGO         01/25 0828	colug	200.103.103.149	SALES-CDUG	01/25 08:29	LOGOO	01/25 08:29	
200.103.103.153         MARKET N4KE         01/01.00.00         E455         01/23.10.16           2 htpun         200.103.103.154         SALES.TSPUN         01/25.08.28         LGGGD         01/25.08.28           2 00.103.103.154         SALES.TSPUN         01/25.08.28         LGGGD         01/25.08.28           2 00.103.103.154         TRUHICX         01/01.00.0         01/25.08.28         01/25.08.28           2 min         2 00.103.103.154         TECH-KEINI         01/17.08.07         LGGD0         01/25.08.29           3 mideb         2 00.103.103.154         SALES-MOLB         01/01.00.00         01/25.08.29         01/25.08.29           4 200.103.103.155         SALES-ODE         01/01.00.00         01/25.08.29         01/25.08.29           6 pdsb         200.103.103.15         SALES-ODE         01/01.00.00         01/25.08.29           7 pdsb         200.103.103.15         SALES-ODE         01/01.00.00         01/25.08.29           9 pdsb         200.103.103.15         SALES-ADOLB         01/01.00.00         01/25.08.29           9 pdsb         200.103.103.15         SALES-ADOLB         01/01.00.00         01/25.08.29           9 pdsb         200.103.103.16         SALES-ADOLB         01/01.00.00         01/25.08.29		200.103.103.150	SALES-RGALL	01/25 08:29	LOGOO	01/25 08:29	
Ippen         200103103154         SALES1STEIN         01/250828         L0G00         01/250828           200103103155         HN-HICK         01/01000         01/250828         01/250828           Pede         200103103155         TECH-JEDIN         01/170827         L0G00         01/250828           Pedeb         200103103157         SALES40088         01/170821         L0G00         01/250828           Pedeb         200103103157         SALES40088         01/170821         L0G00         01/250828           200103103157         SALES40088         01/170821         L0G00         01/250828           200103103161         SALES4008         01/0170726         L0G00         01/250828           200103103161         SALES4008         01/0170726         L0G00         01/250828           200103103161         SALES4009         01/0170726         L0G00         01/250828		200.103.103.151	SALES-AAL	01/25 00:29	L0600	01/25 08:29	
J         200.103.103.195         HR.HHCK         01/01.00.00         01/25.08.20           Jmdin         200.103.103.196         TECH-JEDIN         01/27.08.07         L.00600         01/25.08.29           Jmdubb         200.103.103.195         SALES-MOUBB         01/17.08.07         L.00600         01/25.08.29           J         200.103.103.195         SALES-MOUBB         01/17.07.21         L.00600         01/25.09.29           J         200.103.103.195         SALES-FD0B         01/07.07.26         L.00600         01/25.09.28           J         200.103.103.115         SALES-APDB         01/07.07.26         L.00600         01/25.09.28           J         200.103.103.116         SALES-APDB         01/07.07.26         L.00600         01/25.09.28		200.103.103.153	MARKET-MKE	01/01 00:00	E455	01/23 10:18	
Jmdn         2001103103156         TECH-IEOIN         01/17 08/07         L.0600         01/25 08/29           Imdabb         2001103103157         SALES-MD088         01/17 08/21         L0G00         01/25 08/29           S         2001103103155         SALES-PCID         01/01 08/00         01/25 08/29           J pado         2001103103165         SALES-PCID         01/01 10/00         01/25 08/29           J pado         2001103103165         SALES-PCID         01/01 10/00         01/25 08/29           J pado         2001103103165         SALES-PCID         01/01 10/00         01/25 08/29		200.103.103.154		01/25 08:28	LOGOO	01/25 08:28	
mdubb         200.103.103.157         SALES-MD/0BB         01/17.08.21         L/0G00         01/25.08.29           1         200.103.103.159         SALES-PDL         01/01.000.0         01/25.08.29           2x00.103.103.161         SALES-PD0B         01/01.07.256         L0G00         01/25.08.28           2x00.103.103.161         SALES-PD0B         01/07.07.256         L0G00         01/25.08.28           2x00.103.103.161         SALES-PD0B         01/07.07.256         L0G000         01/25.08.28		200.103.103.155		01/01 00:00		01/25 08:30	
200.103.103.159         SALES-DEL         01/01.00.00         01/25.00.23           pdob         200.103.101.61         SALES-APD.00         01/71.707.26         LOGO0         01/25.00.23           200.103.103.101.61         SALES-APD.00         01/01.00.00         01/25.00.23         01/25.00.23		200.103.103.156	TECH-JEDIN	01/17 09.07	LOGOO	01/25 08:29	
Podob 200.103.103.161 SALES-FD08 01/17.07.26 L0G00 01/25.08.29 200.103.103.162 SALES-AAR 01/01.00.00 01/25.08.29					LOGOO		
200.103.103.162 SALES-AAR 01/01.00.00 01/25.08.20		200.103.103.159					
		200.103.103.161	SALES-PD08	01/17 07:26	L0600	01/25 08:28	
		200.103.103.162	SALES-AAR	01/01 00:00		01/25 08:28	
gdia 200.103.103.163 SALES-GDIA 01/17.06.13 L0G00 01/25.08.28	gdia	200.103.103.163	SALES-GDIA	01/17 06:13	L0G00	01/25 08:28	
abrun 200.103.103.164 SALES-ABRUN 01/25.08.28 L0G00 01/25.08.28	abrun	200.103.103.164	SALES-ABRUN	01/25 08:28	L0G00	01/25 08:28	

Fig. A-15 Primary AD Agent console, Session tab



**NOTE**: The Sessions tab does not display on machines configured to run AD Agent in the satellite role.

In this tab the session table displays, comprised of rows of end user login/logout activity records retrieved by probes set up on all servers (primary and satellite) running the AD Agent. For each row in this table, information is included in the following columns:

- User User profile icon and user name set up on the Windows server, or machine icon and no user name if a user was not detected at the designated workstation.
- IP Address IP address of the workstation.
- Workstation Network name of the workstation.

- Login Date and time the end user last logged in (using the MM/YY HH:MM military time format). If 01/01 00:00 displays, the end user has not logged on at that workstation since the AD Agent service was installed on the network.
- Error If an error code displays, see Troubleshooting at http://www.8e6.com/r3000help/adagent/ 6troubleshoot.html for a list of probe error codes and their corresponding issues.
- Domain Name of the domain to which the user account belongs.
- Verified Date and time (using the MM/YY HH:MM military time format) when the workstation's status was last verified.

The following actions can be performed in the Sessions tab:

- Sort session table data Click a column header to sort all rows in the table in descending order by that column. Click the column header again to resort all rows in the table in ascending order by that column.
- View/download the session table in the Excel spreadsheet format - Click the View as spreadsheet button to launch a spreadsheet in Microsoft Excel containing the contents of the session table, plus additional columns of data (see Session table spreadsheet).
- View Properties of an end user's record The Sessions Properties window shows detailed information about a record in the session table, and is accessible by clicking the Properties button, or double-clicking or right-clicking the end user's record (see Session Properties window).
- Probe a workstation The Workstation Interactive Probe window provides tools to probe a workstation on demand, and is accessible by clicking the Probe workstation button, or right-clicking the end user's record (see Workstation Interactive Probe window).

 View/modify primary AD Agent configuration, stop/start AD Agent service - Click the **Configuration** button to open a pop-up window containing AD Agent configuration tools and configured settings (see Active Directory Agent Configuration window).

#### Session table spreadsheet

The session table spreadsheet contains the contents of the current session table plus these additional columns of data: Record Type; Logged in ("Y" or "N"); Login type ("Interactive" if the end user is logged in and detected by the probe, or "Unknown" if the end user is not logged in or is undetected by the probe); Last update date and Verified time (each using the YYYY-MM-DD HH:MM:SS military time format), Update source (type of probe used), and Quality of the data source (percentage).

#### **Session Properties window**

- 1. To view detailed information about a record in the session table, do one of the following:
  - Double-click the record in the session table to open the Session Properties pop-up window

or

 Click the record in the session table, and then click the Properties button to open the Session Properties popup window

or

• Right-click the record in the session table, and then select Properties from the pop-up menu to open the Session Properties pop-up window:

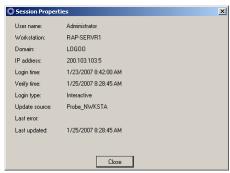


Fig. A-16 Session Properties window

This pop-up window contains the following information: User name; Workstation name; Domain name; IP address; Login time and Verify time (each using the M/ D/YYYY H:M:SS AM/PM format); Login type ("Interactive" if the user is logged in and detected by the probe, "Unknown" if the user is not logged in or is undetected by the probe); Update source (type of probe used); Last error (an error code displays if the probe failed to successfully identify the end user); Last updated (shows the time data last changed for the end user's workstation, using the M/D/YYYY H:M:SS AM/PM format).

