8e6 Technologies

8e6® R3000

USER GUIDE

for Authentication

Model: R3000

Release 3.0.00 • Manual Version 1.01

R3000 AUTHENTICATION USER GUIDE

828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published September 2009
To be used with R3000 User Guide version 1.01 for software release 3.0.00

Printed in the United States of America

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.m86security.com/Support/R3000/documentation.asp

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# R3.3.0_AUG_v1.01-0909

CONTENTS

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 and 3 describe the R3000 Administrator console entries that must be made in order to prepare the network for using authentication for LDAP domains.

NOTE*: Refer to the R3000 Quick Start Guide for information on installing the unit 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 4 explains how to assign groups and members for management by Sub Admin group administrators, and how group administrators create and maintain filtering profiles for entities in their assignment.

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; 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.*

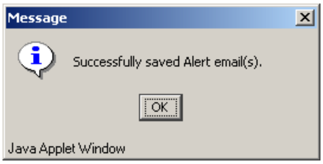
TIP*: The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

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.

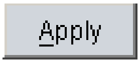
- **alert box** - a message box that opens in response to an entry you made in a dialog box, window, or screen. This box often contains a button (usually labeled “OK”) for you to click in order to confirm or execute a command.


Message

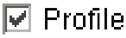
Successfully saved Alert email(s).

Java Applet Window

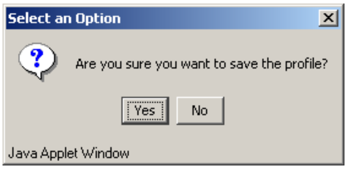
- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.



- **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.


☑ Profile

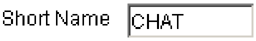
- **dialog box** - a box that opens in response to a command made in a window or screen, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries or selections prior to clicking a button.


Select an Option

Are you sure you want to save the profile?

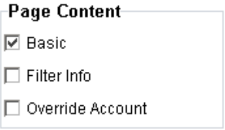
Java Applet Window

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


Short Name CHAT

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-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.



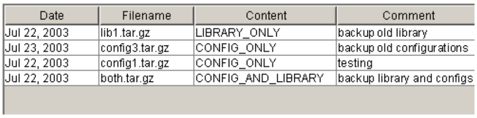
Page Content

☑ Basic

□ Filter Info

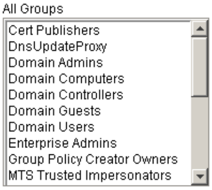
□ Override Account

- **grid** - an area in a frame that displays rows and columns of data, as a result of various processes. This data can be reorganized in the R3000 console, by changing the order of the columns.



Date	Filename	Content	Comment
Jul 22, 2003	lib1.tar.gz	LIBRARY_ONLY	backup old library
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

- **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.

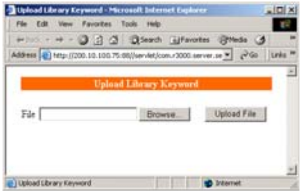


All Groups

Cert Publishers
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Group Policy Creator Owners
MTS Trusted Impersonators

- **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 double-clicked, the tree list opens to reveal items that can be selected.

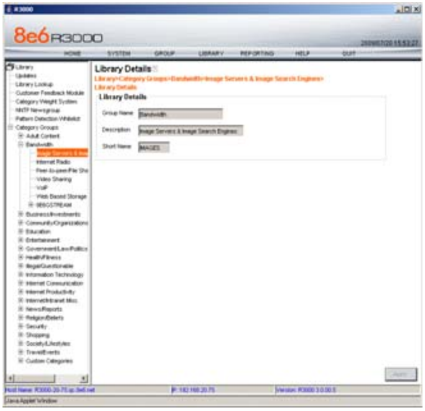
Library
Updates
Library Lookup
CFM
Category Weight System
NNTP Newsgroup
8e6 Supplied Categories
Custom Categories


Upload Library Keyword - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Upload Library Keyword
File
Browse...
Upload File

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

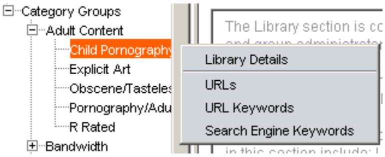
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down-arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.

- **radio button** - a small, circular object 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.



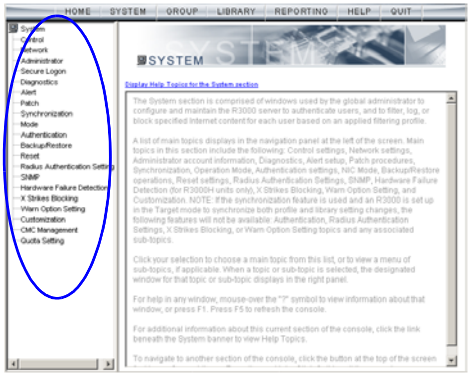
- **screen** - a main object of an application that displays across your monitor. A screen can contain panels, windows, frames, fields, tables, text boxes, list boxes, icons, buttons, and radio buttons.

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



The System section is comprised of windows used by the global administrator to configure and maintain the R3000 server to authenticate users, and to filter, log, or block specified Internet content for each user based on an applied filtering profile.

A list of main topics displays in the navigation panel at the left of the screen. Main topics in this section include the following: Control settings, Network settings, Administrator account information, Diagnostics, Alert setup, Patch procedures, Synchronization, Operation Mode, Authentication settings, NIC Mode, Backup/Restore operations, Reset settings, Radius Authentication Settings, SNMP, Hardware Failure Detection (for R3000H units only), X Strikes Blocking, Warn Option Setting, and Customization. NOTE: If the synchronization feature is used and an R3000 is set up in the Target mode to synchronize both profile and library setting changes, the following features will not be available: Authentication, Radius Authentication Settings, X Strikes Blocking, or Warn Option Setting topics and any associated sub-topics.

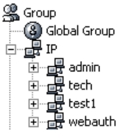
Click your selection to choose a main topic from this list, or to view a menu of sub-topics, if applicable. When a topic or sub-topic is selected, the designated window for that topic or sub-topic displays in the right panel.

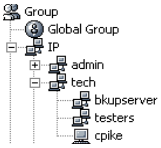
For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link beneath the System banner to view Help Topics.

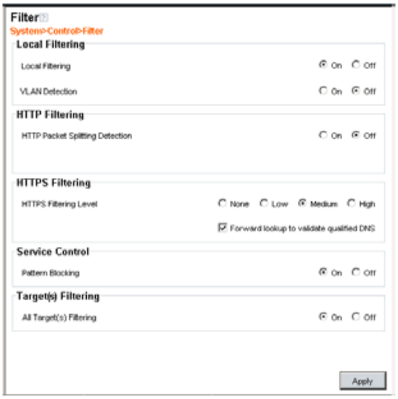
To navigate to another section of the console, click the button at the top of the screen

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


Filter
System>Control>Filter

Local Filtering
Local Filtering ● On ○ Off
VLAN Detection ○ On ● Off

HTTP Filtering
HTTP Packet Splitting Detection ○ On ● Off

HTTPS Filtering
HTTPS Filtering Level ○ None ○ Low ● Medium ○ High
☑ Forward lookup to validate qualified DNS

Service Control
Pattern Blocking ● On ○ Off

Target(s) Filtering
All Target(s) Filtering ● On ○ Off

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**
- **LDAP domain groups**

***NOTES**: 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, and LDAP. If authentication is disabled, only the Global Group and IP branches will be seen.*

A group administrator will only see entities assigned to him/her by the global administrator.

Global Group

The first group that must be set up is the global group, represented in the tree structure by the global icon . 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 sub-group and individual IP members, override account and time profiles, and maintains filtering profiles of all members in the master IP group.

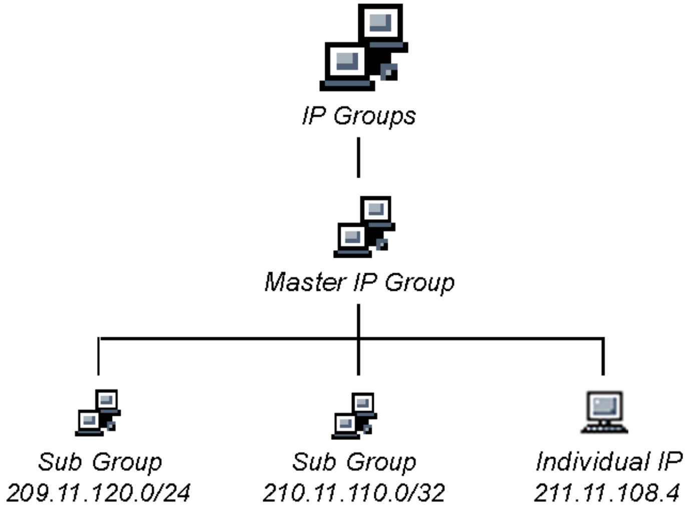


Fig. 1-1 IP diagram with a sample master IP group and its members

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 administrator adds and maintains LDAP domains , and assigns designated group administrators (Sub Admins) access to specific entities (nodes) within that domain. The group administrator creates and maintains filtering profiles for nodes assigned to him/her. For Active Directory or "Other" server types, these nodes include primary or static groups , workstations , users , or containers . For Open Directory, nodes include groups and users. For Novell eDirectory, SunOne, Sun IPlanet, or Netscape Directory server types, these nodes also include dynamic groups . If users belong to more than one group, the global administrator sets the priority for group filtering.

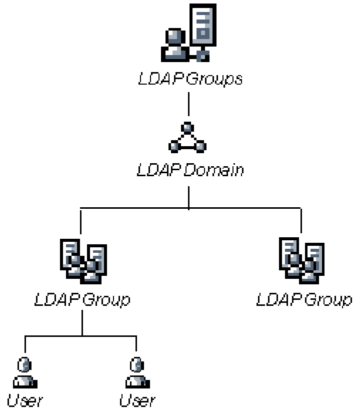


Fig. 1-2 LDAP domain diagram, with sample groups and members

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

- **LDAP group filtering profile** - used by an LDAP group.
- **LDAP workstation filtering profile** - used by an LDAP workstation in an LDAP domain. This is a static profile that is tied to the IP address of a given workstation and not to a particular user.

- **LDAP member filtering profile -** used by an LDAP group member.
- **LDAP container filtering profile** - used by an LDAP container in an LDAP domain.
- **LDAP time profile** - used by an LDAP entity at a specified time.

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.
- **Radius profile -** used by end users on a Radius accounting server if the Radius server is connected to the R3000 and the Radius authentication feature enabled.
- **TAR profile** - used if a Threat Analysis Reporter (TAR) server is connected to the R3000 and an end user is locked out by TAR when attempting to access blocked content in a library category.

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, 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.

LDAP Filtering Profiles

A filtering profile for an LDAP group, workstation, member, or container is created by the group administrator assigned to that entity within a domain.

For group profiles, 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.

For workstation profiles, the profile remains at a given workstation set up within an LDAP domain, so that any user who logs into that workstation will use the same profile as the previous user who logged onto that machine.

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/Bing/Yahoo!/Ask/AOL 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.

***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. Access to an open library category can be restricted to a set number of minutes. 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 and LDAP groups, and takes precedence over filtering settings made for group, member, and workstation 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”

***NOTE**: Using the quota feature, access to an open category can be restricted to a defined number of minutes.*

- **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

***NOTE**: A category that is allowed will override any blocked settings except if the minimum filtering level is set to block that category.*

- **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 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 LDAP authentication domain
2. If a minimum filtering level is defined, it applies to all master IP groups (and their members) and 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.

6. For LDAP users, if a user is authenticated, settings for the user’s group or individual profile from the 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.

***NOTE**: In an LDAP domain, if a user belongs to a container, that profile takes precedence over the group profile for that user.*

   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. A profile for a workstation takes precedence over a user’s individual profile.

   d. If the user has a time profile, that profile takes precedence over other profiles. A group time profile takes precedence over a domain time profile, and a container time profile takes precedence over a group time profile. An individual time profile takes precedence over a container time profile, and a workstation time profile takes precedence over an individual time profile.

***NOTE**: A Radius profile is another type of authentication profile and is weighted the same as LDAP authentication profiles in the precedence hierarchy.*

7. An override account profile takes precedence over an authentication profile or a time 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.

***NOTE**: A Threat Analysis Reporter (TAR) profile is another type of lock profile that is weighted the same as a lock profile in the precedence hierarchy.*

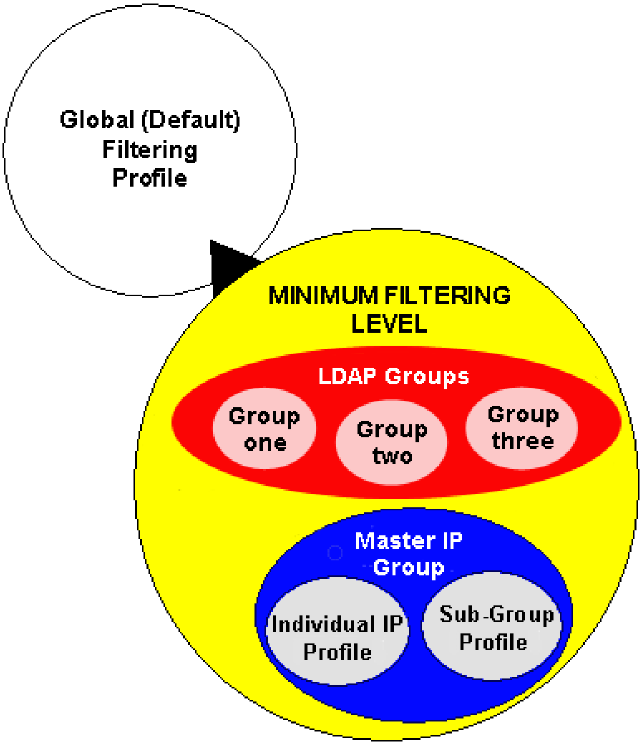


Fig. 1-3 Sample filtering hierarchy diagram

Authentication Solutions

LDAP Authentication Protocol

The R3000 supports the authentication protocol Lightweight Directory Access Protocol (LDAP).

LDAP authentication supports all versions of LDAP, such as Microsoft Active Directory, Novell eDirectory, Sun ONE, OpenLDAP, and Open Directory.

R3000 Authentication Tiers and Options

R3000 authentication tiers

The R3000 authentication architecture for the LDAP authentication protocol is comprised of three tiers. When using 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 Active Directory domains.
- Tier 2: Time-based, Web authentication for the LDAP authentication method.
- Tier 3: Session-based, Web authentication for the 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 Authenticator**	**eDirectory 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 Authenticator	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 2000/2003 Server (both Mixed and Native modes)	Tier 1 "net use" 8e6 Authenticator for Windows AD Agent	Tier 2 or Tier 3
Novell eDirectory	8e6 Authenticator for Windows 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 for Windows Novell eDirectory Agent AD Agent	Tier 2 or Tier 3
Open Directory	8e6 Authenticator for Apple	Tier 2 or Tier 3

Ports for Authentication System Access

The following ports should be used for authentication system access:

Type	No.	Function
TCP	8081	Used between the R3000's transmitting interface and the SSL block page for Tier 2 or Tier 3 authentication.
TCP	836	Used between the R3000's Virtual IP address and Java applet for Tier 3 authentication.
TCP	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 controllers in order to bind with them so that user/ group information can be queried/accessed.
LDAPS	636	Used for communicating with domain controllers 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 *255.255.255.255* 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 Active Directory servers.
   - Tier 2: Choose this option if you wish to use timed Web-based authentication for 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 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”.

5. Select “Authentication” from the navigation panel, and then select Authentication SSL Certificate from the pop-up 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 Re-authentication 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 re-authentication purposes.

7. Select “Administrator” from the navigation panel to access the Administrator window. Add group administrator (Sub Admin) accounts in this window. Sub Admin

group administrators will later be assigned to manage entities (nodes) in the LDAP branch of the Group tree.

Group section

In the Group section of the Administrator console, choose 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. Do either of the following as necessary:
   - Assign a group administrator to oversee the newly-added domain and to set up filtering profiles for all groups and members within that domain
   - Assign Sub Admin group administrators to specific groups and let them create filtering profiles for their group and its members
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.

CHAPTER 2: NETWORK SETUP

Environment Requirements

Workstation Requirements

Administrator

Minimum system requirements for the administrator include the following:

- Windows 2000 or later operating system (not compatible with Windows server 2003) running Internet Explorer (IE) 6.0 or 7.0, or Firefox 3.0
- Macintosh OS X Version 10.5 running Safari 3.1.2, or Firefox 3.0
- 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 user interface.*

End User

Minimum system requirements for the end user include the following:

- Windows 2000 or later operating system (not compatible with Windows server 2003) running Internet Explorer (IE) 6.0 or 7.0, or Firefox 3.0
- Macintosh OS X Version 10.5 running Safari 3.1.2, or Firefox 3.0
- Linux OS running Firefox 3.0
- 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
- 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

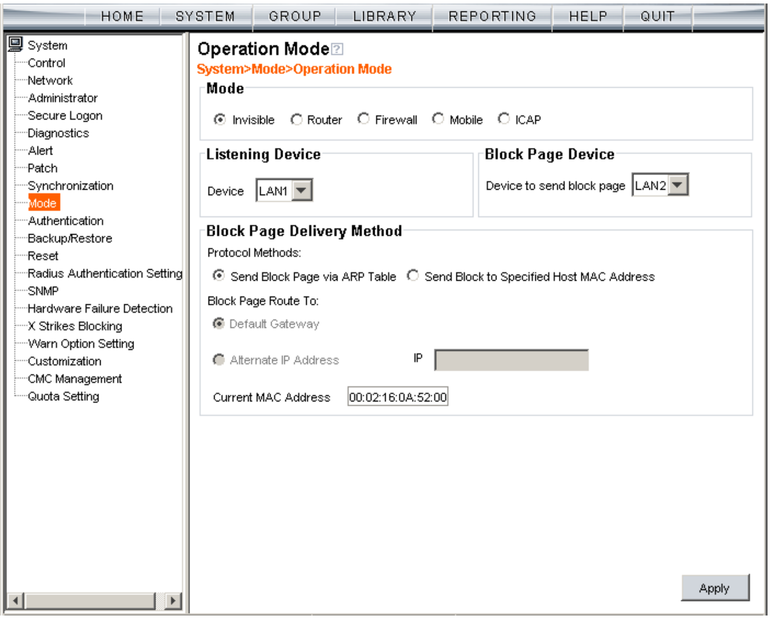
Set up the Network for Authentication

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), 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.

View Log File can be used for troubleshooting authentication setup.

Specify the operation mode

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



Operation Mode

System>Mode>Operation Mode

Mode

● Invisible ○ Router ○ Firewall ○ Mobile ○ ICAP

Listening Device

Device LAN1

Block Page Device

Device to send block page LAN2

Block Page Delivery Method

Protocol Methods:

● Send Block Page via ARP Table ○ Send Block to Specified Host MAC Address

Block Page Route To:

● Default Gateway

○ Alternate IP Address IP

Current MAC Address 00:02:16:0A:52:00

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:

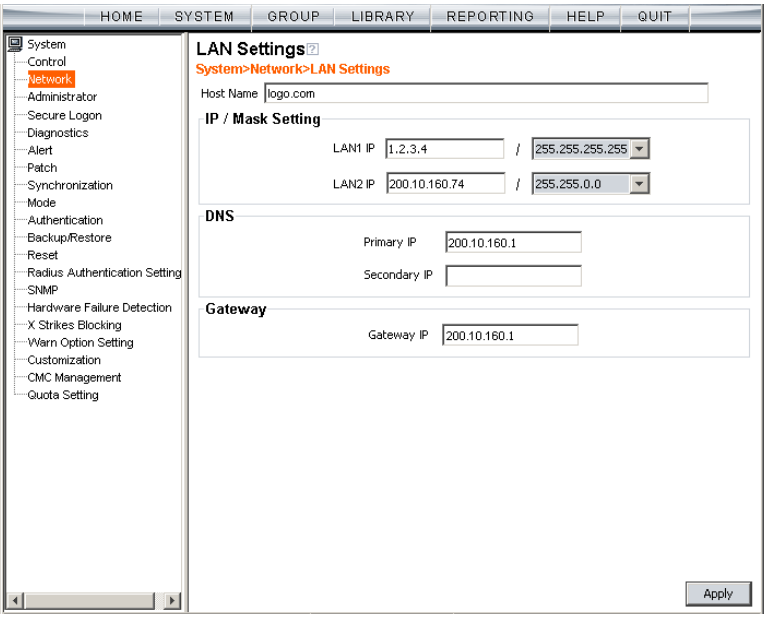
     - “Default Gateway” - this option indicates that the default gateway on your network will be used for sending block pages.
     - “Alternate IP Address” - this option should be used if block pages are not being served.

       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:



LAN Settings

System>Network>LAN Settings

Host Name: logo.com

IP / Mask Setting

LAN1 IP: 1.2.3.4 / 255.255.255.255

LAN2 IP: 200.10.160.74 / 255.255.0.0

DNS

Primary IP: 200.10.160.1

Secondary IP:

Gateway

Gateway IP: 200.10.160.1

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.

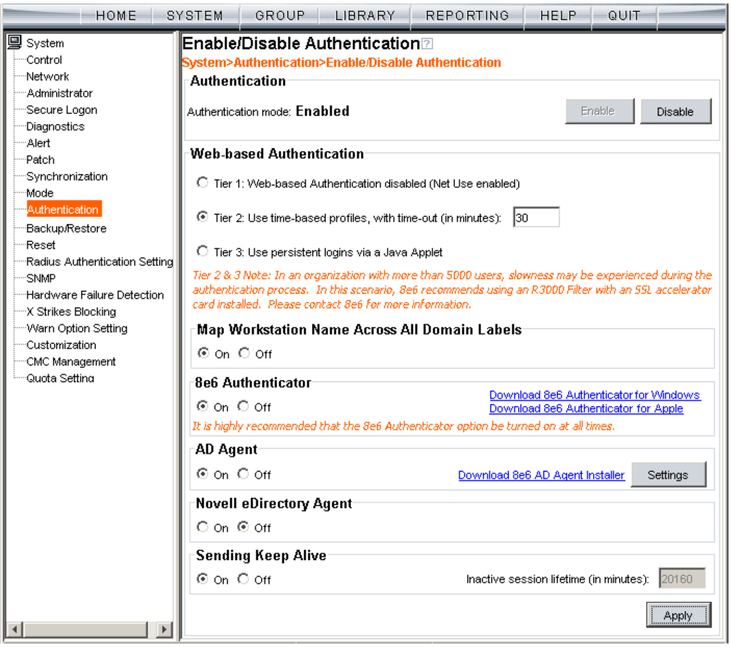
***NOTE**: Whenever modifications are made in this window, the server must be restarted in order for the changes to take effect.*

Enable authentication, specify criteria

1. 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:



Enable/Disable Authentication

System>Authentication>Enable/Disable Authentication

Authentication

Authentication mode: **Enabled**

Web-based Authentication

○ Tier 1: Web-based Authentication disabled (Net Use enabled)

● Tier 2: Use time-based profiles, with time-out (in minutes): 30

○ Tier 3: Use persistent logins via a Java Applet

Tier 2 & 3 Note: 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.

Map Workstation Name Across All Domain Labels

● On ○ Off

8e6 Authenticator

● On ○ Off

It is highly recommended that the 8e6 Authenticator option be turned on at all times.

AD Agent

● On ○ Off

Novell eDirectory Agent

○ On ● Off

Sending Keep Alive

● On ○ Off

Inactive session lifetime (in minutes): 20160

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:

    - If using LDAP authentication and workstation profiles, click “On” in the Map Workstation Name Across All Domain Labels frame to enable the R3000 to search other domain labels if it can’t find the workstation’s NetBIOS name under a specified domain label, based on the user’s full Distinguished Name.
    - 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 for Windows (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 downloading the 8e6 Authenticator for Apple (Authenticator), an Open Directory server should be used. The end user will be automatically authenticated when logging into the 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 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.

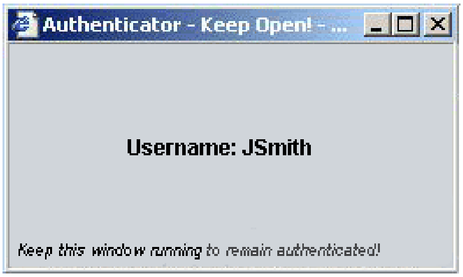
NOTE*: If selecting either Tier 2 or Tier 3, please be informed that in an organization with more than 5000 users, slowness may be experienced during the authentication process. In this scenario, 8e6 recommends using an R3000 Filter with an SSL accelerator card installed. Please contact 8e6 for more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

Tier 2: Use time-based profiles, with time-out (in minutes) – Choose this option if using 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 LDAP authentication, and you want the user to maintain a persistent network connection.

This option opens a profile window that uses a Java applet:



Username: JSmith

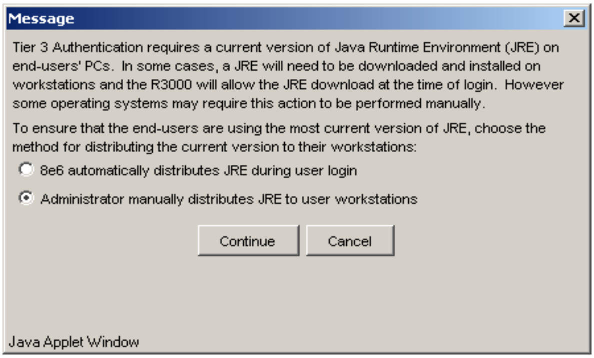
Keep this window running to remain authenticated!

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

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:

○ 8e6 automatically distributes JRE during user login

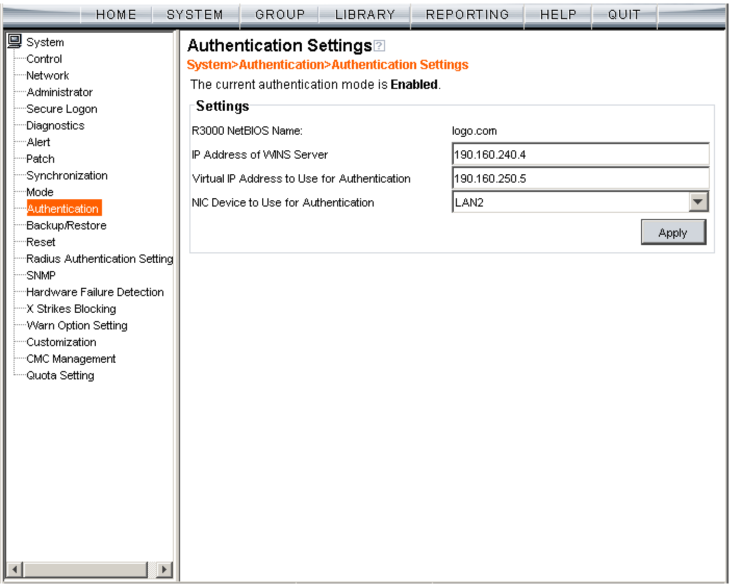
● Administrator manually distributes JRE to user workstations

Fig. 2-5 Tier 3 dialog box

3. 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

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



Authentication Settings

System>Authentication>Authentication Settings

The current authentication mode is **Enabled**.

Settings

R3000 NetBIOS Name: logo.com

IP Address of WINS Server: 190.160.240.4

Virtual IP Address to Use for Authentication: 190.160.250.5

NIC Device to Use for Authentication: LAN2

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.

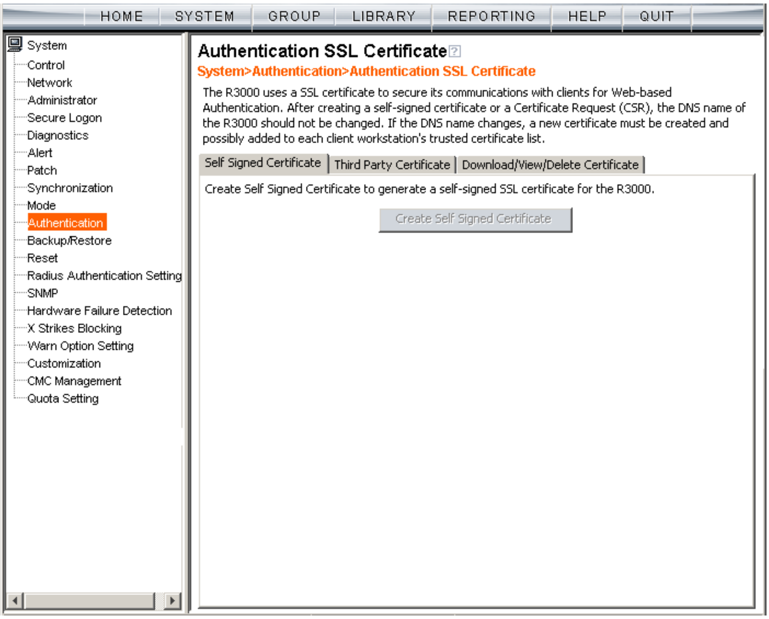
⚠ ***WARNING****: If the IP address entered here is not in the same subnet as this R3000, the net use connection will fail.*

4. From the **NIC Device to Use for Authentication** pull-down 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.

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:



Authentication SSL Certificate

System>Authentication>Authentication SSL Certificate

The R3000 uses a SSL certificate to secure its communications with clients for Web-based Authentication. After creating a self-signed certificate or a Certificate Request (CSR), the DNS name of the R3000 should not be changed. If the DNS name changes, a new certificate must be created and possibly added to each client workstation's trusted certificate list.