2. After viewing the contents of this pop-up window, click **Close** to close the window.

#### Workstation Interactive Probe window

- 1. To access tools to probe a workstation on demand, do one of the following:
  - Click the record in the session table, and then click the Probe workstation button to open the Workstation Interactive Probe pop-up window

or

 Right-click the record in the session table, and then select Probe Workstation from the pop-up menu to open the Workstation Interactive Probe pop-up window:

IP Ac	dress: 20	0.103.103.5	Nwksta Pi	robe WM	II Probe		Clear log		🗙 Close					
01	4	In-memory sessio	n table rea	and for this	weiketsti	on: U.U.C	COOVAdmi	nistrator	IP-200 102	102 5 1	ADAD C	DI/D1	111-017	DE 22.7
01	Å.	Extended attribut						riisu auor	. 16.200.10.	. 103.3 . V	V.HMP130	nyni	. LO.0172	50 20.4
01	4	NwstaProbe	16				dministrator	. IP:200	103.103.5	W:BAP-	SERVR1	. LU:01.	/25 23:40	):38 Z
01	4	NwkstaProbe	15	User lo	in re-con	firmed fo	r logoo\adm	inistrator	at 200.10.1	01.101				
robe c	ompleted,	result=200					-							
00	Success	@ISE.1.13		101.101	RAP-S		Admini		LOGO				7-01-26 1	
01	4	In-memory sessio	in table reci	ord for this	workstati	on: U:LC	)GOO\Admi	nistrator	. IP:200.103	103.5 . \	√:RAP-SI	ERVR1	. LU:01/2	25 23:4
01	4	Extended attribut		ng.lp=1/2	5/2007 3:	42:21 PI	м							
01	4	WmiProbe	15	Starting	WMI proi	be on m	achine 200."	103.103.	5					
_	1600\Adr	1.1.4												<u> </u>

Fig. A-17 Workstation Interactive Probe window

The IP Address of the workstation displays above the blank screen, along with the following buttons: Nwksta Probe, WMI Probe, Clear log, X Close.

Beneath the blank screen, the following information displays: User domain name and username, Workstation name.

- 2. Click either of the probe buttons to activate the probe search on demand:
  - **Nwksta Probe** this is the default probe used for identifying workstations. This probe requires the user's domain account to have administrator permissions on the workstation if running on a Windows 2000 Professional operating system.
  - WMI Probe this probe is disabled by default and can be enabled via the Options page in the Active Directory Agent Configuration window. This probe (which takes longer to identify an end user) requires the dcagent\_service account to be a Domain Admins group member.



**NOTE**: An error code displays in the probe results if the probe fails to run successfully. Consult the list of troubleshooting codes for more information about the error.



**TIP**: Click Clear log to clear the screen of probe results.

3. After performing the necessary actions in this window, click **X Close** to close the window.

## Active Directory Agent Configuration window

The Active Directory Agent Configuration window lets you modify settings for the AD Agent team, if there are changes to the AD Agent setup or to the R3000 on your network. For satellite hosts, most of this information can only be viewed on the pages in this window, but the role of the AD Agent can be changed from satellite to primary, and the service also can be stopped or started.

 Click Configuration on either the Session tab or Activity tab to open the Active Directory Agent Configuration window:

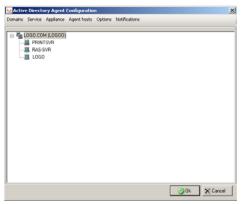


Fig. A-18 Primary host Configuration, Domains

The Domains button displays by default, showing the selection of Active Directory domains and domain controllers on your network.

- 2. Click any of the following buttons to go to the page of your selection:
  - **Service** used for viewing/modifying the status of the service, or stopping/starting the service.
  - **Appliance** used for specifying R3000 transmission criteria on the primary host, or for viewing this information on a satellite host.

- Agent hosts used for specifying the role (primary or satellite) the AD Agent will play on the current machine being configured.
- Options used for specifying configuration options for the primary host, or for viewing this information on a satellite host.
- **Notifications** used for setting up email criteria for the administrator of the primary host to be notified in the event of a critical system error, or for viewing this information on a satellite host.

**NOTES**: The Ok and Cancel buttons at the bottom of this window are deactivated by default and become activated if entries are made in any of the pages.

For satellite hosts, fields in all pages display greyed-out. The following message displays at the bottom of the window on all pages except the Service page: "These settings cannot be modified because the service mode for this machine is set to 'satellite'. The primary server (server name) can be used to make teamwide configuration".

 After making all configuration edits, click Ok to save your settings, close the Active Directory Agent Configuration window, and to restart the AD Agent.

**NOTE**: For existing satellites, changes made to the Agent team are automatically distributed, and satellite services automatically restarted.

#### Service page

1. Click Service to display the Service page:

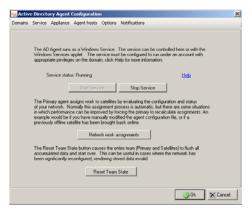


Fig. A-19 Primary host Configuration, Service

The Server status displays to indicate the status of AD Agent on the current machine: Running, StopPending, Stop, StartPending.

- 2. Perform any of the following actions:
  - **Start Service** This button is activated if the AD Agent service is not running. Clicking this button begins running the AD Agent service.
  - **Stop Service** This button is activated if the AD Agent service is running. Clicking this button stops running the AD Agent service.
  - **Refresh work assignments** This button is activated if the AD Agent service is running on the primary host. Clicking this button forces the primary Agent to recalculate the delegation of work assignments to all satellite hosts.

• Reset Team State - This button is activated if the AD Agent service is running on the primary host. Clicking this button flushes all accumulated session data for the entire team (primary and satellite hosts), except the configuration file, and newly rebuilds all data.

### Appliance page

1. Click Appliance to display the Appliance page:

Domains	e Directory Agent Configuration Service Appliance Agent hosts Op	otions Notifications	2
	The primary AD Agent sends user w filter appliance. This information is n with the appliance.		
	Enable transmissions	to this appliance.	Help
	Appliance address:	200.10.100.23	
	Port.	26267	
	Appliance passphrase:		
	(Repeat passphrase):	1000000	
	Descriptive name:	Filter #1	
	Normally life: AD Agent sends small only new use sessions. In some ci on the filter appliance), it can be use Re	ses (such as when maintena	
			Ok X Cancel

Fig. A-20 Primary host Configuration, Appliance

By default, the fields in this page are populated with entries made during the configuration wizard setup process. If necessary, changes can be made to any of these fields for the primary host.

- 2. If necessary, click the following objects on a primary host to perform the specified actions:
  - "Enable transmissions to this appliance" De-select this option if the R3000 should not be receiving data from the primary host.
  - **Resend all data** Click this button to resend the entire session table from the primary host to the R3000.

TIP: View the Activity log for transmission results.

## Agent hosts page

1. Click Agent Hosts to display the Agent hosts page:

omains	Service Appliance A	Agent hosts O	ptions Not	fications		
	only one AD Agent se	e designated as plex configuration	work, it show the primary ons, includin	id be the prin and the other a networks w	tellite" roles. If you have mary. If you have multiple rs should be satellites. For alth multiple filtering	
	Role	Prim	ary	•	Help	
	Primary	server: USM	ITH23	_		
	AD Agent servers:					
	AD Agent servers: Machine	Role	Status	1	Add_	
	Machine JSMITH23	Primary	Online	1		
	Machine JSMITH23 PJOHNSON54			I	Add Remove	
	Machine JSMITH23	Primary Satellite	Online Online	I		
	Machine JSMITH23 PJOHNSON54	Primary Satellite	Online Online	1	Remove Configuration	
	Machine JSMITH23 PJOHNSON54	Primary Satellite	Online Online	1	Remove	
	Machine JSMITH23 PJOHNSON54	Primary Satellite	Online Online	1	Remove Configuration	
	Machine JSMITH23 PJOHNSON54	Primary Satellite	Online Online	1	Remove Configuration	
	Machine JSMITH23 PJOHNSON54	Primary Satellite	Online Online	1	Remove Configuration	

Fig. A-21 Primary host Configuration, Agent hosts

By default, the fields in this page are populated with entries made during the configuration wizard setup process. The Role field displays the function of the AD Agent ("Primary" or "Satellite") on the current server. The Primary server field displays the name of the primary server—greyed-out on servers functioning as the primary host.

The AD Agent servers list box includes all AD Agent hosts that have been manually added to the list box on the primary server. This list box displays greyed-out on servers functioning as satellite hosts.

- 2. The following buttons are activated in the specified scenarios:
  - Add On a primary host server, clicking this button opens a dialog box in which a new satellite is set up and added to the list box.
  - **Remove** On a primary host server, selecting a satellite in the AD Agent servers list box and clicking this activated button removes the satellite from the list box.

- Configuration On a primary host server, selecting a satellite in the AD Agent servers list box and clicking this activated button opens a dialog box in which servers and/or workstations to be scanned by the satellite are specified.
- **Status** Selecting an AD Agent in the list box and clicking this button opens a pop-up window showing the current workload on the specified machine running the AD Agent.

#### Add a satellite

On a primary host server:

1. Click Add to open the Add New Satellite pop-up window:

Add	New Satellite
	Enter the name of the satellite machine to be added to the team. Any Windows XP, 2000, or 2003 machine can be used as a satellite.
	Satellite machines perform network scanning tasks assigned to them by the primary machine.
	You must also install the AD Agent software on the satellite machine.
	Machine name:
	Gk. Cancel
_	

Fig. A-22 Add New Satellite

- 2. Enter the **Machine name** of the Windows 2000/2003/XP machine that will function as a satellite.
- 3. Click **Ok** to accept your entry and to close the dialog box and to add your entry in the AD Agent servers list box.

#### Remove a satellite

On a primary host server:

- 1. Select the satellite Machine in the AD Agent servers list box.
- 2. Click **Remove** to remove the satellite from the list box.

#### Configure a satellite

On a primary host server:

- 1. Select the satellite Machine in the AD Agent servers list box.
- 2. Click **Configuration** to open the Satellite Agent Configuration dialog box:

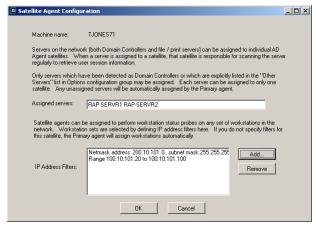


Fig. A-23 Satellite Agent Configuration

The names of Assigned servers and IP Address Filters previously entered in this dialog box display, indicating the servers and/or machines this satellite has been manually assigned to scan. If entries are not made here, the primary host will automatically assign servers/ machines for this satellite to scan.

- 3. If the satellite being added will be assigned specific servers and/or machines to scan, enter that criteria:
  - If the satellite will be manually assigned one or more specific servers to scan, enter the name(s) in the Assigned servers field, leaving a space between each server name.

If the satellite will not be manually assigned any machines on the network to scan, click **OK** to close the dialog box and to display any entries (if made) in the Assigned servers field of the Satellite Agent Configuration dialog box.

 If the satellite will be manually assigned one or more machines to scan on the network, click Add to open the IP Filter Properties dialog box:



Fig. A-24 IP Filter Properties dialog box, Netmask

- 4. In the IP Filter Properties dialog box, go to **Filter type** and specify whether a subnet or IP address range will be used as criteria for determining which machines to scan:
  - To specify a subnet to scan, choose the default "Netmask" and make the following entries:
    - a. Enter the Network address.
    - b. Enter the Subnet mask.
    - c. Click **OK** to close the dialog box and to display your entries in the IP Address Filters list box of the Satellite Agent Configuration dialog box.
  - To specify an IP address range to scan, choose "Range" and make the following entries:

IP Filter Properties			
subnet mask, whi	le a Range filter spe	ers: a Netmask filter spec cifies lower and upper IP teria will be assigned to th	
Filter type:	○ Netmask ⓒ Range	Lowest IP address: Highest IP address:	100.10.101.20
	OK	Cancel	]

Fig. A-25 IP Filter Properties dialog box, Range

- a. Enter the Lowest IP address in the range.
- b. Enter the Highest IP address in the range.
- c. Click **OK** to close the dialog box and to display your entries in the IP Address Filters list box of the Satellite Agent Configuration dialog box.
- 5. In the Satellite Agent Configuration dialog box, click **OK** to close the dialog box.

#### Check the status of a satellite

To check a specific host's current workload—to determine whether or not the workload needs to be redistributed:

- 1. Select the Machine in the AD Agent servers list box.
- 2. Click Status to open the Status Detail window:

.ast status up	date: 2/1/200	7 1:00:03 PM					
Period end	Workstations	Avg. queue age	Memory used	CPU used	Verify count	Threads	Sources
13:00	26	0:38	38.2 Mb	10.1%	21	91	NetscanWorkStats,MonitorProcStats,NetscanP
12:50	26	0:34	38.2 Mb	10.6%	21	91	MonitorProcStats,NetscanWorkStats,CollectorF
12:40	26	0:43	38.2 Mb	9.6%	21	91	MonitorProcStats,CollectorProcStats,NetscanPr
12:30	26	4:20	38.2 Mb	10.1%	21	91	MonitorProcStats,NetscanWorkStats,NetscanP
12:20	26	0:41	38.2 Mb	10.4%	21	91	MonitorProcStats,CollectorProcStats,NetscanW
12:10	26	0:44	38.2 Mb	10.1%	21	91	CollectorProcStats,NetscanWorkStats,MonitorF
12:00	26	0:45	38.2 Mb	9.1%	21	91	MonitorProcStats,NetscanWorkStats,CollectorF
11:50	26	12:36	38.2 Mb	0.0%	6	91	MonitorProcStats,NetscanWorkStats,NetscanP
11:30	65	2:13	28.2 Mb	9.3%	54	75	MonitorProcStats,NetscanProcStats,NetscanW
11:20	65	2:10	28.2 Mb		54	75	MonitorProcStats,NetscanProcStats,NetscanW

Fig. A-26 Status Detail

The Machine name of the AD Agent host displays, along with the Role of the server ("Primary" or "Satellite"), and the Last status update (using the M/D/YYYY H:M:S AM/ PM format).

The following columns of information display for each record in the table:

- Period end the time period (using the HH:MM military time format) of each 10-minute interval in which servers/machines were scanned. The most recent 10-minute interval displays as the first record among the rows of records.
- Workstations the number of workstations included in the local session table for this host during the specified time period.
- Avg. queue age the average amount of time it took to probe a workstation (using the M:S time format) during the specified time period. If using the default fiveminute interval (specified in the Options page), any interval of time greater than the amount shown in this column may signify a problem in probing some workstations on the network.
- Memory used the amount of memory used by the host during the specified time period.
- CPU used the average percentage of CPU used by the host during the specified time period.
- Verify count the number of workstations verified by the probe scan for the specified time period. If this count is lower than the number of Workstations probed, the amount shown in this column may signify a problem in verifying some workstations on the network.
- Threads the number of units comprising the workload for the specified time period. An unusually high number of threads may indicate a problem with the workload for the host.
- Sources a list of the modules that reported during the specified time period in which data was obtained.
- 3. Click **Close** to close this window.

## Options page

On a primary host server:

1. Click **Options** to display the Options page:

🍋 Activ	e Directo	ory Agent (	Configuratio	n				
Domains	Service	Appliance	Agent hosts	Options	Notifications			
	When th to "catch	e agent start	ts up, it perforr current state of	ns a scan-	back of recent e	detect user logins. vent log history nit how far back in tir	ne this	
	Maximum	event log hi	istory scan-ba	sk: 72	hours.			
	and dete workstat	ct logoffs. on when bol	The agent au	tomatically I. WMI pro	selects the best obes are disable	on to verify the curren probe type for each d if the dcagent_serv		
		Enable	WMI workstat	ion probes	t.			
		🔽 Enable	NetWkstaUse	rEnum wo	rkstation probes			
		Minimum pro	obe interval:	5 mir	nutes.			
	known u	ser when a p	probe fails to fi	nd the wor		itomatically logs off t e this option if the I auto-logoffs:	ne last	
		Auto-log	goff unrespons	ive workst	tations			
	workstati	ons which ar				n these to discover domain controllers.	Jse	
	Other se	vers:	RAP-SERVF	1 RAP-SE	RVR2 PRINTS	/R1 PRINTSVR2		
							Ok	🗙 Cancel

Fig. A-27 Primary host Configuration, Options

- 2. Modify entries or make selections in this page as pertinent to your AD Agent setup:
  - Maximum event log history scan-back: By default, 72 hours displays as the number of hours of activity for scanning all domain controllers and including this information in the newly-built activity log. The entry in this field applies only to scenarios in which the AD Agent console opens for the first time, or when the AD Agent's state has been reset to purge all current data and new data is needed to rebuild the activity log (see Reset Team State option in the Service page).
  - "Enable WMI workstation probes": By default, this probe process is not selected to run.



**NOTE**: In order to use this probe, the dcagent\_service account must be a Domain Admins group member.

- "Enable NetWkstaUserEnum workstation probes": By default, this probe process is selected to run.
- **Minimum probe interval**: By default, *5* minutes displays as the interval of time in which the selected probe type(s) will probe workstations.
- "Auto-logoff unresponsive workstations": By default, this checkbox is checked, indicating that any workstation a probe fails to find will be automatically logged off in the activity log.
- **Other servers**: By default, this field is blank. If there are servers to be probed on the network, enter the host names of all servers, including a space between each name. Any server listed in this field will be assigned a host—unless a satellite host has already been assigned using the Satellite Agent Configuration dialog box, accessible via the Agent hosts page.

**NOTE**: Domain controllers should **not** be added to the Other servers list.

#### Notifications page

On a primary host server:

1. Click **Notifications** to display the Notifications page:

ee Activ	e Directo	ory Agent	Configuratio	n			>
Domains	Service	Appliance	Agent hosts	Options	Notifications		
		you des system configu	ignate. Notifica	ations are ; ecify the r	otifications to an administrato generated in response to ser ecipient and SMTP mail serv	ious	
			Recipient emai		jsmith23@logo.com	_	
			SMTP server:	addroot.	LOGO	_	
			Port:		25		
			Sender email a	ddress:	dcagent_service@logo.c	com	
			[	Send to	est message		
						ØDk	X Cancel

Fig. A-28 Primary host Configuration, Notifications

- 2. If using an SMTP server, enter the following criteria to specify the email address to be used in the event of a critical system error:
  - "Enable e-mail notifications" Click this checkbox to activate the fields in this page.
  - Recipient email address Enter the email address of the recipient of server error messages.
  - **SMTP server** Enter the IP address of the SMTP server.
  - **Port** By default, *25* displays as the port number used for sending email. This port number should be changed if the sending mail connection fails.
  - Sender email address Enter the email address of the server sending the email message.

3. Click Send test message to test the email setup connection. Make any necessary modifications to your entries if the sending mail connection fails.