Create Self Signed Certificate to generate a self-signed SSL certificate for the R3000.

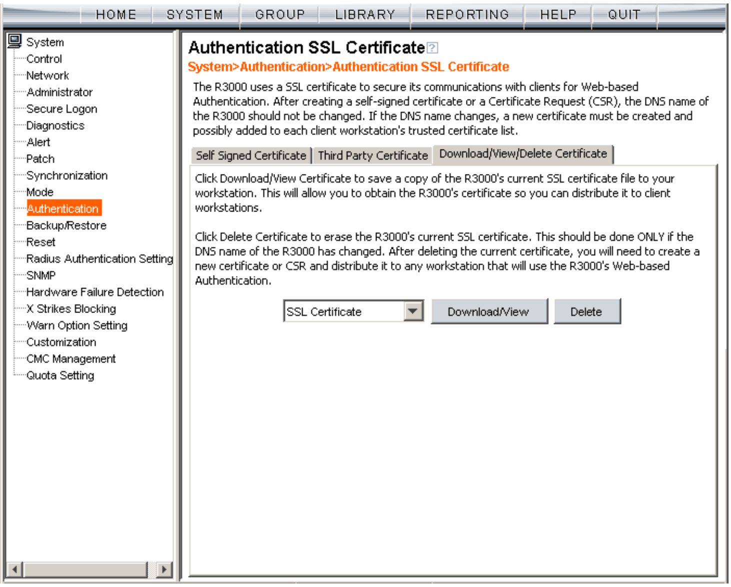
Fig. 2-7 Authentication SSL Certificate window

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, upload, 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:



Authentication SSL Certificate

System>Authentication>Authentication SSL Certificate

The R3000 uses a SSL certificate to secure its communications with clients for Web-based Authentication. After creating a self-signed certificate or a Certificate Request (CSR), the DNS name of the R3000 should not be changed. If the DNS name changes, a new certificate must be created and possibly added to each client workstation's trusted certificate list.

Click Download/View Certificate to save a copy of the R3000's current SSL certificate file to your workstation. This will allow you to obtain the R3000's certificate so you can distribute it to client workstations.

Click Delete Certificate to erase the R3000's current SSL certificate. This should be done ONLY if the DNS name of the R3000 has changed. After deleting the current certificate, you will need to create a new certificate or CSR and distribute it to any workstation that will use the R3000's Web-based Authentication.

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

3. Select the type of certificate from the pull-down menu: “SSL Certificate” or “Intermediate Certificate”. An intermediate certificate is a signing certificate for an SSL certificate.

4. 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 certificate to a specified folder on your workstation.

***NOTE**: While the 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.*

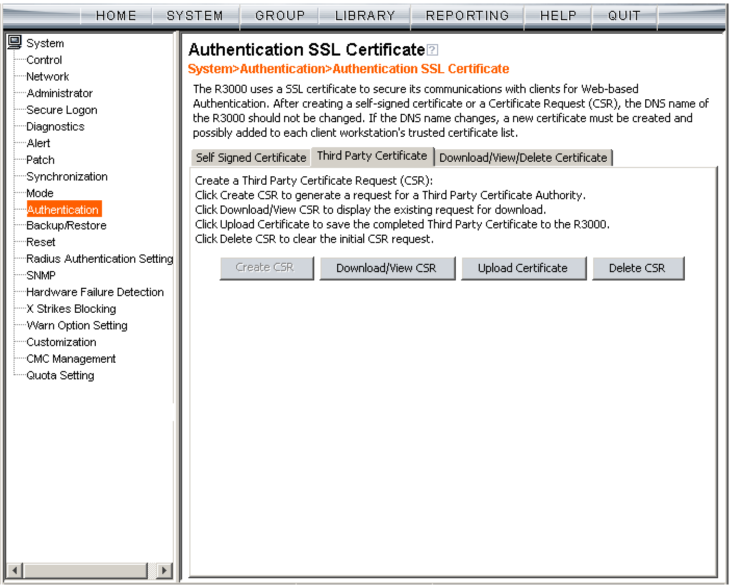
Once the certificate is saved to your workstation, it can be distributed to client workstations for users who need to be authenticated.

***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:



Authentication SSL Certificate

System>Authentication>Authentication SSL Certificate

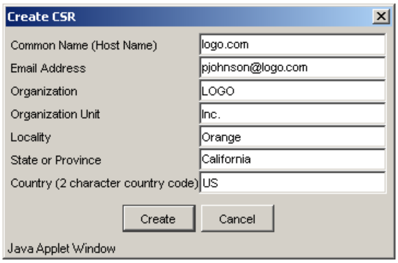
The R3000 uses a SSL certificate to secure its communications with clients for Web-based Authentication. After creating a self-signed certificate or a Certificate Request (CSR), the DNS name of the R3000 should not be changed. If the DNS name changes, a new certificate must be created and possibly added to each client workstation's trusted certificate list.

Create a Third Party Certificate Request (CSR):
Click Create CSR to generate a request for a Third Party Certificate Authority.
Click Download/View CSR to display the existing request for download.
Click Upload Certificate to save the completed Third Party Certificate to the R3000.
Click Delete CSR to clear the initial CSR request.

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): logo.com
Email Address: pjohnson@logo.com
Organization: LOGO
Organization Unit: Inc.
Locality: Orange
State or Province: California
Country (2 character country code): US

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. In the Third Party Certificate tab, click **Upload Certificate** to open the Upload Signed SSL Certificate for R3000 pop-up window:

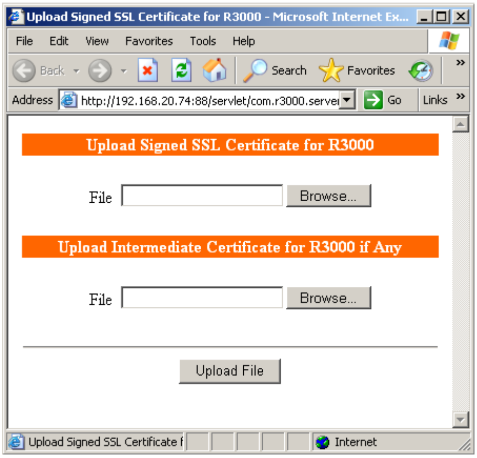

Upload Signed SSL Certificate for R3000 - Microsoft Internet Ex...
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.20.74:88/servlet/com.r3000.server Go Links
Upload Signed SSL Certificate for R3000
File Browse...
Upload Intermediate Certificate for R3000 if Any
File Browse...
Upload File
Upload Signed SSL Certificate f
Internet

Fig. 2-11 Upload Signed SSL Certificate box

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

***NOTE**: Do not click this button until performing the actions in the following steps.*

***TIP**: Click **Cancel** in the dialog box to cancel the procedure.*

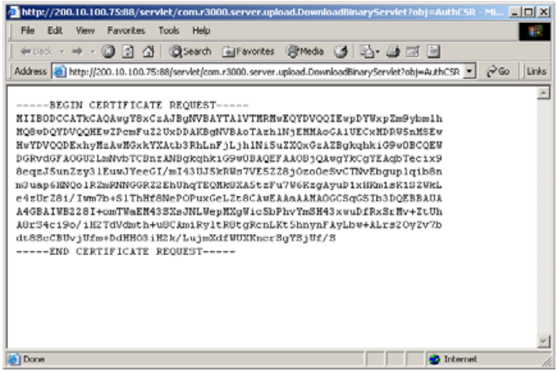
2. In the Upload Signed SSL Certfficate for R3000 pop-up window, do one of the following, as appropriate:
   - Click **Browse** in the Upload Signed SSL Certificate for R3000 section if the certificate to be uploaded is an SSL certificate.
   - Click **Browse** in the Upload Intermediate Certificate for R3000 if Any section if an intermediate certificate is required for signing an uploaded SSL certificate.

Clicking the Browse button opens 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

1. In the Third Party Certificate tab, click **Download/View CSR** to open a pop-up window containing the contents of the certificate request:



http://200.10.100.75:88/servlet/com.r3000.server.upload.DownloadBinaryServlet?obj=AuthCSR - Mi...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://200.10.100.75:88/servlet/com.r3000.server.upload.DownloadBinaryServlet?obj=AuthCSR
Go
Links
Done
Internet