**& NOTE**: The primary AD Agent sends an alert email message each day to the administrator's email address designated in this page. This email message includes all alert messages for that day.

# APPENDIX B: DISABLE SMB SIGNING REQUIREMENTS

SMB Signing is a Windows security feature that is not currently supported by the R3000. If you are running a Windows 2000 or Windows 2003 server and are using NTLM, then you need to make SMB Signing "not required."

# **SMB Signing Compatibility**

Server	R3000 Auth Mode	SMB Signing Enabled	SMB Signing Disabled	SMB Signing Not Defined
Win2000 mixed	NT Tier 1, 2, 3	Not compatible	Compatible	Compatible
Win2000 native	NT Tier 1, 2, 3	Not compatible	Not compatible	Not compatible
Win2003 mixed	NT Tier 1, 2, 3	Not compatible	Compatible	Not compatible
Win2003 native	NT Tier 1, 2, 3	Not compatible	Not compatible	Not compatible
Win2000 mixed	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible
Win2000 native	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible
Win2003 mixed	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible
Win2003 native	LDAP Tier 1, 2, 3	Compatible	Compatible	Compatible

To find out whether SMB Signing on your Windows server is compatible with the R3000, refer to the chart below:

# **Disable SMB Signing in Windows 2003**

By default, the SMB protocol in Windows 2003 is set to "Not Defined = On". To disable (turn "Off") SMB Signing, do the following:

 From your Windows 2003 workstation, go to Start > All Programs > Administrative Tools > Active Directory Users and Computers:



Fig. B-1 Go to Active Directory Users and Computers

2. When the Active Directory Users and Computers window opens, click Domain Controllers in the left panel to open the pop-up menu:

🐗 Active Directory l	Users and Comp	uters			_ 🗆 🗡
Ile Action Vie	w <u>W</u> indow <u>H</u> e	эlp			_ <b>8</b> ×
← → 1 1	% 💼 🛛 🗙 🖻	12 🗟 😫 🦉	1 🖉 💩 💎 🍕 🛅		
Active Directory Use	ers and Computer:	Domain Controllers	1 objects		
E Saved Queries		Name	Туре	Description	
QCAD. local     QCAD. local     QCAD. local     QCAD. local     QOmain Conductor     QDomain Conductor	Delegate Contro Find New All Tasks View New Window fro	> > >	Computer		
Opens property sheet I	Refresh Export List			1	
poporto property project	Properties			1	
	Help				

Fig. B-2 Select Properties in the Domain Controllers pop-up menu

3. Select Properties to open the Domain Controllers Properties dialog box:

Domain Controllers Properties	? ×
General Managed By COM+ Group Policy	
Current Group Policy Object Links for Domain Controller	\$
Group Policy Object Links No Override Dis	sabled
Default Domain Controllers Policy	
Group Policy Objects higher in the list have the highest priority.	
This list obtained from: tyudt.QCAD.local	
New Add Edit U	P
Delete Properties Do	wn
☐ <u>B</u> lock Policy inheritance	
OK Cancel	Apply

Fig. B-3 Domain Controllers Properties

4. Click the Group Policy tab, choose the Default Domain Controllers Policy, and then click **Edit** to open the Group Policy Object Editor window:

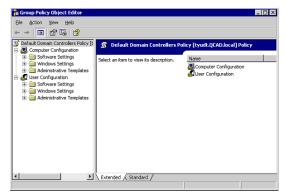


Fig. B-4 Group Policy Object Editor window

5. In the left panel, go to the Computer Configuration branch of the tree and select the Windows Settings folder to display the Windows Settings contents in the right panel:

Fin Group Policy Object Editor E/e Action Yew Help ← → € ⊡ ⊡ E3 C2		
Default Domain Controllers Policy [tyudt.QCAD.local] Policy         Image: Computer Configuration         Image: Default Domain Settings         Image: Default Domain Settings	Windows Settings Select an Rem to view Rs description.  Extended / Standard /	Name Scripts (Startup/Shutdown) Security Settings

Fig. B-5 Group Policy Object Editor window, Windows Settings

6. Choose Security Settings to display the contents of this folder in the right panel:

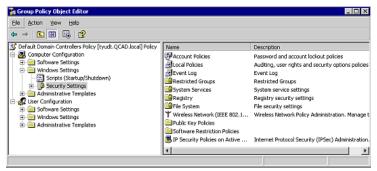


Fig. B-6 Group Policy Object Editor window, Security Settings

7. Select Local Policies to display the contents of this folder in the right panel:

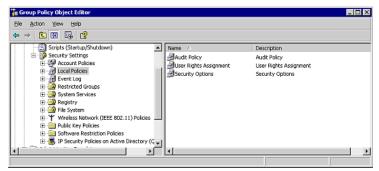


Fig. B-7 Group Policy Object Editor window, Local Policies

8. Select Security Options to display the contents of this folder in the right panel:

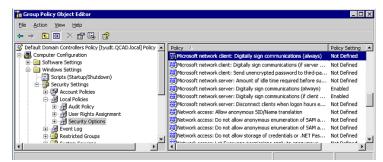


Fig. B-8 Group Policy Object Editor window, Security Options

Scroll down and find "Microsoft network client: Digitally sign communications (always)".

9. Right-click this item to open the pop-up menu, and select Properties to open the dialog box with the Security Policy Setting tab:



Fig. B-9 Define this policy setting

Click in the "Define this policy setting" checkbox to activate the radio buttons. Choose "Diabled", and then click **OK**.

- 10.Go back to the Group Policy Object Editor window (see Fig. B-8) and find the policies for the following items:
  - Microsoft network server: Digitally sign communications (always)
  - Domain controller: LDAP server signing requirements
  - Domain controller: LDAP client signing requirements

For each of these items, follow the instructions in step 9.

# APPENDIX C: OBTAIN, EXPORT AN SSL CERTIFICATE

When using Web-based authentication, the LDAP server's SSL certificate needs to be exported and saved to the hard drive, then uploaded to the R3000 so that the R3000 will recognize LDAP server as a trusted source.

This appendix provides steps on exporting an SSL certificate from a Microsoft Active Directory or Novell server—the most common types of LDAP servers. Also included is information on obtaining a Sun ONE server's SSL certificate.

# Export an Active Directory SSL Certificate

## Verify certificate authority has been installed

 From the console of the LDAP server, go to Start > Programs > Administrative Tools > Certification Authority to open the Certification Authority window:

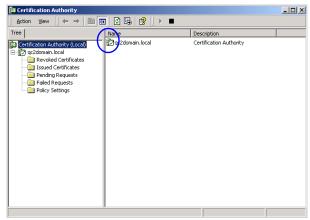


Fig. C-1 Certfication Authority window

2. Verify that the certificate authority has been installed on this server and is up and running—indicated by a green check mark on the server icon (see circled item in Fig. C-1).

## Locate Certificates folder

 Go to Start > Run to open the Run dialog box. In the Open field, type in mmc.exe to specify that you wish to access the Microsoft Management Console:

Run	? ×
5	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmc.exe
	OK Cancel Browse

Fig. C-2 Run dialog box

2. Click **OK** to open the Console window:

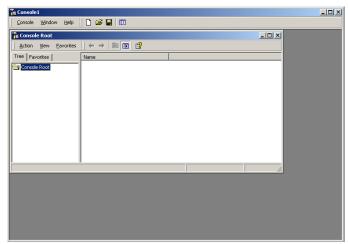


Fig. C-3 Microsoft Console window

3. From the toolbar, click Console to open the pop-up menu. Select Add/Remove Snap-in to open the Add/ Remove Snap-in dialog box:

Add/Remove Snap-in	? ×
Standalone Extensions	
Use this page to add or remove a standalone Snap-in from the console.	
Snap-ins added to: Console Root	
Description	-1
Add Remove About	
OK C4	ancel

Fig. C-4 Add/Remove Snap-in

4. Click **Add** to open the Add Standalone Snap-in dialog box:

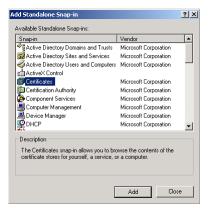


Fig. C-5 Add Standalone Snap-in

5. Select Certificates, and click **Add** to open the Certificates snap-in wizard dialog box:

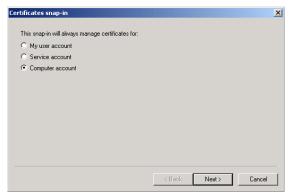


Fig. C-6 Certificates snap-in dialog box

6. Choose "Computer account", and click **Next** to go to the Select Computer wizard page:

Select Computer	x
Select the computer you want this Snap-in to manage.	
This snap-in will always manage:	
Cocal computer: (the computer this console is running on)	
C Another computer: Browse	
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

Fig. C-7 Select Computer dialog box

- 7. Choose "Local computer: (the computer this console is running on)", and click **Finish** to close the wizard dialog box.
- Click Close to close the Add Standalone Snap-in dialog box. Click OK to close the Add/Remove Snap-in dialog box.