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBODCCATkCAQAwgY8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MQ8wDQYDVQQHEwZPcmFuZ2UxDDAKBgNVBAoTAzhlNjEMMAoGA1UECxMDRW5nMSEw
HwYDVQQDExhyMzAwMGxkYXAtb3RhLnFjLjhlNi5uZXQxGzAZBgkqhkiG9w0BCQEW
DGRvdGFAOGU2LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAqbTecix9
8eqzJ5unZzy31EuwJYeeGI/mI43UJ5kRWs7VE5ZZ8jOzoOeSvCTNvEhgup1qib8n
mJuap6HNQo1R2mRNNGGR22EhUhqTEQMkUXAStzFu7W6KzgAyuD1xHKm1sK1S2WkL
e4zUrZ8i/Iwm7b+S1ThHf8NePOPuxGeLZt8CAwEAAaAAMA0GCSqGSIb3DQEBBAUA
A4GBAIWB228I+omTWaEM43SXsJNLWepMXgWic5bPhvYmSH43xwuDfRxSrMv+ZtUh
A0rS4ci9o/iH2TdVdmth+u8CAmiRy1tR8tgRcnLKt5hnynFAyLbw+ALrs2Oy2v7b
dt8ScCBUvjUfm+DdHH03iH2k/LujmXdfWUXKncrSgYSjUf/S
-----END CERTIFICATE REQUEST-----
```

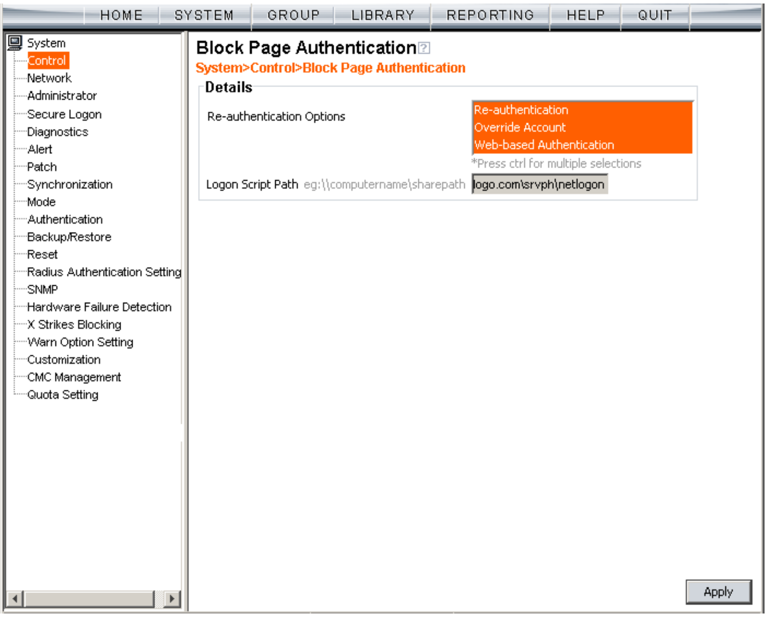
Fig. 2-12 Download CSR pop-up window

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.*

Specify block page settings

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



Block Page Authentication

System>Control>Block Page Authentication

Details

Re-authentication Options: Re-authentication, Override Account, Web-based Authentication

*Press ctrl for multiple selections

Logon Script Path eg:\\computername\sharepath logo.com\srvph\netlogon

Fig. 2-13 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 the LDAP authentication method.
   - **Re-authentication** - select this option for the re-authentication 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.

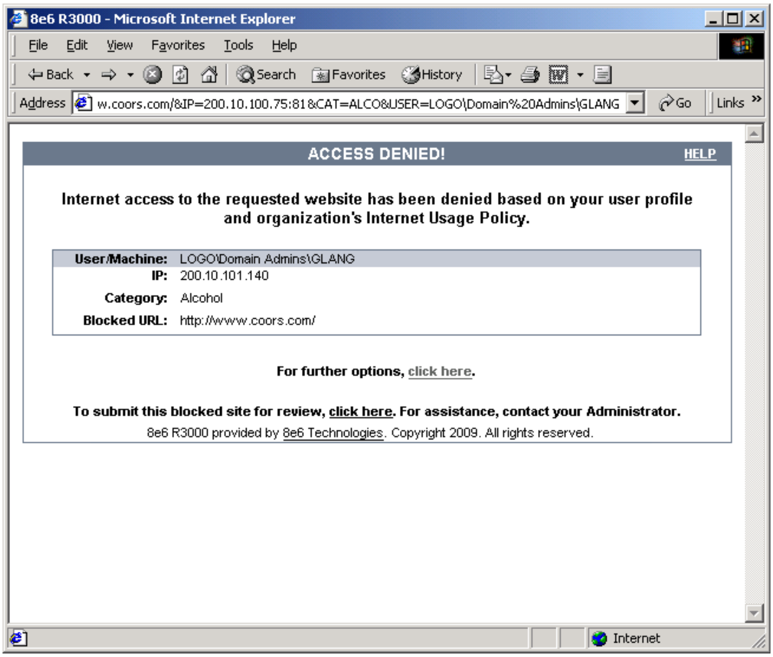
***TIP**: Multiple options can be selected by clicking each option while pressing the Ctrl key on your keyboard.*

***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 Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
Internet

w.coors.com/&IP=200.10.100.75:81&CAT=ALCO&USER=LOGO\Domain%20Admins\GLANG

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
Blocked URL:	http://www.coors.com/

For further options, click here.

To submit this blocked site for review, click here. For assistance, contact your Administrator.

8e6 R3000 provided by 8e6 Technologies. Copyright 2009. All rights reserved.

Fig. 2-14 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 B: 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 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.

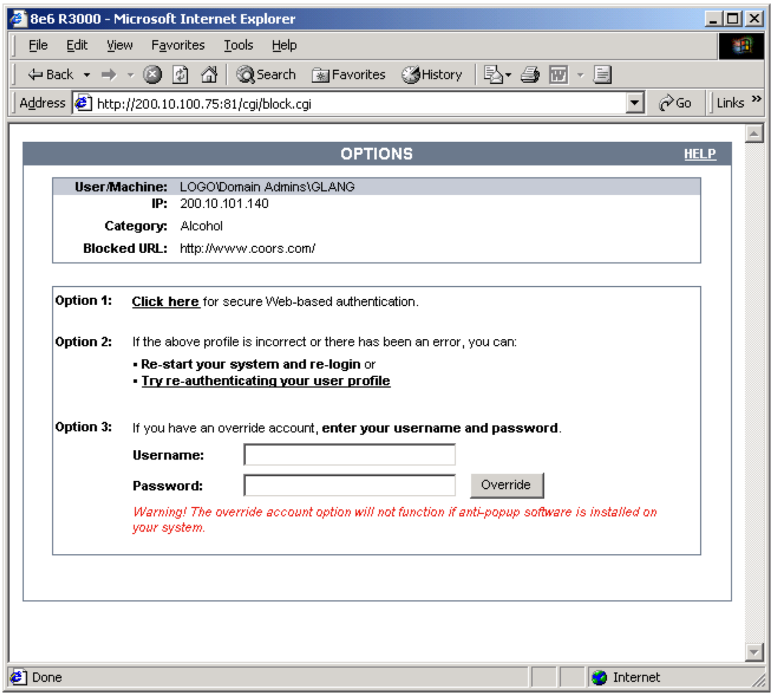
Optional Links

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

- **For further options, click here. -** 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, click here. -** 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, click here.**


8e6 R3000 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://200.10.100.75:81/cgi/block.cgi
Go Links
Done
Internet

OPTIONS HELP

User/Machine: LOGO\Domain Admins\GLANG
IP: 200.10.101.140
Category: Alcohol
Blocked URL: http://www.coors.com/

Option 1: Click here 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
- **Try re-authenticating your user profile**

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.

Fig. 2-15 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

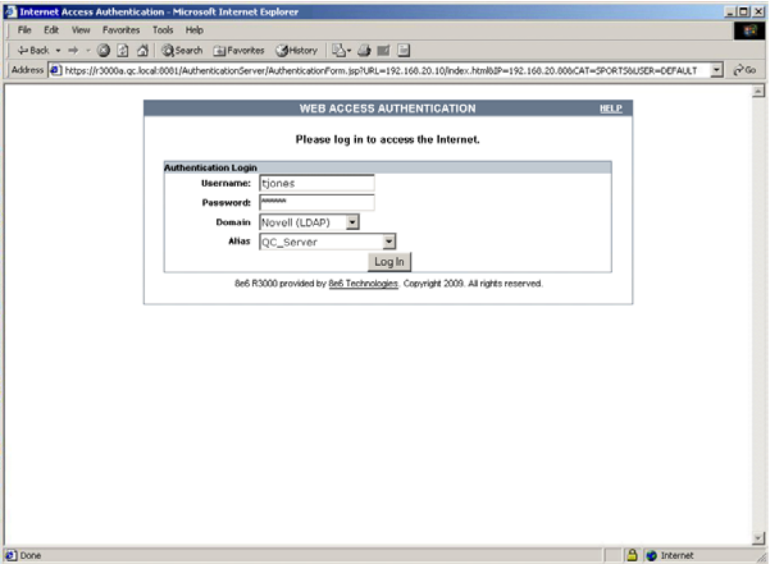
The frame beneath the User/Machine frame includes information for options (1, 2, and/or 3) based on settings made in the Block Page Authentication window.

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:



Internet Access Authentication - Microsoft Internet Explorer

Address: https://r3000a.qc.local:8081/AuthenticationServer/AuthenticationForm.jsp?URL=192.168.20.10/index.html&IP=192.168.20.80&CAT=SPORTS&USER=DEFAULT

WEB ACCESS AUTHENTICATION

Please log in to access the Internet.

Authentication Login

Username: tjones
Password: ******
Domain: Novell (LDAP)
Alias: QC_Server

8e6 R3000 provided by 8e6 Technologies. Copyright 2009. All rights reserved.

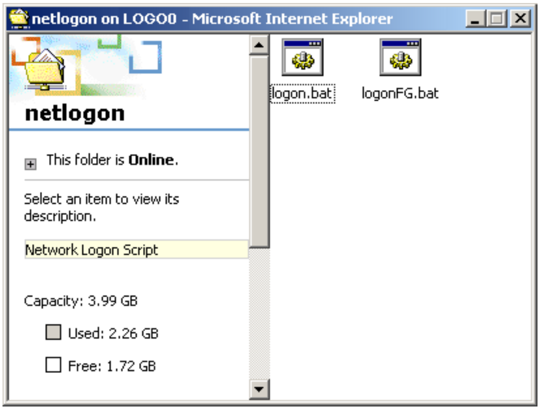
Fig. 2-16 Authentication Request Form

***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 Re-authentication Options (Re-authentication, or Web-based 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.
- **Try re-authenticating your user profile** - This link displays if “Re-authentication” was selected at the Re-authentication Options field, and an entry was made in the Logon Script Path field. When the user clicks this link, a window opens:



This folder is **Online**.

Select an item to view its description.

Network Logon Script

Capacity: 3.99 GB

Used: 2.26 GB

Free: 1.72 GB

Fig. 2-17 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.

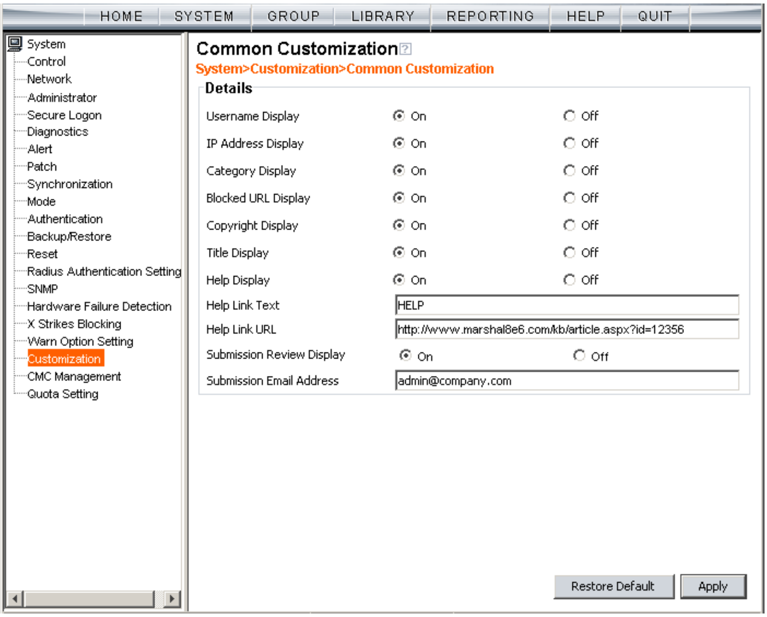
***NOTES**: See Appendix E: Override Pop-up Blockers for information on how a user with an override account can authenticate if a pop-up blocker is installed on his/her workstation.*

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:



Common Customization

System>Customization>Common Customization

Details

Username Display	● On	○ Off
IP Address Display	● On	○ Off
Category Display	● On	○ Off
Blocked URL Display	● On	○ Off
Copyright Display	● On	○ Off
Title Display	● On	○ Off
Help Display	● On	○ Off
Help Link Text	HELP	
Help Link URL	http://www.marshal8e6.com/kb/article.aspx?id=12356	
Submission Review Display	● On	○ Off
Submission Email Address	admin@company.com	

Fig. 2-18 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.m86security.com/kb/article.aspx?id=12356* 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 **click here** 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.*

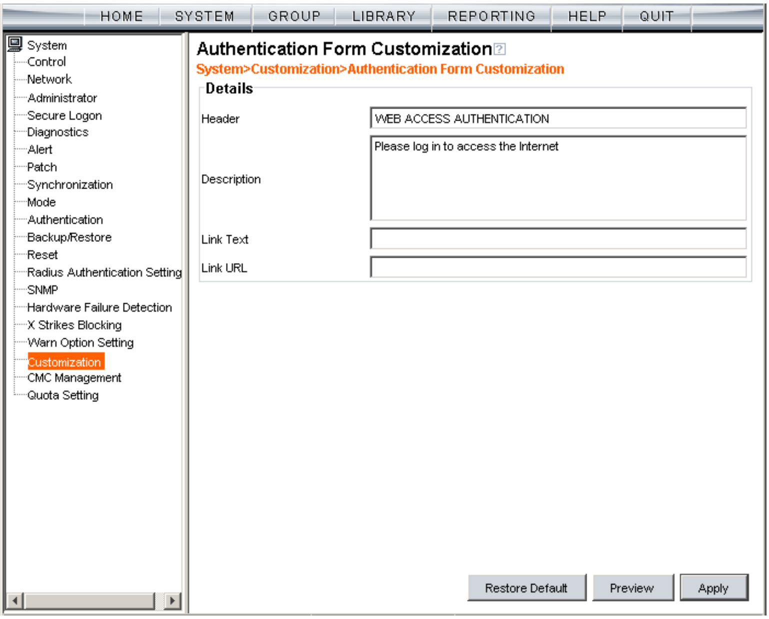
- **Submission Email Address** - By default, *admin @company.com* displays in block pages as the email address of the administrator to receive feedback on content the end user feels has been incorrectly blocked. Enter the global administrator's email address.

2. Click **Apply** to save your entries.