Notice that the snap-in has now been added to the Console Root folder:

🖆 Console Window Help			] 🗋 🚅 🖬 🔟 💷	9)×
Action Yew Envorites	) 📧 🗈 🕼 😭			
ree Favorites	Issued To /	Issued By	Expiration Date	1
	⊡ 2000eserver ac3dman.iocal ⊇ qc2doman.iocal	gc2doman.local gc2doman.local	6,77,2006 6,77,2024	
( ) )	4			

Fig. C-8 Console Root with snap-in

## Export the master certificate for the domain

- 1. Go to the right panel of the Console and select the master certificate for the domain that you just added.
- 2. Right-click the certificate to open the pop-up menu, and select All Tasks > Export:

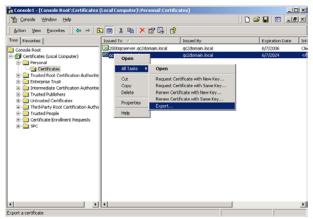


Fig. C-9 Select the certificate to be exported

This action launches the Certificate Export Wizard:



Fig. C-10 Certificate Export Wizard

3. Click **Next** to go to the Export Private Key page of the wizard:



Fig. C-11 Export Private Key

4. Select "No, do not export the private key", and click **Next** to go to the Export File Format page of the wizard:

Select	the format you want to use:
C	DER encoded binary X.509 (.CER)
e	Base-64 encoded X.509 (.CER)
C	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	$\hfill \square$ Include all certificates in the certification path if possible
С	Personal Information Exchange - PKC5 #12 (.PFX)
	$\square$ Include all certificates in the certification path if possible
	Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
	Delete the private key if the export is successful

Fig. C-12 Export File Format

5. Select "Base-64 encoded X.509 (.CER)" and click **Next** to go to the File to Export page of the wizard:

ificate Export Wizard ile to Export	
Specify the name of the file you	u want to export
File name:	
E:\domain.cer	Browse
,	
	and the second
	< Back Next > Cano

Fig. C-13 File to Export

 Enter the File name of the file to be exported, followed by the .cer extension. Click Next to go to the final page of the wizard:

Certificate Export Wizard		X
	Completing the Certificate Export Wizard You have successfully completed the Certificate Export witard. You have specified the following settings:	t
	File Name E:\dom No Export Keys No Include al certificates in the certification path No File Format Base64	
	< Back Finish Can	el

Fig. C-14 Settings

- 7. Notice that the specified settings display in the list box, indicating the certificate has been successfully copied from the console to your disk. Click **Finish** to close the wizard dialog box.
- 8. Close the Console.

The certificate can now be uploaded to the R3000.

# **Export a Novell SSL Certficate**

1. From the console of the LDAP server, go to the tree in the left panel and open the Security folder to display the contents in the Console View (right panel):

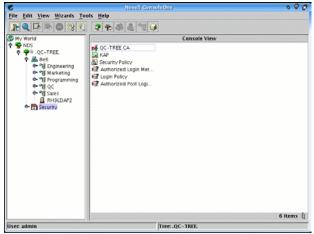


Fig. C-15 Novell Console window

2. Find the tree's folder and right-click it to open the pop-up menu. Select Properties to open the Properties dialog box:

6		Properties of QCTITEE CA
General Certificate Self Signed	es . d Certificate	NDS Rights - Other Rights to Files and Folders
Subject name:	Provide a strand strand	nizational CA.0=QC-TREE
Issuer name:	Concernance of the second	nizational CA.0=QC-TREE
Effective date:	Providence of the second secon	004 9.31.31 AM PDT
Expiration date:	July 12, 20	014 9:31:31 AM PDT
		Details Export Replace
Page Options		OK Cancel Apply Help

Fig. C-16 Properties dialog box

- 3. Click the Certificates tab to go to the Self Signed Certificate page.
- 4. Click **Export** to open the Export A Certificate pop-up window:

8	Export A Certificate	
Output format	ormat for the certificate. TY DER format 264 format	
Filename:	/root/SelfSignedCert.der	ii.

Fig. C-17 Export A Certificate pop-up window

- 5. Select "File in binary DER format" for the Output format. The path of the certificate displays in the Filename field.
- 6. Click **Export** to open another pop-up window that asks where you would like to save the certificate—the most convenient place would be your desktop.

The certificate can now be uploaded to the R3000.

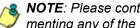
# **Obtain a Sun ONE SSL Certificate**

Unlike Microsoft or Novell, the Sun ONE LDAP directory does not have a tool for exporting an SSL certificate once it has been imported to the LDAP server.

Therefore, a copy of the root certificate—in the .cer or .der format—that was used to sign the LDAP server's certificate must be uploaded to the R3000. This certificate can be an internally generated root certificate (if you have a certificate authority to generate the certificate), or can be the root certificate used by the external signing authority.

# **APPENDIX D: LDAP SERVER CUSTOMIZATIONS**

The R3000 has been tested on common types of standard LDAP servers with default settings. However, due to the number of LDAP servers available, and the limitless ways in which any type of LDAP server can be configured, customizations may need to be made on such an LDAP server that fits either description.



**NOTE**: Please contact technical support for assistance in implementing any of the changes described in this appendix.

# **OpenLDAP Server Scenario**

## Not all users returned in User/Group Browser

In this scenario, a query is performed in the LDAP User/ Group Browser window on an OpenLDAP server, and not all users are returned.

To resolve this problem, do the following:

- 1. Change the current directory to /usr/local/shadow/etc/ Idapgroup
- Find the subdirectory bearing the name of the LDAP domain, and change the current directory to that subdirectory.
- 3. Open the file "Idapobjectdef.conf" for editing.
- 4. Search for the line "LDC LDAP query name prefix CN="
- 5. Replace "CN=" with "uid=" and save these changes.
- 6. Restart the R3000.

# APPENDIX E: USER/GROUP FILE FORMAT AND RULES

The file with user/group profiles you upload to the server must be set up in a specified format, with one complete user/group profile per line. The format for the file will differ depending on whether the file contains a list of user or group profiles for an NT or LDAP server.

Each filtering profile in the file must contain the following items:

- 1. The username or group name.
- 2. Filtering profile criteria:
  - Rule number (Rule0, Rule1, etc.), or
  - rule criteria:
    - a. Ports to Block or Filter
    - b. Categories to Block or Open
    - c. Filter Mode
- 3. Redirect URL (optional).
- 4. Filter Options (optional). A zero should be placed at the end of a profile string with all filter options disabled.

## **Username Formats**

NOTE: For examples of valid username entries, see File Format: Rules and Examples in this appendix, or go to http:// www.8e6.com/r3000help/files/2group\_textfile\_user.html

# **Rule Criteria**

Rule criteria consists of selections made from the following lists of codes that are used in profile strings:

### Port command codes:

- A = Filter all ports
- B = Filter the defined port number(s)
- I = Open all ports
- J = Open the defined port number(s)

J J = Open port(s) defined after the first "J", and always allow port(s) defined after the second "J"

- Q = Block all ports
- R = Block the defined port number(s)

### Port Numbers:

- 21 = FTP (File Transfer Protocol)
- 80 = HTTP (Hyper Text Transfer Protocol)
- 119 = NNTP (Network News Transfer Protocol)
- 443 = HTTPS (Secured HTTP Transmission)

Other

### • Filter Mode Values:

- 1 = Default, Block Mode
- 2 = Monitoring Mode
- 4 = Bypassing Mode

### Category command codes:

- I = One of two codes that must be positioned at the end of a profile string (the other code being "Q"). When positioned after "blocked" categories at the end of the profile string, this code indicates that all other categories should be "open."
- J = Positioned before the category/categories defined as "open."

- J J = First "J" positioned before the category/categories defined as "opened," second "J" positioned before the category/categories defined as "white listed."
- Q = One of two codes that must be positioned at the end of a profile string (the other code being "I"). When positioned at the end of the profile string, this code indicates that all other categories should be "blocked."
- M = Positioned before the category/categories defined as containing URLs potentially against the organization's policies, and accompanied by a warning message.
- R = Positioned before the category/categories defined as "blocked."
- Category Codes:

For the list of category codes (short names) and their corresponding descriptions (long names), go to http://www.8e6.com/r3000help/files/ 2group\_textfile\_cat.html#cat

**NOTE**: The list of library category codes and corresponding descriptions is subject to change due to the addition of new categories and modification of current categories. For explanations and examples of category items, go to http://www.8e6.com/database-categories.html

- Filter Option codes:
  - 0x2 = X Strikes Blocking
  - 0x4 = Google/Yahoo! Safe Search
  - 0x100 = Search Engine Keyword
  - 0x200 = URL Keyword
  - 0x400 = Bypass Minimum Filtering Level for Override Account
  - 0x1000= Extend URL Keyword Filter Control



 NOTES: To enable multiple filter codes, add the codes together.
 For example, to enable all features for an IP profile, add 1 + 2 + 4 + 100 + 200 + 400 + 1000 = 1707, which means that 0x1707 should be entered at the end of the profile string.

To disable all filter codes for an IP profile, enter **0x1** at the end of the profile string.

See http://www.8e6.com/r3000help/files/ 2group\_textfile\_format\_nt.html for examples of NT filtering profile entries, and http://www.8e6.com/r3000help/files/ 2group\_textfile\_format\_ldap.html for examples of LDAP filtering profile entries.

# File Format: Rules and Examples

When setting up the file to upload to the server, the following items must be considered:

- Each profile must be entered on a separate line in the file.
- Category Codes must be entered in capital letters.
- Port and category command codes must be entered in capital letters.
- A redirect URL cannot exceed 200 characters in length.
- The string must end with a "0" (zero) if no filter options will be enabled.