***TIP**: Click **Restore Default** and then **Apply** 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:



Authentication Form Customization

System>Customization>Authentication Form Customization

Details

Header: WEB ACCESS AUTHENTICATION

Description: Please log in to access the Internet

Link Text:

Link URL:

Fig. 2-19 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.

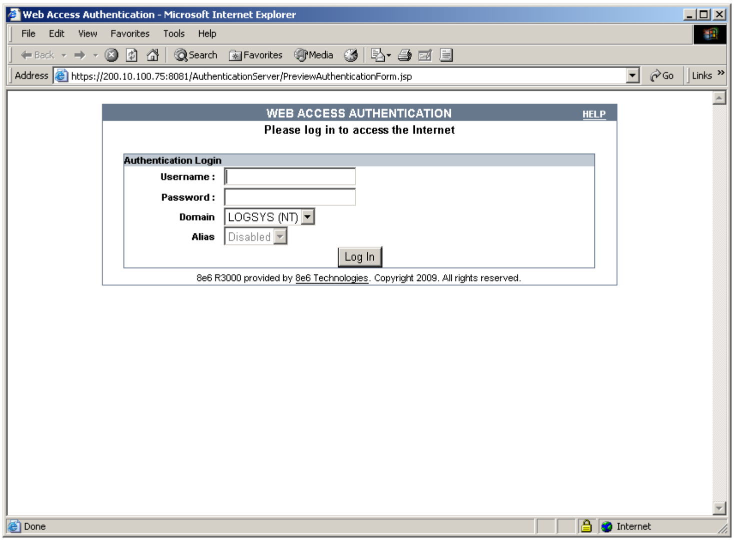
   Any entries made in these fields will display centered in the Authentication Request Form, using the Arial font type.

2. Click **Apply**.

***TIP**: Click **Restore Default** and then **Apply** 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

Address https://200.10.100.75:8081/AuthenticationServer/PreviewAuthenticationForm.jsp

WEB ACCESS AUTHENTICATION HELP

Please log in to access the Internet

Authentication Login

Username :

Password :

Domain LOGSYS (NT)

Alias Disabled

Log In

8e6 R3000 provided by 8e6 Technologies. Copyright 2009. All rights reserved.

Done Internet

Fig. 2-20 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:

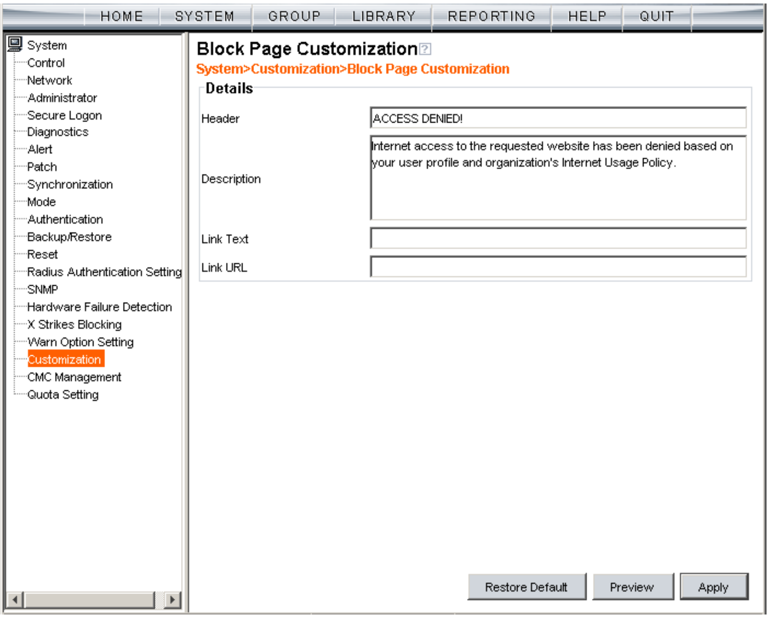
- **HELP** - Clicking this link takes the user to 8e6’s Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6’s Web site.

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:



Block Page Customization

System>Customization>Block Page Customization

Details

Header: ACCESS DENIED!

Description: Internet access to the requested website has been denied based on your user profile and organization's Internet Usage Policy.

Link Text:

Link URL:

Fig. 2-21 Block Page Customization window

***NOTE**: See Appendix B: 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.

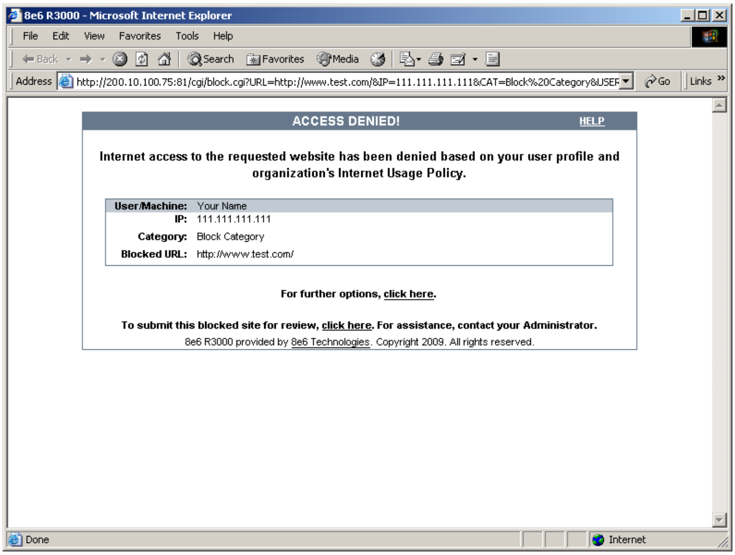
   Any entries made in these fields will display centered in the customized block page, using the Arial font type.

2. Click **Apply**.

***TIP**: Click **Restore Default** and then **Apply** 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:


8e6 R3000 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Go
Links
Done
Internet

Address http://200.10.100.75:81/cgi/block.cgi?URL=http://www.test.com/&IP=111.111.111.111&CAT=Block%20Category&USER

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:	Your Name
IP:	111.111.111.111
Category:	Block Category
Blocked URL:	http://www.test.com/

For further options, click here.

To submit this blocked site for review, click here. For assistance, contact your Administrator.

8e6 R3000 provided by 8e6 Technologies. Copyright 2009. All rights reserved.

Fig. 2-22 Sample Customized Block Page

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

- **User/Machine** field - The username displays for the 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, click here.** - 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 subsection.
- **To submit this blocked site for review, click here.** - 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.*

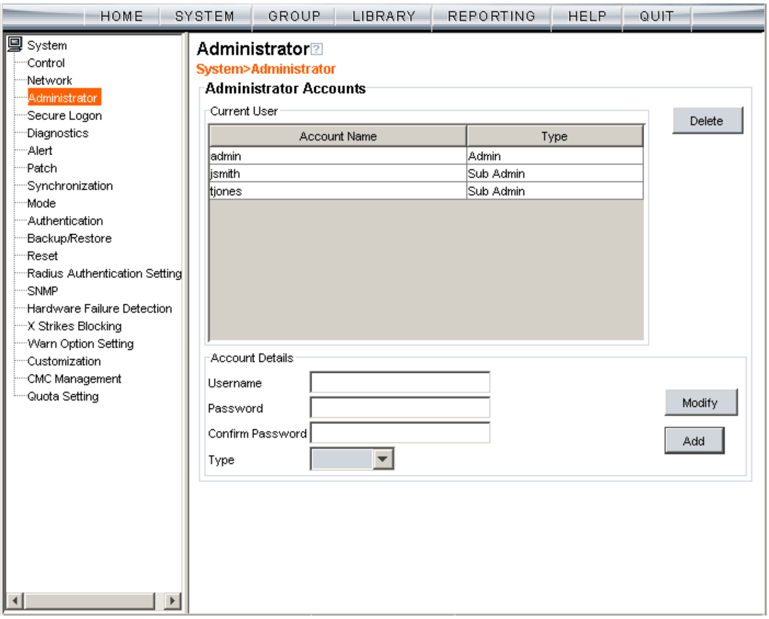
Set up Group Administrator Accounts

The global administrator creates group administrator (Sub Admin) accounts so that these group administrators can be assigned to manage specific LDAP entities (nodes) set up in the Group tree. Sub Admin group administrator accounts are set up in the Administrator window from the System section of the console.

NOTE: *IP group administrator accounts are set up in the IP branch of the Group tree when new IP groups are created. See Chapter 2: Group screen from the Global Administrator Section of the R3000 User Guide for information on creating IP groups.*

Add Sub Admins to manage nodes

Click Administrator to display the Administrator window:



Account Name	Type
admin	Admin
jsmith	Sub Admin
tjones	Sub Admin

Fig. 2-23 Administrator window

Add a group administrator account

To add an LDAP group administrator (Sub Admin) account:

1. In the Account Details frame, enter the username in the **Username** field.
2. In the **Password** field, enter eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
3. Make the same entry again in the **Confirm Password** field.
4. Select "Sub Admin" from the **Type** pull-down menu.
5. Click **Add** to include the username and account type in the Current User list box.

Update the group administrator's password

1. Select the username from the Current User list box; this action populates the Account Details frame with data.
2. In the **Password** field, enter eight to 20 characters for a new password—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
3. Enter the same new password again in the **Confirm Password** field.
4. Click **Modify** to apply your settings.

Delete a group administrator account

To delete an administrator account:

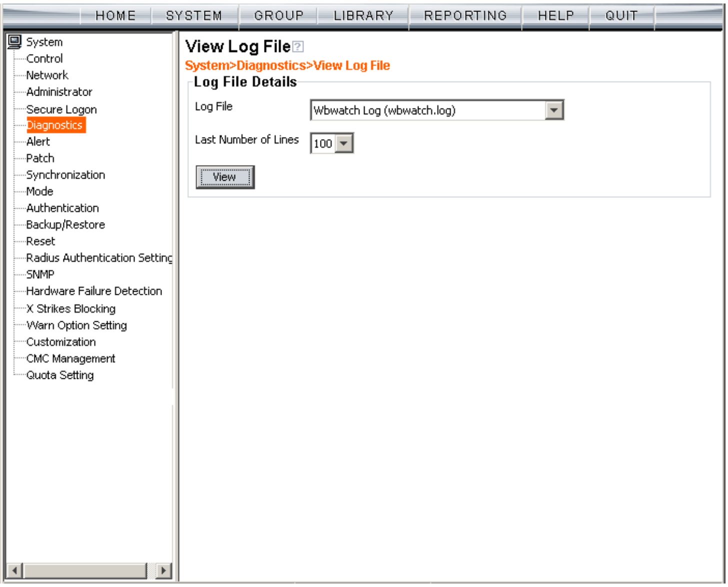
1. Select the username from the Current User list box.
2. Click **Delete** to remove the account.

NOTE*: If a group administrator assigned to an LDAP node is deleted, that group administrator must be removed from assignment to that node and another group administrator set up for assignment to manage that node. See Chapter 4: Manage Nodes for information on assigning and re-assigning a node for management.*

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 pop-up menu to display the View Log File window:



View Log File

System>Diagnostics>View Log File

Log File Details

Log File: Wbwatch Log (wbwatch.log)

Last Number of Lines: 100

Fig. 2-24 View Log File window

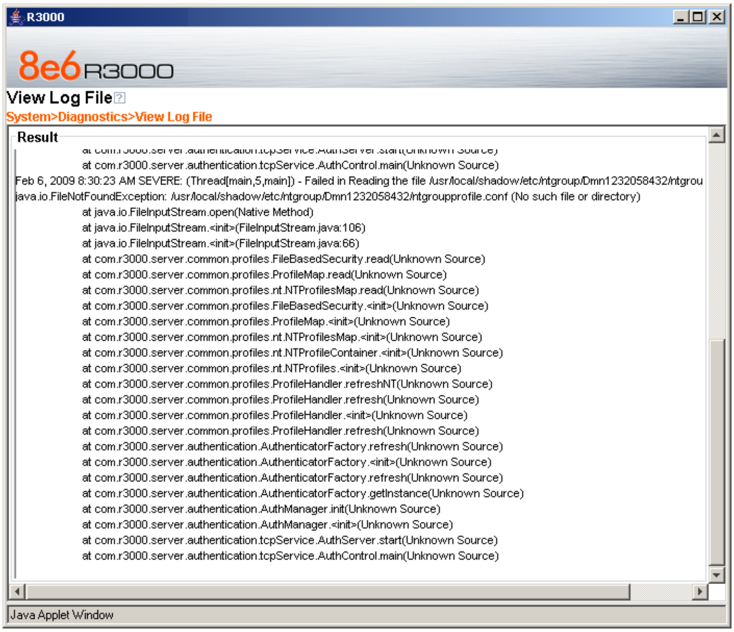
***NOTE**: In this user guide, only authentication-related options will be addressed. For information about all other options, see the View Log File window in the R3000 User Guide.*

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.
   - “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:



```
                at com.r3000.server.authentication.tcpService.AuthServer.start(Unknown Source)
                at com.r3000.server.authentication.tcpService.AuthControl.main(Unknown Source)
Feb 6, 2009 8:30:23 AM SEVERE: (Thread[main,5,main]) - Failed in Reading the file /usr/local/shadow/etc/ntgroup/Dmn1232058432/ntgrou
java.io.FileNotFoundException: /usr/local/shadow/etc/ntgroup/Dmn1232058432/ntgroupprofile.conf (No such file or directory)
                at java.io.FileInputStream.open(Native Method)
                at java.io.FileInputStream.<init>(FileInputStream.java:106)
                at java.io.FileInputStream.<init>(FileInputStream.java:66)
                at com.r3000.server.common.profiles.FileBasedSecurity.read(Unknown Source)
                at com.r3000.server.common.profiles.ProfileMap.read(Unknown Source)
                at com.r3000.server.common.profiles.nt.NTProfilesMap.read(Unknown Source)
                at com.r3000.server.common.profiles.FileBasedSecurity.<init>(Unknown Source)
                at com.r3000.server.common.profiles.ProfileMap.<init>(Unknown Source)
                at com.r3000.server.common.profiles.nt.NTProfilesMap.<init>(Unknown Source)
                at com.r3000.server.common.profiles.nt.NTProfileContainer.<init>(Unknown Source)
                at com.r3000.server.common.profiles.nt.NTProfiles.<init>(Unknown Source)
                at com.r3000.server.common.profiles.ProfileHandler.refreshNT(Unknown Source)
                at com.r3000.server.common.profiles.ProfileHandler.refresh(Unknown Source)
                at com.r3000.server.common.profiles.ProfileHandler.<init>(Unknown Source)
                at com.r3000.server.common.profiles.ProfileHandler.refresh(Unknown Source)
                at com.r3000.server.authentication.AuthenticatorFactory.refresh(Unknown Source)
                at com.r3000.server.authentication.AuthenticatorFactory.<init>(Unknown Source)
                at com.r3000.server.authentication.AuthenticatorFactory.refresh(Unknown Source)
                at com.r3000.server.authentication.AuthenticatorFactory.getInstance(Unknown Source)
                at com.r3000.server.authentication.AuthManager.init(Unknown Source)
                at com.r3000.server.authentication.AuthManager.<init>(Unknown Source)
                at com.r3000.server.authentication.tcpService.AuthServer.start(Unknown Source)
                at com.r3000.server.authentication.tcpService.AuthControl.main(Unknown Source)
```

Fig. 2-25 View Log File Result pop-up window

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

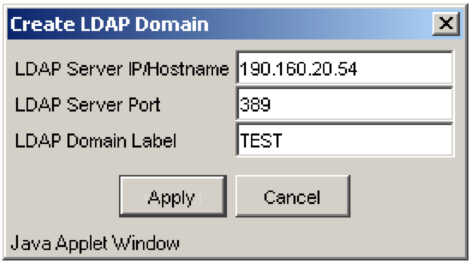
CHAPTER 3: LDAP AUTHENTICATION SETUP

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

1. 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

Fig. 3-1 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.

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.*

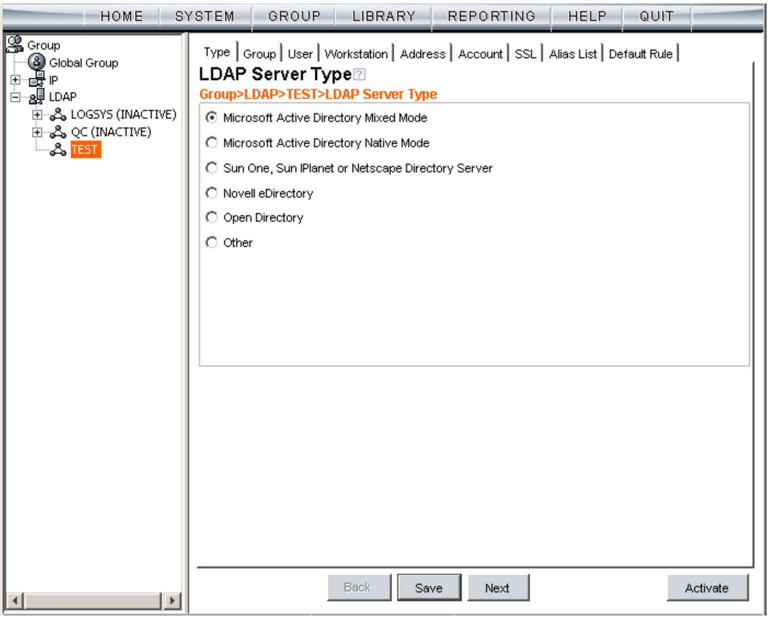
5. Click **Apply** to add the domain to the tree. This action takes you directly to the LDAP domain window (see View, modify, enter LDAP domain details).

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:



LDAP Server Type

Group>LDAP>TEST>LDAP Server Type

● Microsoft Active Directory Mixed Mode

○ Microsoft Active Directory Native Mode

○ Sun One, Sun IPlanet or Netscape Directory Server

○ Novell eDirectory

○ Open Directory

○ Other

Fig. 3-2 Domain Details window, Type tab

The LDAP domain window is comprised of the following wizard tabs: Type, Group, User, Workstation, 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.

1. 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”, “Open Directory”, 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.

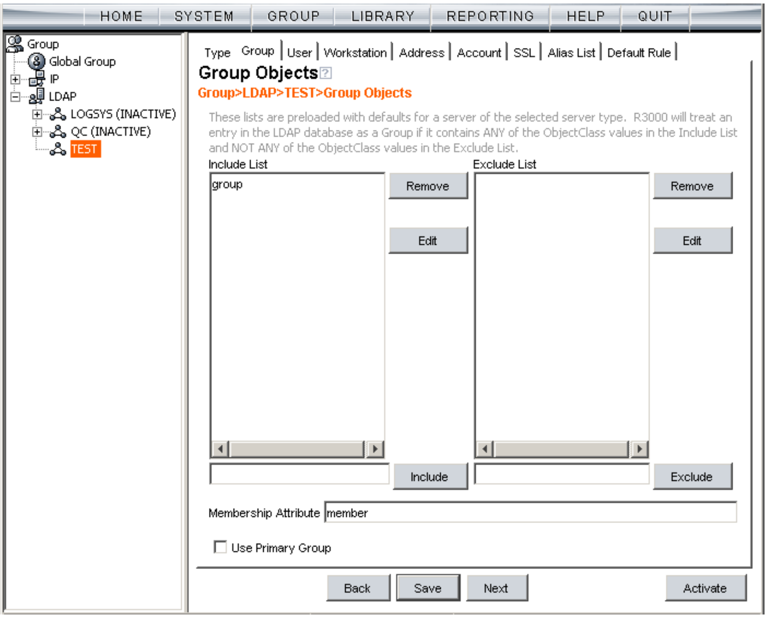
NOTE*: If the server type is changed on this tab, object type settings will be overwritten with the new object type settings. User settings will not be modified.*

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.



Group Objects

Group>LDAP>TEST>Group Objects

These lists are preloaded with defaults for a server of the selected server type. R3000 will treat an entry in the LDAP database as a Group if it contains ANY of the ObjectClass values in the Include List and NOT ANY of the ObjectClass values in the Exclude List.

Include List: group

Exclude List:

Membership Attribute: member

□ Use Primary Group

Fig. 3-3 Domain Details window, Group tab

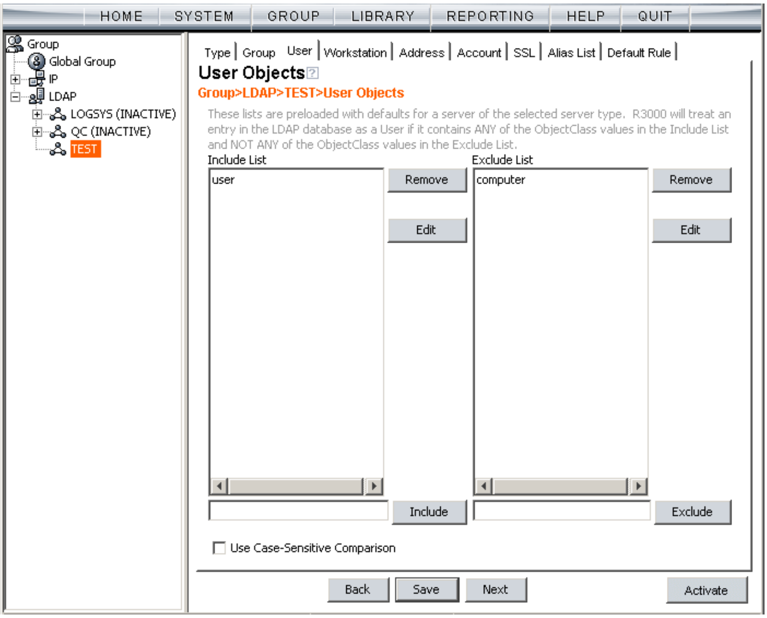
By default, this tab is populated as follows:

- 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.



User Objects

Group>LDAP>TEST>User Objects

These lists are preloaded with defaults for a server of the selected server type. R3000 will treat an entry in the LDAP database as a User if it contains ANY of the ObjectClass values in the Include List and NOT ANY of the ObjectClass values in the Exclude List.

Include List: user

Exclude List: computer

□ Use Case-Sensitive Comparison

Fig. 3-4 Domain Details window, User tab

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

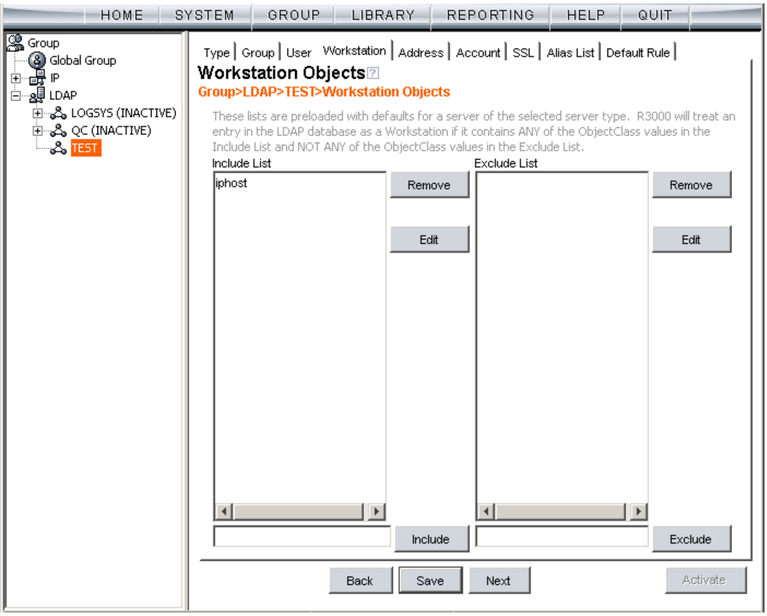
1. Generally, no action needs to be performed on this tab. However, under special circumstances, the following actions can be performed:
   - A user object can be added or excluded by making an entry in the appropriate field, and then clicking the **Include** or **Exclude** button.
   - A user object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

Workstation Objects

The Workstation tab is used for including or excluding workstation objects in the LDAP domain.



Workstation Objects

Group>LDAP>TEST>Workstation Objects

These lists are preloaded with defaults for a server of the selected server type. R3000 will treat an entry in the LDAP database as a Workstation if it contains ANY of the ObjectClass values in the Include List and NOT ANY of the ObjectClass values in the Exclude List.

Include List: iphost

Exclude List:

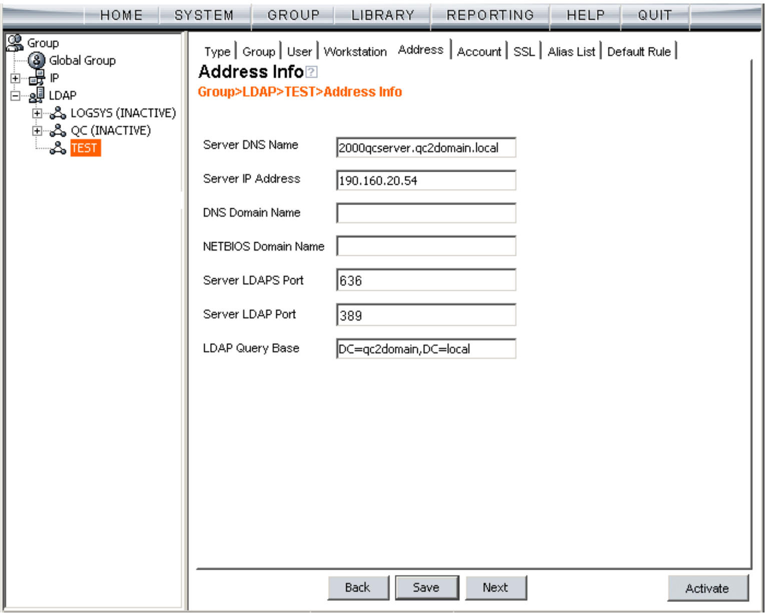
Fig. 3-5 Domain Details window, Workstation tab

By default, the Include List and Exclude List are populated with appropriate workstation 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 workstation object can be added or excluded by making an entry in the appropriate field, and then clicking the **Include** or **Exclude** button.
   - A workstation object name can be edited by selecting the workstation object from the appropriate list box, editing the name in the field, and then clicking the **Edit** button.
   - A workstation object can be removed by selecting the workstation object and then clicking **Remove**.
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:



Address Info

Group>LDAP>TEST>Address Info

Server DNS Name: 2000qcserver.qc2domain.local

Server IP Address: 190.160.20.54

DNS Domain Name:

NETBIOS Domain Name:

Server LDAPS Port: 636

Server LDAP Port: 389

LDAP Query Base: DC=qc2domain,DC=local

Fig. 3-6 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.

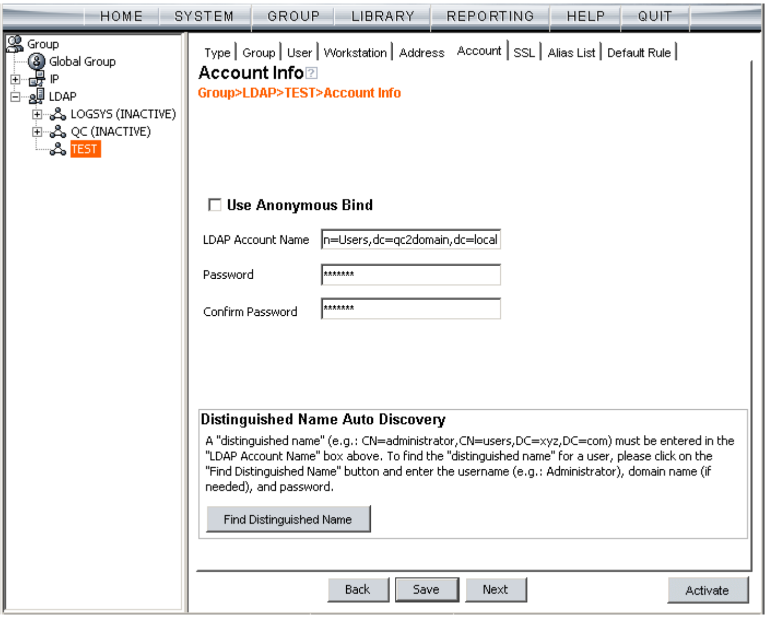
- If necessary, the **NETBIOS Domain Name** can be entered.
- By default, *636* displays in the **Server LDAPS Port** field.
- By default, the value that was entered in the LDAP Server Port field of the Create LDAP Domain dialog box displays in the **Server LDAP Port** field.
- By default, the **LDAP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



Account Info

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 "LDAP Account Name" box above. To find the "distinguished name" for a user, please click on the "Find Distinguished Name" button and enter the username (e.g.: Administrator), domain name (if needed), and password.

Fig. 3-7 Domain Details window, Account tab

***NOTE**: The Distinguished Name Auto Discovery frame only displays if the type of LDAP server is Microsoft Active Directory.*

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, if it displays—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.

- For an Active Directory LDAP server type, 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:

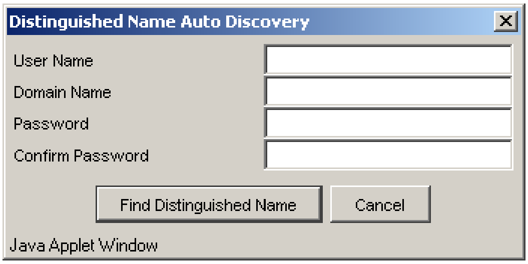


Fig. 3-8 Distinguished Name Auto Discovery box

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**.

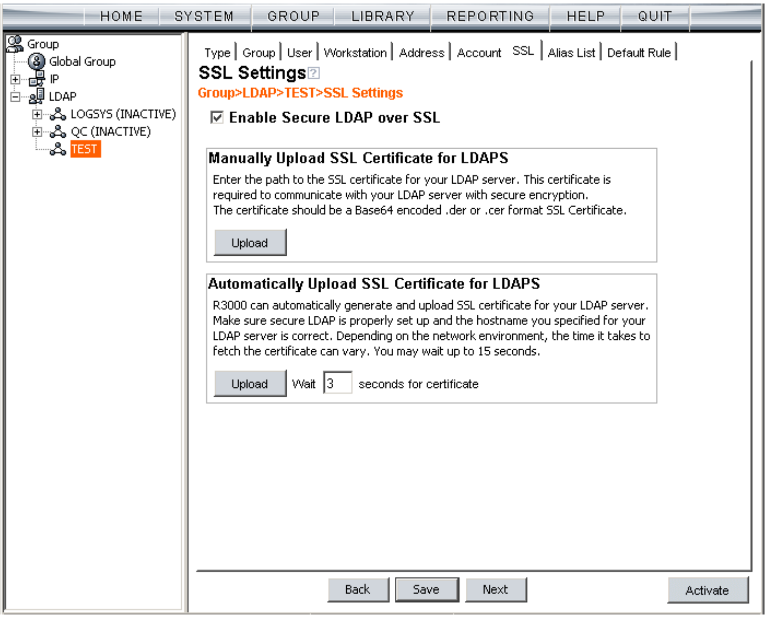
Click **Find Distinguished Name** to perform the search for the LDAP Distinguished Name. If the administrator's user name and password are successfully retrieved, the pop-up box closes and the fields on this tab become populated with appropriate data.

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

2. Click **Save** to save your entries.
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.



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

Fig. 3-9 Domain Details window, SSL tab

***NOTE**: See Appendix B: 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 certficate to your desktop and then upload it to the R3000.*

1. 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:

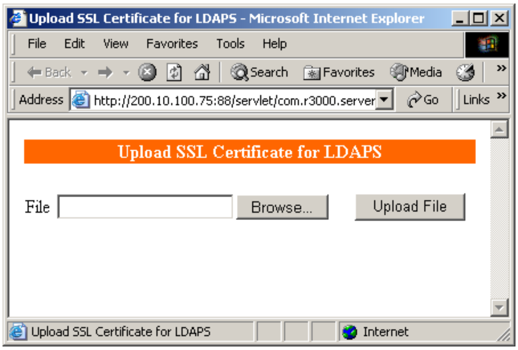

Upload SSL Certificate for LDAPS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.100.75:88/servlet/com.r3000.server Go Links
Upload SSL Certificate for LDAPS
File
Browse...
Upload File
Upload SSL Certificate for LDAPS
Internet

Fig. 3-10 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.

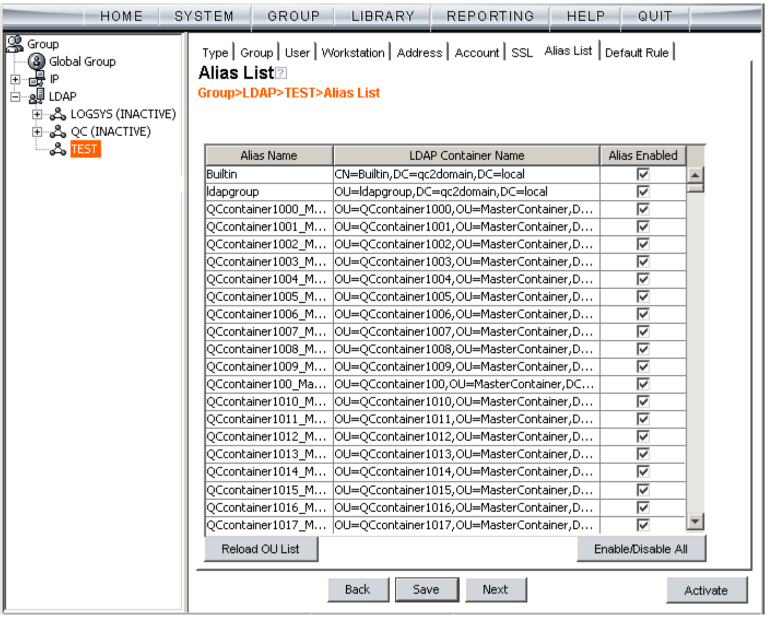
***WARNING**: If using a Novell server, be sure the name on the SSL certificate (to be uploaded to the server) matches the Server DNS Name entered in the Address Info tab.*

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.



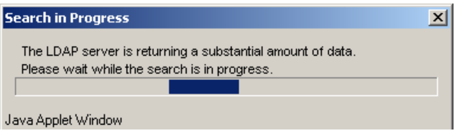
Alias List

Group>LDAP>TEST>Alias List

Alias Name	LDAP Container Name	Alias Enabled
Builtin	CN=Builtin,DC=qc2domain,DC=local	☑
ldapgroup	OU=ldapgroup,DC=qc2domain,DC=local	☑
QCcontainer1000_M...	OU=QCcontainer1000,OU=MasterContainer,D...	☑
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...	☑
QCcontainer1006_M...	OU=QCcontainer1006,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...	☑

Fig. 3-11 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. 3-12 Search in Progress box

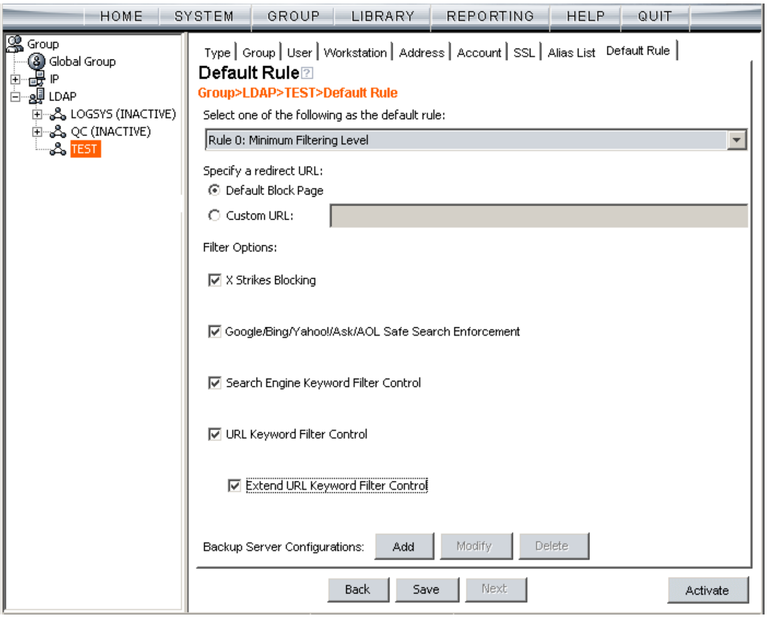
After the search is completed, the Search in Progress box closes, and the list displays the Alias Name and the corresponding LDAP Container Name.

***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.*

1. 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.



Default Rule

Group>LDAP>TEST>Default Rule

Select one of the following as the default rule:

Rule 0: Minimum Filtering Level

Specify a redirect URL:

● Default Block Page

○ Custom URL:

Filter Options:

☑ X Strikes Blocking

☑ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement

☑ Search Engine Keyword Filter Control

☑ URL Keyword Filter Control

☑ Extend URL Keyword Filter Control

Backup Server Configurations:

Fig. 3-13 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/Bing/Yahoo!/Ask/AOL 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.*

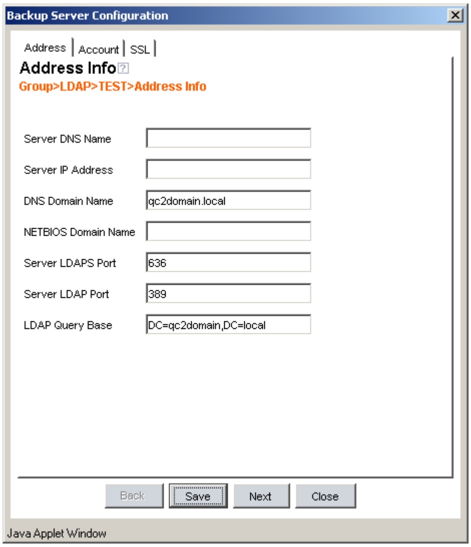
NOTE*: To enter profile information for LDAP groups and users, see Create and Maintain Filtering Profiles in Chapter 4.*

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:


Backup Server Configuration
Address | Account | SSL |
Address Info
Group>LDAP>TEST>Address Info
Back
Save
Next
Close
Java Applet Window

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

Fig. 3-14 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

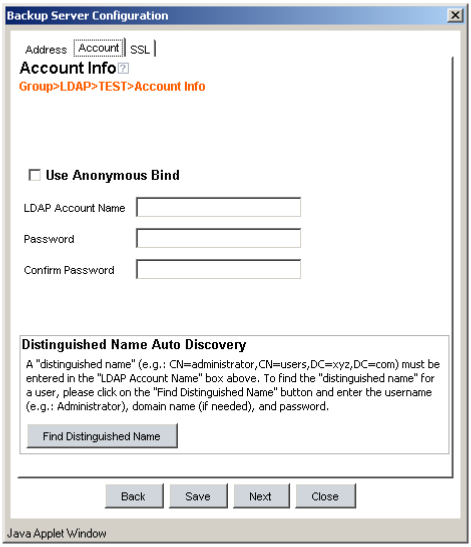
***NOTES**: If your LDAP server's name is not a resolvable, fully qualified DNS name, you may be able to enter the domain name.*

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

Account Info

Group>LDAP>TEST>Account Info

☐ Use Anonymous Bind

LDAP Account Name

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 "LDAP Account Name" box above. To find the "distinguished name" for a user, please click on the "Find Distinguished Name" button and enter the username (e.g.: Administrator), domain name (if needed), and password.

Find Distinguished Name

Java Applet Window

Fig. 3-15 Backup Server Configuration, Account Info

***NOTE**: The Distinguished Name Auto Discovery frame only displays if the type of LDAP server is Microsoft Active Directory.*

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 the LDAP server type is Active Directory, and 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. 3-8).

  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.

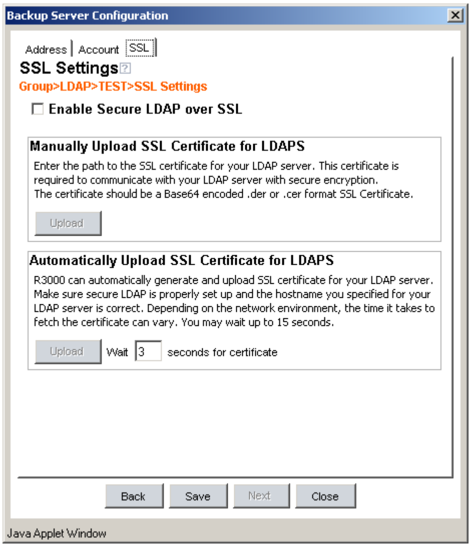
  d. Enter the password in the **Password** and **Confirm Password** fields.

  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.

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

6. Click **Save** to save your entries.

7. Click **Next** to go to the SSL tab:



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.

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.

Wait 3 seconds for certificate

Fig. 3-16 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 B: 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. 3-9).
- 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.

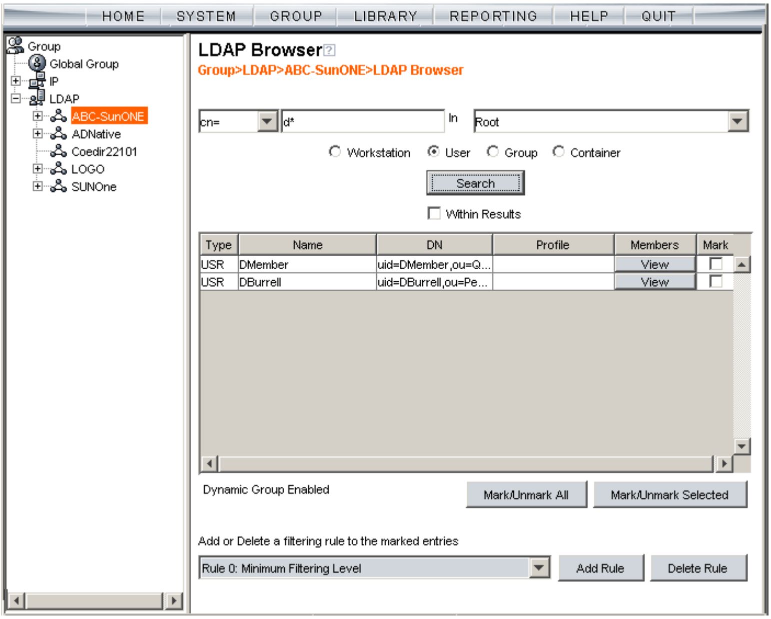
Set up LDAP Domain Nodes

In the navigation panel, the LDAP domain branch of the tree menu includes options for setting up entities (nodes) in the domain so that filtering profiles can later be created. The following options are used in this setup process: Manage Profile Objects, Set Group Priority, Manually Add Workstation, Manually Add Member, Manually Add Group, and Upload Profile.

Add nodes to the domain tree list

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

Select the LDAP domain, and choose Manage Profile Objects from the pop-up menu to display the LDAP Browser window:



LDAP Browser

Group>LDAP>ABC-SunONE>LDAP Browser

cn= | d* | In | Root

○ Workstation ● User ○ Group ○ Container

□ Within Results

Type	Name	DN	Profile	Members	Mark
USR	DMember	uid=DMember,ou=Q...		View	□
USR	DBurrell	uid=DBurrell,ou=Pe...		View	□

Dynamic Group Enabled

Add or Delete a filtering rule to the marked entries

Rule 0: Minimum Filtering Level

Fig. 3-17 LDAP Browser window

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

***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 C: LDAP Server Customizations if using an OpenLDAP server.

Perform a basic search

1. Specify the type of search by clicking the “Workstation”, “User”, “Group”, or “Container” radio button.
2. 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 workstation name, username, group name, 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.
5. Click **Search** to display rows of results in the grid below. The following information is included for each entity: Type (WRK, 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 nodes with rules applied to them appear in the tree.

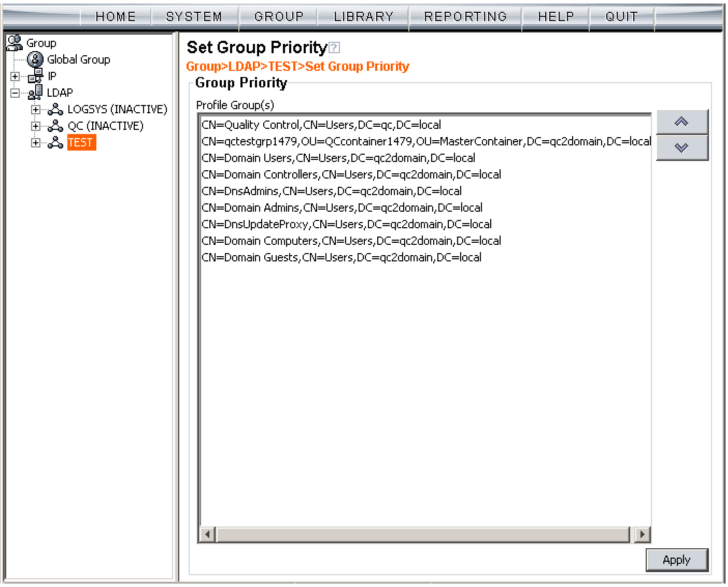
Delete a rule

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:



CN=Quality Control,CN=Users,DC=qc,DC=local
CN=qctestgrp1479,OU=QCcontainer1479,OU=MasterContainer,DC=qc2domain,DC=local
CN=Domain Users,CN=Users,DC=qc2domain,DC=local
CN=Domain Controllers,CN=Users,DC=qc2domain,DC=local
CN=DnsAdmins,CN=Users,DC=qc2domain,DC=local
CN=Domain Admins,CN=Users,DC=qc2domain,DC=local
CN=DnsUpdateProxy,CN=Users,DC=qc2domain,DC=local
CN=Domain Computers,CN=Users,DC=qc2domain,DC=local
CN=Domain Guests,CN=Users,DC=qc2domain,DC=local

Fig. 3-18 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 LDAP Browser 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 workstation name to the tree

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

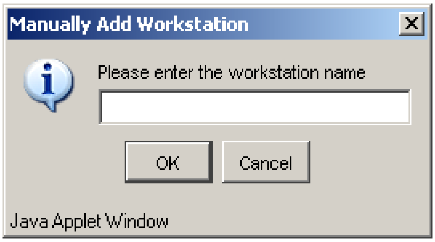


Fig. 3-19 Manually Add Workstation box

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

2. Enter the workstation name in the text box, using the entire Distinguished Name. For example: *cn=engineering, cn=tester, dc=logo, dc=com*

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

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

***NOTE**: See Add or maintain a node's profile under Create and Maintain Filtering Profiles in Chapter 4 for information on defining the filtering profile for the group.*

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:

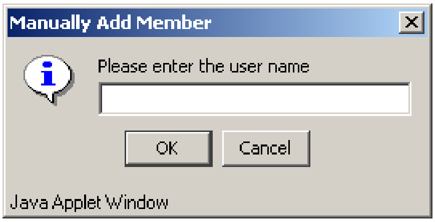


Fig. 3-20 Manually Add Member box

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.*

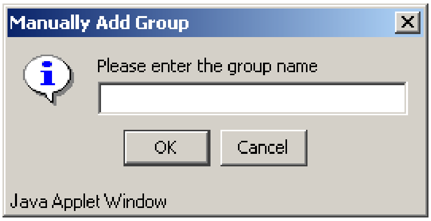
Examples:
CN=Jane Doe, CN=Users, DC=qc, DC=local
CN=Public\, Joe Q., OU=Users, OU=Sales, DC=qc, DC=local
CN=Doe\, John, CN=Users, DC=qc, DC=local
cn=dyn-grp,ou=progrm,o=nwrd-org

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

***NOTE**: See Add or maintain a node's profile under Create and Maintain Filtering Profiles in Chapter 4 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

Fig. 3-21 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.

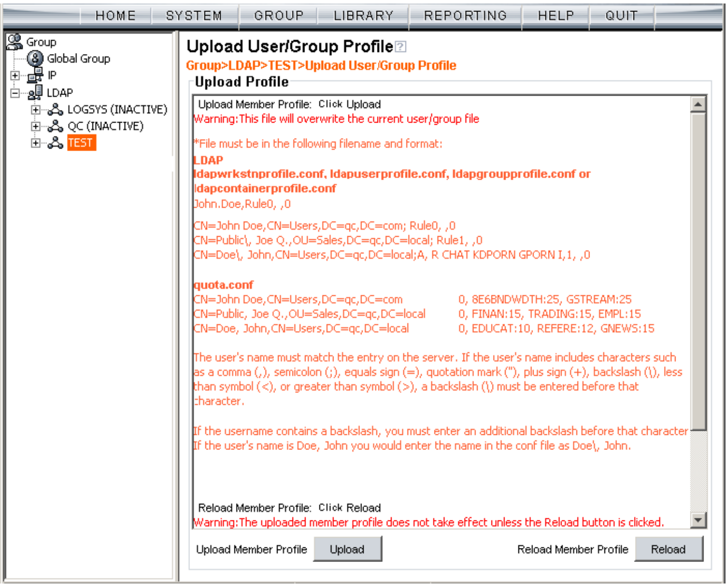
2. Enter the group's name in the text box, using the entire Distinguished Name format.

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

NOTE*: See Add or maintain a node's profile under Create and Maintain Filtering Profiles in Chapter 4 for information on defining the filtering profile for the group.*

Upload a file of filtering profiles to the tree

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



Upload User/Group Profile

Group>LDAP>TEST>Upload User/Group Profile

Upload Profile

Upload Member Profile: Click Upload

Warning:This file will overwrite the current user/group file

*File must be in the following filename and format:

LDAP

ldapwrkstnprofile.conf, ldapuserprofile.conf, ldapgroupprofile.conf or ldapcontainerprofile.conf