# NT User List Format and Rules

When setting up the "ntuserprofile.conf" file, each entry must consist of the username, and either a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Segments of the profile string should be separated by commas (,). A zero (0) should be placed at the end of a profile string without any filter options enabled.

#### JSmith, B 80 R 21 ,J J FINAN Q, 1, http:// www.8e6.com,0 John\_Doe, Q, R AUTO GENTER I, 1, ,0x104 Doe-Jane, Rule1, , 0x202

When translated, these strings of code mean:

- NT profile for a user with ID "JSmith": Filter port 80, Block port 21, White List and Open Financial Category and Block all other categories, use filter mode 1, use redirect URL http://www.8e6.com in place of the standard block page, all filter options disabled.
- NT profile for a user with ID "John\_Doe": Block all ports, Block Automobile and Entertainment categories, use filter mode 1, Google/Yahoo! Safe Search and Search Engine Keyword filter options enabled.
- NT profile for a user with ID "Doe-Jane": Bypass all categories, use standard block page, X Strikes Blocking and URL Keyword filter options enabled.

# NT Group List Format and Rules

When setting up the "ntgroupprofile.conf" file, each entry must consist of the group name, and either a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Segments of the profile string should be separated by commas (,). A zero (0) should be placed at the end of a profile string without any filter options enabled.

#### Admin, Rule1, http://www.cnn.com, ,0x4 Sales, Rule2, ,0x300 Tech, A, R CHAT KDPORN FINAN GGAMES GPORN I, 1, , 0x6

When translated, these strings of code mean:

- NT profile for a group with ID "Admin": Bypass all categories, use redirect URL http://www.cnn.com in place of the standard block page, Google/Yahoo! Safe Search filter option enabled.
- NT profile for a group with ID "Sales": Block Porn category, use standard block page, Search Engine Keyword and URL Keyword filter options enabled.
- NT profile for a group with ID "Tech": Filter all ports, Block Chat, Child Porn, Finance, and Games categories, but leave all other categories open, use filter mode 1, use standard block page, X Strikes Blocking and Google/ Yahoo! Safe Search filter options enabled.

# LDAP User List Format and Rules

When setting up the "Idapuserprofile.conf" file, each entry must consist of the Distinguished Name (DN), with each part of the DN separated by commas (,). The DN should be followed by a semicolon (;), and then a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Each segment of the profile string following the semicolon for the DN should be separated by commas (,). A zero (0) should be placed at the end of a profile string without any filter options enabled. For example:

#### CN=Jane Doe, CN=Users, DC=qc, DC=local; R 21 A, J J FINAN Q, 1, http://www.cnn.com, 0x2 CN=Public\, Joe Q., OU=Users, OU=Sales, DC=qc, DC=local; Q, R AUTO GENTER I, 1, ,0x4

**NOTE**: The DN format must contain the username and user group "CN" ("common name") attribute type, and the domain and DNS suffix "DC" ("domain component") attribute type. The "OU" ("organizational unit") attribute type also can be included. Each attribute type should be followed by an equals sign (=), and separated by a comma (,).

When translated, these strings of code mean:

• LDAP profile for a user with username "Jane Doe", user group "Users", domain "qc", DNS suffix ".local": Block port 21 and Filter all other ports, White List and Open Financial Category and Block all other categories, use filter mode 1, use redirect URL http://www.cnn.com in place of the standard block page, X Strikes Blocking filter option enabled.  LDAP profile for a user with username "Public\, Joe Q.", organizational units "Users" and "Sales", domain "qc", DNS suffix ".local": Block all ports, Block Automobile and Entertainment categories, use filter mode 1, use standard block page, Google/Yahoo! Safe Search filter option enabled.

# LDAP Group List Format and Rules

When setting up the "Idapgroupprofile.conf" file, each entry must consist of the Distinguished Name (DN), with each part of the DN separated by commas (,). The DN should be followed by a semicolon (;), and then a rule number or rule criteria (port, category, and filter mode specifications). A redirect URL can be included, if a specific URL should be used in place of the standard block page. If a redirect URL is not included, a blank space should be entered in its place in the profile string. Each segment of the profile string following the semicolon for the DN should be separated by commas (,). A zero (0) should be placed at the end of a profile string without any filter options enabled. For example:

#### CN=Sales, CN=Users, DC=qc, DC=local; Rule1, 1, http://www.cnn.com, 0x102

**NOTE**: The DN format must contain the group name—and, if applicable—user group "CN" ("common name") attribute type, and the domain and DNS suffix "DC" ("domain component") attribute type. The "OU" ("organizational unit") attribute type also can be included. Each attribute type should be followed by an equals sign (=), and separated by a comma (,).

When translated, this string of code means:

• LDAP profile for group with ID "Sales", user group "Users", domain "qc", DNS suffix ".local": Bypass all categories, use filter mode 1, use redirect URL http://www.cnn.com in place of the standard block page, X Strikes Blocking and Search Engine Keyword filter options enabled.

# APPENDIX F: OVERRIDE POP-UP BLOCKERS

An override account user with pop-up blocking software installed on his/her workstation will need to temporarily disable pop-up blocking in order to authenticate him/herself via the Options page:

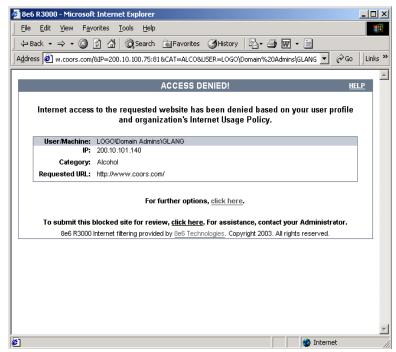


Fig. F-1 Options page

This appendix provides instructions on how to use an override account if typical pop-up blocking software is installed, as in the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, Mozilla Firefox, and Windows XP Service Pack 2 (SP2).

# Yahoo! Toolbar Pop-up Blocker

# If pop-up blocking is enabled

- 1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
- 2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

# Add override account to the white list

If the override account window was previously blocked by the Yahoo! Toolbar, it can moved from the black list and added to the white list so that it will always be allowed to pass. To do this:

1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:



Fig. F-2 Select menu option Always Allow Pop-Ups From

2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:

Yahoo! Pop-Up Blocker	×			
Sources of Recently Blocked Pop-Ups:				
edit.companion.yahoo.com	Allow			
Always Allow Pop-Ups From These Sources:				
8e6.com	Remove			
Help	Close			

Fig. F-3 Allow pop-ups from source

- 3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.
- 4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.
- 5. Click **Close** to save your changes and to close the dialog box.

# Google Toolbar Pop-up Blocker

# If pop-up blocking is enabled

- 1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
- 2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

# Add override account to the white list

To add the override account window to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the # blocked icon:



Fig. F-4 # blocked icon enabled

Clicking this icon toggles to the Site pop-ups allowed icon, adding the override account window to your white list:

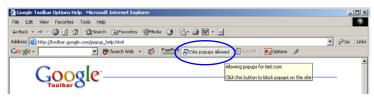


Fig. F-5 Site pop-ups allowed icon enabled

# AdwareSafe Pop-up Blocker

# If pop-up blocking is enabled

- 1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
- 2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

# Temporarily disable pop-up blocking

AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the popup icon.

- 1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.
- 2. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
- 3. Click the **Override** button to open the override account pop-up window.
- 4. Go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # popups blocked. This action turns on pop-up blocking again.

# Mozilla Firefox Pop-up Blocker

# Add override account to the white list

- 1. From the browser, open the Preferences dialog box.
- 2. Go to the Category list box and select Privacy & Security> Popup Windows to display the Popup Windows page:

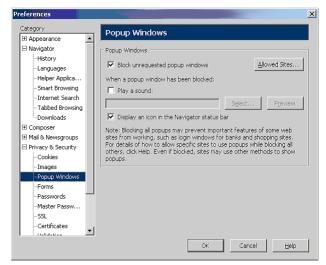


Fig. F-6 Mozilla Firefox Popup Windows Preferences

- 3. With the "Block unrequested popup windows" checkbox checked, click **Allowed Sites** and enter the URL to allow the override account window to pass.
- 4. Click **OK** to save your changes and to close the dialog box.

# Windows XP SP2 Pop-up Blocker

# Set up pop-up blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

## Use the Internet Options dialog box

- 1. From the IE browser, go to the toolbar and select Tools > Internet Options to open the Internet Options dialog box.
- 2. Click the Privacy tab:

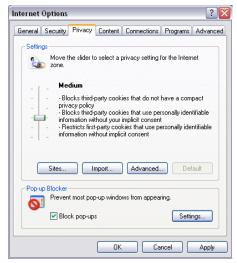


Fig. F-7 Enable pop-up blocking

- 3. In the Pop-up Blocker frame, check "Block pop-ups".
- 4. Click Apply and then click OK to close the dialog box.

# Use the IE toolbar

In the IE browser, go to the toolbar and select Tools > Popup Blocker > Turn On Pop-up Blocker:

Microsoft Office Online: Installation Troubleshooter - Microsoft Internet Explorer				
File Edit View Favorites	Tools Help			
Geber Sack -	Mail and News			
Address 🕘 http://office.microso	Synchronize Windows Update ) 🕘 866 Channel Partners Newsletter e 🌒 TurboPipe 💩 866 Website User Manageme			
	Windows Messenger Microsoft.com Home   Site Map ICQ Uite Sun Java Console			
	Internet Options earch: Downloads 🔽 😡			

Fig. F-8 Toolbar setup

When you click Turn On Pop-up Blocker, this menu selection changes to Turn Off Pop-up Blocker and activates the Pop-up Blocker Settings menu item.

You can toggle between the On and Off settings to enable or disable pop-up blocking.

# Temporarily disable pop-up blocking

- 1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
- 2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

# Add override account to the white list

There are two ways to disable pop-up blocking for the override account and to add the override account to your white list.

## Use the IE toolbar

 With pop-up blocking enabled, go to the toolbar and select Tools > Pop-up Blocker > Pop-up Blocker Settings to open the Pop-up Blocker Settings dialog box:



Fig. F-9 Pop-up Blocker Settings

- 2. Enter the Address of Web site to allow, and click Add to include this address in the Allowed sites list box. Click **Close** to close the dialog box. The override account window has now been added to your white list.
- 3. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
- 4. Click the **Override** button to open the override account pop-up window.

## Use the Information Bar

With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked popups or allowing pop-ups from a specified site.

## Set up the Information Bar

- Go to the toolbar and select Tools > Pop-up Blocker > Pop-up Blocker Settings to open the Pop-up Blocker Settings dialog box (see Fig. F-9).
- 2. In the Notifications and Filter Level frame, click the checkbox for "Show Information Bar when a pop-up is blocked."
- 3. Click **Close** to close the dialog box.

## Access your override account

- 1. In the Options page (see Fig. F-1), enter your **Username** and **Password**.
- 2. Click the **Override** button. This action displays the following message in the Information Bar: "Pop-up blocked. To see this pop-up or additional options click here...":



Fig. F-10 Information Bar showing blocked pop-up status

3. Click the Information Bar for settings options:

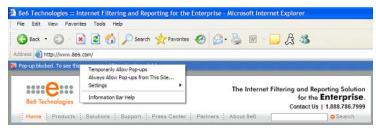


Fig. F-11 Information Bar menu options

4. Select Always Allow Pop-ups from This Site—this action opens the Allow pop-ups from this site? dialog box:

Allow po	op-ups from this site?	X
<b></b>	Would you like to allow pop-upe from \www.8e6.com?	
	Yes No	

Fig. F-12 Allow pop-ups dialog box

5. Click **Yes** to add the override account to your white list and to close the dialog box.

NOTE: To view your white list, go to the Pop-up Blocker Settings dialog box (see Fig. F-9) and see the entries in the Allowed sites list box.

6. Go back to the Options page and click **Override** to open the override account window.

# **APPENDIX G: GLOSSARY**

# Definitions

This glossary includes definitions for terminology used in this user guide.

**ADS** - Active Directory Services is a Windows 2000 directory service that acts as the central authority for network security, by letting the operating system validate a user's identity and control his or her access to network resources.

**attribute** - A component of a group base or Distinguished Name (DN) that has a type and value. Attribute types include "cn" for common name, "dc" for domain component, and "ou" for organizational unit.

**authentication method** - A way to validate users on a network. Methods include SMB/NT (referred to as "NT" throughout this user guide) and LDAP.

**authentication server** - The domain controller on a domain. This server is used for authenticating users on the network.

**block setting** - A setting assigned to a service port or library category when creating a rule, or when setting up a filtering profile or the minimum filtering level. If an item is given a block setting, users will be denied access to it.

**common name (cn)** - An attribute type entered for a username and group when using LDAP.

**container** - An LDAP server object that can be comprised of containers, organizational units, or domains. Container objects can also "contain" other objects, such as user objects, group objects, and computer objects.

**directory** - This information source on a server contains attribute-based data relevant to a DN entry.

**directory service** - Uses a directory on a server to automate administrative tasks for storing and managing objects on a network (such as users, passwords, and network resources users can access). ADS, DNS, and NDS (Novell Directory Services) are types of directory services.

**Distinguished Name (DN)** - A string of "cn" and "dc" attribute types comprised of the username and group name, domain name, and DNS suffix. For example: "cn=admin\_user, cn=admin, dc=yahoo, dc=com". The "ou" attribute type also could be a part of the DN. For example: "cn=Joe Smith, ou=users, ou=sales, dc=acme, dc=com".

**DNS** - Domain Name Service is a distributed Internet directory service. DNS is used mostly for making translations between domain names and IP addresses.

**domain** - An entity on a network comprised of servers, workstations, and peripherals.

**domain component (dc)** - An attribute type entered for a domain name and DNS suffix when using LDAP.

**domain controller** - An authentication server that answers logon requests from workstations in a Windows NT domain. There are two types of domain controller servers: Primary Domain Controller (PDC) and Backup Domain Controller (BDC).

**dynamic group** - a virtual LDAP group that does not contain names of its members but is derived automatically by matching certain user data criteria. (See also "static group".)

**entry** - A collection of attribute types that comprise a Distinguished Name (DN). Each attribute type of the Distinguished Name has a type and one or more values. These types are mnemonic strings, such as "cn" for common name, "dc" for domain component, or "ou" for organizational unit. **filter setting** - A setting made for a service port. A service port with a filter setting uses filter settings created for library categories (block, open, or always allow settings) to determine whether users should be denied or allowed access to that port.

**firewall mode** - An R3000 set up in the firewall mode will filter all requests. If the request is appropriate, the original packet will pass unchanged. If the request is inappropriate, the original packet will be blocked from being routed through.

**global administrator** - An authorized administrator of the network who maintains all aspects of the R3000, except for managing master IP groups and their members, and their associated filtering profiles. The global administrator configures the R3000, sets up master IP groups, and performs routine maintenance on the server.

**group administrator** - An authorized administrator of the network who maintains a master IP group, setting up and managing members within that group. This administrator also adds and maintains customized library categories for the group.

**group name** - The name of a group set up for a domain on an NT server. For example: "production" or "sales".

**invisible mode** - An R3000 set up in the invisible mode will filter all connections on the Ethernet between client PCs and the Internet, without stopping each IP packet on the same Ethernet segment. The unit will only intercept a session if an inappropriate request was submitted by a client.

**LDAP** - One of two authentication method protocols used by the R3000. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names).

**LDAP host** - The LDAP domain name and DNS suffix. For example: "yahoo.com" or "server.local".

**login (or logon) script** - Consists of syntax that is used for re-authenticating a user if the network connection between the user's machine and the server is lost.

**machine name** - Pertains to the name of the user's workstation machine (computer).

**minimum filtering level** - A set of library categories and service ports defined at the global level to be blocked or opened. If the minimum filtering level is established, it is applied in conjunction with a user's filtering profile. If a user does not belong to a group, or the user's group does not have a filtering profile, the default (global) filtering profile is used, and the minimum filtering level does not apply to that user.

**name resolution** - A process that occurs when the R3000 attempts to resolve the IP address of the authentication server with the machine name of that server. This continuous and regulated automated procedure ensures the connection between the two servers is maintained.

**net use** - A command that is used for connecting a computer to—or disconnecting a computer from—a shared resource, or displaying information about computer connections. The command also controls persistent net connections.

**NetBIOS** - Network Basic Input Output System is an application programming interface (API) that augments the DOS BIOS by adding special functions to local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. NetBIOS relies on a message format called Server Message Block (SMB).

**NetBIOS name lookup** - An authentication method used for validating a client (machine) by its machine name.

**Network Address Translation (NAT)** - Allows a single real IP address to be used by multiple PCs or servers. This is

accomplished via a creative translation of inside "fake" IP addresses into outside real IP addresses.

**open setting** - A setting assigned to a service port or library category when creating a rule, or when setting up a filtering profile or the minimum filtering level. If an item is given an open (pass) setting, users will have access to it.

**organizational unit (ou)** - An attribute type that can be entered in the LDAP Distinguished Name for a user group.

**override account** - An account created by the global group administrator or the group administrator to give an authorized user the ability to access Internet content blocked at the global level or the group level.

**PDC** - A Primary Domain Controller functions as the authentication server on a Windows NT domain. This server maintains the master copy of the directory database used for validating users.

**profile string** - The string of characters that define a filtering profile. A profile string can consist of the following components: category codes, service port numbers, and redirect URL.

**protocol** - A type of format for transmitting data between two devices. LDAP and SMB are types of authentication method protocols.

**proxy server** - An appliance or software that accesses the Internet for the user's client PC. When a client PC submits a request for a Web page, the proxy server accesses the page from the Internet and sends it to the client. A proxy server may be used for security reasons or in conjunciton with caching for bandwidth and performance reasons.

**router mode** - An R3000 set up in the router mode will act as an Ethernet router, filtering IP packets as they pass from one card to another. While all original packets from client PCs are allowed to pass, if the R3000 determines that a request is inappropriate, a block page is returned to the client to replace the actual requested Web page or service.

**rule** - A filtering component comprised of library categories set up to be blocked or opened. Each rule created by the global administrator is assigned a number and a name that should be indicative of its theme. Rules are used when creating filtering profiles for entities on the network.

**search engine** - A program that searches Web pages for specified keywords and returns a list of the pages or services where the keywords were found.

**service port** - Service ports can be set up to blocked. Examples of these ports include File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Network News Transfer Protocol (NNTP), Secured HTTP Transmission (HTTPS), and Other ports such as Secure Shell (SSH).

**SMB** - One of two authentication method protocols used by the R3000. Server Message Block is a "client/server, request/response" protocol.

**static group** - an LDAP group that contains names of its members. (See also "dynamic group".)

**sub-group** - An entity of a master IP group with an associated member IP address, and filtering profile.

**time-based profile** - A user profile used by both the NT and LDAP authentication methods to give a user a time limit on his/her Internet connection.

**time profile** - A customized filtering profile set up to be effective at a specified time period for designated users.

**tiers** - Levels of authentication methods. Tier 1 uses net use based authentication for NT or LDAP. Tier 2 uses timebased profiles for both the NT and LDAP authentication methods. Tier 3 uses persistent login connections for either the NT or LDAP authentication methods. **URL** - An abbreviation for Uniform Resource Locator, the global address of Web pages and other resources on the Internet. A URL is comprised of two parts. The first part of the address specifies which protocol to use (such as "http"). The second part specifies the IP address or the domain name where the resource is located (such as "203.15.47.23" or "8e6.com").

virtual IP address - The IP address used for communicating with all users who log on the network.

**warn setting** - A setting assigned to a library category when creating a rule, or when setting up a filtering profile. This designation indicates URLs in the library category may potentially be in opposition to the organization's policies, and are flagged with a warning message that displays for the end user if a URL from that library category is requested.

**Web-based** - An authentication method that uses timebased profiles or persistent login connections.

**white list** - A list of approved library categories for a specified entity's filtering profile.

# INDEX

## **Numerics**

3-try login script *188* 8e6 Authenticator *24*, *210* 8e6 supplied category *17* 

## Α

Account tab 113 Active Directory Agent 24, 221 active filtering profiles 14 Address tab 110 ADS. definition 295 alert box, terminology 3 Alias List tab 118 Alias Name 119 always allowed 19 Anonymous Bind 113, 124 attribute. definition 295 authentication activate NT 188 activate on network 159 activate Web-based for Global Group 172 activated Web-based for IP group 160 configuration procedures 28 methods 198 net use based module diagram 196 net use based process 196 servlet 42 setup procedures 194 specifications and requirements 198 test net use settings 158 test settings 147 test Web-based settings 149 Authentication Form Customization 69 authentication method. definition 295 Authentication Request Form 63, 147, 156 figure 147, 157

authentication server 11 definition 295 function in net use based process 196 login scripts 201 Authentication Settings window 45 join the domain 77 authentication solution single user compatibility chart 25 system deployment options on a network 26 Authentication SSL Certificate window 47 authmodule.log 55

## В

Backup Domain Controller (BDC) 296 backup server configuration 121 Backup Server Configuration wizard 122 Block page 59 block page 13, 14, 15 Block Page Authentication 58 Block Page Customization 73 block setting 19 definition 295 button, terminology 3

## С

category custom categories 17 library 17 category codes 276 Category Profile LDAP domain 142 NT domain 97 Category tab LDAP domain 142 NT domain 97 checkbox, terminology 3 Common Customization 66 common name (cn), definition 295 container 11, 21 container, definition 295 Create CSR 51 Create Domain Controller 79 Create LDAP Domain dialog box 102 custom categories 17

## D

Default Rule tab 120 dialog box, terminology 3 directory service, definition 296 directory, definition 295 Distinguished Name (DN) definition 296 LDAP protocol 199 DNS, definition 296 domain definition 296 delete profile 128 domain component (dc), definition 296 domain controller, definition 296 Domain Name Service (DNS) 296 dynamic group 11 dynamic group, definition 296

### Ε

edirAgent.log 55 eDirectory 212, 218 edirEvent.log 55 Enable/Disable Authentication window 39 entry, definition 296 environment requirements 32 eth0, eth1 35

#### F

field, terminology 3 file formats 278 filter option codes 276 filter options 100, 145 filter setting 19 definition 297 filtering 276 LDAP container 15 profile components 16 profile types 12 rules 20 static profiles 13 user, machine 15 firewall mode 35, 37 definition 297 frame, terminology 4 FTP 33

## G

gateway IP address 37 global administrator, definition 297 global filtering profile 14 global group 8 grid, terminology 4 group global 8 IP 9 LDAP 11 NT 10 types of 8 group administrator, definition 297 group name, definition 297 group objects 107 Group tab 106 Group/Member Details window LDAP domain 139 NT domain 94

### Η

HTTPS 33

## I

IANA 199 individual IP member profile type 14 Internet Explorer 32 invisible mode 35, 37 definition 297 IP group 9 diagram 9 IPC share 196

#### J

Java applet 43 Java Plug-in 32 Java Runtime Environment 32, 43 Java Virtual Machine 32 JavaScript 32 join the domain 78

### L

LAN Settings window 37 LAN1, LAN2 38, 46 LDAP Active Directory Service usage 203 authentication protocol 23 definition 297 domain diagram 11 domain groups 11 name resolution method 200 profile file format 137 protocol 199 server customizations 273 server setup 203 LDAP domain add 102 add groups, users 129 LDAP domain window 104 LDAP host. definition 297 LDAP Query Base 112, 123

LDAP Server Type 105 LDAP User/Group Browser window 130 library categories 17 category codes list 276 list box, terminology 4 lock profile 13 profile type 15 log view files 55 login (or logon) script definition 298 examples 201 usage 196

#### Μ

machine name, definition 298 Manually Add Group dialog box LDAP 135 NT domain 90 Manually Add Member dialog box LDAP 134 NT domain 89 master IP group 9 filtering profile 13 methods authentication 198 name resolution 200 Microsoft Active Directory Mixed Mode 105, 194 Native Mode 105, 194 minimum filtering level 18 definition 298

## Ν

name resolution definition 298 methods 200 WINS Server 200 NAT

definition 298 navigation panel terminology 4 net use command 188 definition 298 syntax 201 **NetBIOS** definition 298 name lookup, definition 298 NetBIOS Domain Name 111, 123 NetBIOS name 45 Netscape Directory Server 105 Network Address Translation (NAT), definition 298 network requirements 33 NIC device 46 Novell 23, 105, 117, 195, 199, 212, 216, 262 Novell eDirectory Agent 24, 218 NT domain diagram 10 domain groups 10 profile file format 92 NT domain add 79 Default Rule 83 Domain Settings 81 NTLM authentication protocol 23, 77

## 0

open setting 19 definition 299 OpenLDAP 23, 130 server customizations 273 Operation Mode window 35 Options page 62 organizational unit (ou), definition 299 override account AdwareSafe popup blocking 288 block page authentication 58 definition 299 Google Toolbar popup blocking 287 Mozilla Firefox popup blocking 289 override popup blockers 284 profile type 15 Windows XP SP2 popup blocking 290 Yahoo! Toolbar popup blocking 285

### Ρ

**PDC 78** definition 299 pop-up blocking, disable 284 pop-up box/window, terminology 5 primary IP address 38 Primary Domain Controller (PDC) 296 profile string definition 299 elements 275 Profile window 96 LDAP domain 141 protocol definition 299 LDAP 199 SMB 198 proxy server definition 299 pull-down menu, terminology 5

## R

radio button, terminology 5 re-authentication block page authentication 58 net use based process 198 Redirect URL tab LDAP domain 144 NT domain 99 requirements environment 32 router mode 35, 37 definition 299 rule 18 criteria 275 definition 300 rules LDAP server setup 203

## S

screen, terminology 5 search engine, definition 300 secondary IP address 38 Select Groups/Members from Domain window 86 Server Message Block (SMB), definition 300 service port 18 definition 300 session-based authentication (Tier 3) 23 Set Group Priority window LDAP domain 133 NT domain 87 Single Sign-On Novell eDirectory authentication 218 Tier 1 authentication 196 single sign-on authentication (Tier 1) 23 SMB definition 300 disable Signing requirements in Windows 2003 257 protocol 198 Signing 198 SMB/NT name resolution method 200 SSL certificate 48 Active Directory 262 Novell 270 obtain, export from LDAP server 262 Sun ONE 272 SSL settings 116 SSL tab 116 SSO 218 static filtering profiles 13 static group 11 static group, definition 300

sub-group definition 300 sub-topic terminology 6 Sun IPlanet 105 Sun ONE 23 Sun One 105 system requirements 32 technical support 191 text box, terminology 6 Tier 1 net use based authentication 29, 41, 159, 196 Tier 1 and Tier 2 Script 207 Tier 2 time-based, Web-based authentication 204 Tier 2 Script 206 Tier 2, Tier 3 Web-based authentication 29, 42, 159 Tier 3 session-based, Web-based authentication 209 tiers definition 300 Web-based authentication 159 time profile definition 300 profile type 15 time-based authentication (Tier 2) 23 time-based profile 42, 58 topic, terminology 6 tree, terminology 7 Type tab 104

## U

Т

Upload User/Group Profile window LDAP domain 136 NT domain 91 URL, definition 301 Usage Graphs 148 usage logs 55 user objects 108 User tab 108 username formats 274

## V

View Log File window 54 virtual IP address 46, 201 definition 301

#### W

warn setting 19
warn setting, definition 301
wbwatch.log 55
Web-based authentication 28, 39, 47
block page authentication 58
SSL certificate 30
Web-based, definition 301
white list, definition 301
window, terminology 7
Windows 2003
SMB Signing 198
WINS Server 45
name resolution usage 200
workstation requirements 32