```
John.Doe,Rule0, ,0

CN=John Doe,CN=Users,DC=qc,DC=com; Rule0, ,0
CN=Public\, Joe Q.,OU=Sales,DC=qc,DC=local; Rule1, ,0
CN=Doe\, John,CN=Users,DC=qc,DC=local;A, R CHAT KDPORN GPORN I,1, ,0
```

quota.conf

```
CN=John Doe,CN=Users,DC=qc,DC=com           0, 8E6BNDWDTH:25, GSTREAM:25
CN=Public, Joe Q.,OU=Sales,DC=qc,DC=local   0, FINAN:15, TRADING:15, EMPL:15
CN=Doe, John,CN=Users,DC=qc,DC=local        0, EDUCAT:10, REFERE:12, GNEWS:15
```

The user's name must match the entry on the server. If the user's name includes characters such as a comma (,), semicolon (;), equals sign (=), quotation mark ("), plus sign (+), backslash (\), less than symbol (<), or greater than symbol (>), a backslash (\) must be entered before that character.

If the username contains a backslash, you must enter an additional backslash before that character
If the user's name is Doe, John you would enter the name in the conf file as Doe\, John.

Reload Member Profile: Click Reload

Warning:The uploaded member profile does not take effect unless the Reload button is clicked.

Fig. 3-22 Upload User/Group Profile window

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

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

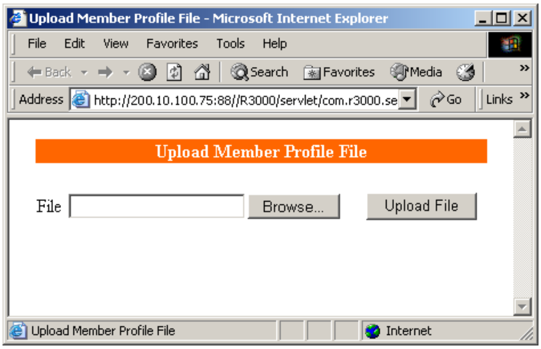

Upload Member Profile File - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.100.75:88//R3000/servlet/com.r3000.se
Go Links
Upload Member Profile File
File
Browse...
Upload File
Upload Member Profile File
Internet

Fig. 3-23 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 profile file.*

Each 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 workstation, user or group profiles, or quota profiles. Based on the type of file format used, the file should have the following name:

- **ldapwrkstnprofile.conf** - if the file contains LDAP workstation profiles
- **ldapuserprofile.conf** - if the file contains LDAP user profiles
- **ldapgroupprofile.conf** - if the file contains LDAP group profiles
- **ldapcontainerprofile.conf -** if the file contains LDAP container profiles

- **quota.conf** - if the file contains LDAP workstation, user, group, or container profiles with quotas included. A quota in a profile indicates the user can spend a specified amount of time at a designated passed library category before he/she is blocked from further accessing URLs in that category.

***NOTE**: See Appendix D: Profile 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.

CHAPTER 4: MANAGE NODES

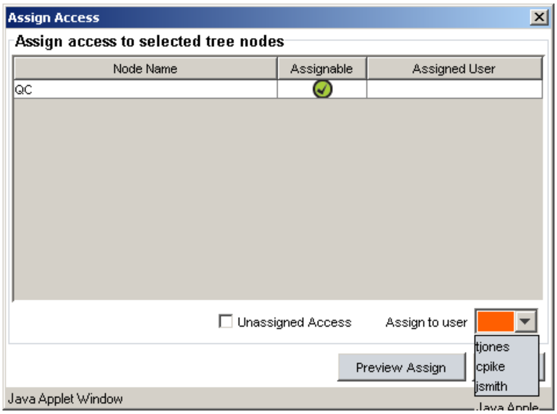
Once LDAP domains are set up in the Group tree, the global administrator assigns Sub Admin group administrators the following entities (nodes) to manage: domain, group(s), workstations, members, and/or containers.

***NOTE**: See Set up Group Administrator Accounts in Chapter 2: Network Setup for information on creating and managing Sub Admin group administrator accounts.*

Assign Sub Admin to an LDAP Node

A group administrator assigned to an LDAP node (domain, group, workstation, member, or container) has the privileges to add, edit, or delete entities to/from that node to which he/ she is assigned. This Sub Admin group administrator is also responsible for creating and maintaining filtering profiles for entities in his/her assignment.

1. Click Assign to at any level of the LDAP Group tree (domain, group, workstation, member, or container) to open the Assign Access pop-up window (see Fig. 4-1). In the Assign Access to selected tree nodes frame, the name of the entity (Node Name) displays, along with that node’s Assignable status. If the node has already been assigned to a group manager, the username for the Assigned User displays.
2. From the **Assign to user** field, choose from the list of available Sub Admins:



Assign Access

Assign access to selected tree nodes

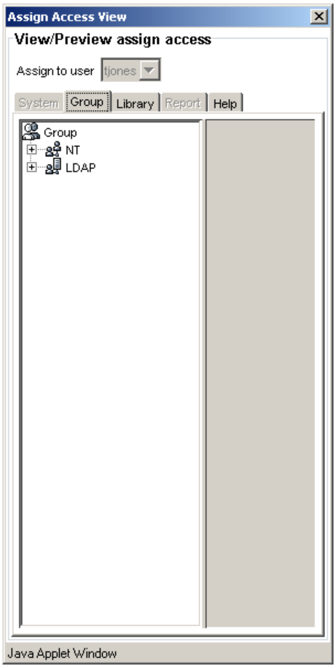
Node Name	Assignable	Assigned User
QC	✓	

□ Unassigned Access

Assign to user

Fig. 4-1 Assign Access window

3. To preview the access view for the proposed Sub Admin, click **Preview Assign** to open the Assign Access View pop-up window:



Assign Access View

View/Preview assign access

Assign to user: tjones

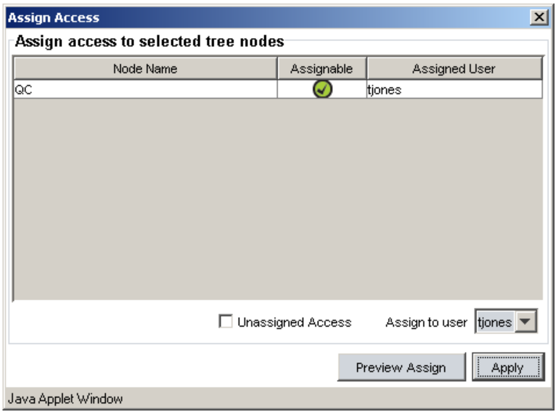
Fig. 4-2 Assign Access View window

4. Click the Group, Library, and Help tabs to view the menu topics, sub-topics, and tree nodes currently available to that Sub Admin.

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

***TIP**: If necessary, another Sub Admin from the Assign to user field can be assigned to that node.*

6. Click **Apply** to assign the Sub Admin to that node and to enter that Sub Admin’s username in the Assigned User column in the list box:



Assign Access

Assign access to selected tree nodes

Node Name	Assignable	Assigned User
QC	✓	tjones

□ Unassigned Access   Assign to user: tjones

Fig. 4-3 Assign Access window with node assigned

7. Click the “X” in the upper right corner of the Assign Access pop-up window to close it.

***TIP**: To unassign the Sub Admin from that node, click the **Unassigned Access** checkbox and then click **Apply**. To re-assign the node to another Sub Admin, click the **Unassigned Access** checkbox again to remove the check mark from the checkbox. A different Sub Admin can now be selected from the **Assign to user** pull-down menu.*

Create and Maintain Filtering Profiles

If a Sub Admin group administrator is assigned to an LDAP domain, he/she can add groups and members to that domain. A Sub Admin group administrator assigned to an LDAP group can add members and filtering profiles for all nodes he/she oversees.

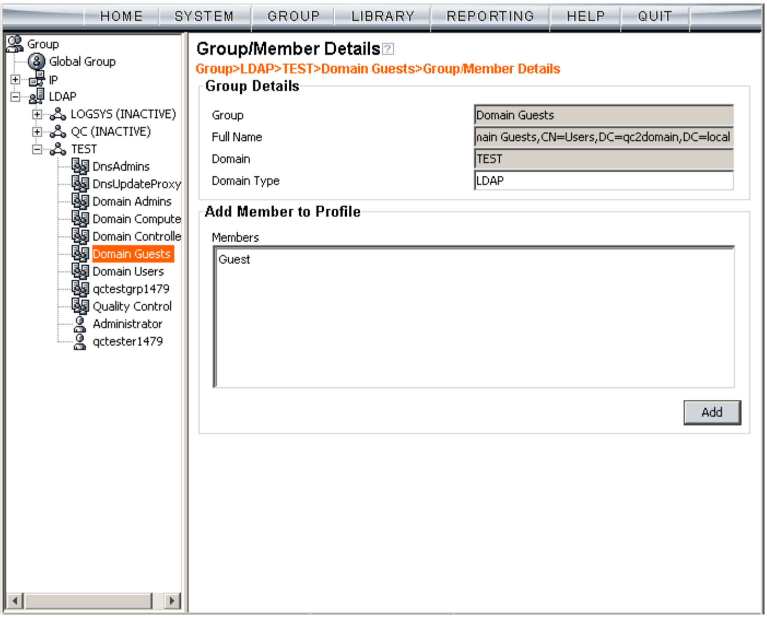
For LDAP groups, the following options are available for filtering profile creation and maintenance: Group Member Details, Profile, Exception URL, Time Profile, Remove, and Assign to. For LDAP workstations, members, and containers, the following options are available for filtering profile creation and maintenance: Profile, Exception URL, Time Profile, Remove, and Assign to.

***TIPS**: See Assign Sub Admin to an LDAP Node for information on changing the assignment of an LDAP node to another Sub Admin.*

See Set up LDAP Domain Nodes for information on setting up groups in an LDAP domain.

Add a group member to the tree list

From the domain, select the group and choose Group Member Details from the pop-up menu to display the Group/ Member Details window:



Group/Member Details

Group>LDAP>TEST>Domain Guests>Group/Member Details

Group Details

Group: Domain Guests
Full Name: nain Guests,CN=Users,DC=qc2domain,DC=local
Domain: TEST
Domain Type: LDAP

Add Member to Profile

Members: Guest

Fig. 4-4 Group Member Details window, LDAP group

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

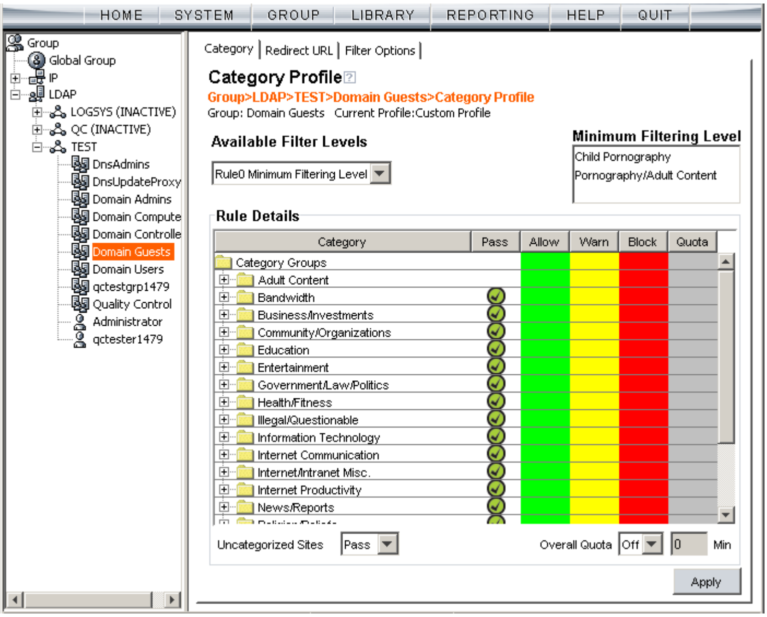
In the Group Details frame, the following details display: **Group** name, **Full Name** (Distinguished Name) of the group, **Domain** name, and **Domain Type**. Members that belong to the group display in the Members list box in the Add Member to Profile frame.

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 a node's profile

From the domain, select the node and choose Profile from the pop-up menu to display the default Category tab of the Profile window:



Category Profile

Group>LDAP>TEST>Domain Guests>Category Profile

Group: Domain Guests   Current Profile:Custom Profile

Available Filter Levels

Rule0 Minimum Filtering Level

Minimum Filtering Level

Child Pornography
Pornography/Adult Content

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups		🟩	🟨	🟥	
Adult Content		🟩	🟨	🟥	
Bandwidth	✓	🟩	🟨	🟥	
Business/Investments	✓	🟩	🟨	🟥	
Community/Organizations	✓	🟩	🟨	🟥	
Education	✓	🟩	🟨	🟥	
Entertainment	✓	🟩	🟨	🟥	
Government/Law/Politics	✓	🟩	🟨	🟥	
Health/Fitness	✓	🟩	🟨	🟥	
Illegal/Questionable	✓	🟩	🟨	🟥	
Information Technology	✓	🟩	🟨	🟥	
Internet Communication	✓	🟩	🟨	🟥	
Internet/Intranet Misc.	✓	🟩	🟨	🟥	
Internet Productivity	✓	🟩	🟨	🟥	
News/Reports	✓	🟩	🟨	🟥	

Uncategorized Sites: Pass

Overall Quota: Off   0 Min

Fig. 4-5 Group Profile window, Category tab, LDAP group

The Profile option is used for viewing/creating the filtering profile of the defined node (LDAP static or dynamic group, workstation, 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. 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 five rule choices: Rule1 BYPASS”, “Rule2 BLOCK Porn”, “Rule3 Block IM and Porn”, “Rule4 8e6 CIPA Compliance”, and “Block All”.*

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

1. 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.

3. Make a selection from the **Uncategorized Sites** pull-down menu to specify how to handle a URL that has not yet been categorized: “Pass”, “Warn”, or “Block”.
4. To use the quota feature to restrict the end user’s access to a passed library group/category, do the following:

- In the **Quota** column, enter the number of minutes the user will be able to access the library group/category. The minimum number of minutes is “1” and the maximum is “1439” (one day minus one minute). The number of minutes entered here combines with the seconds per hit (minimum one second to maximum 3600 seconds) defined in the Quota Settings window to determine when the end user will be blocked from further access to URLs in that library group/category.

TIP*: If a quota entry is made for a category group, all library categories in that group will show the same number of quota minutes.*

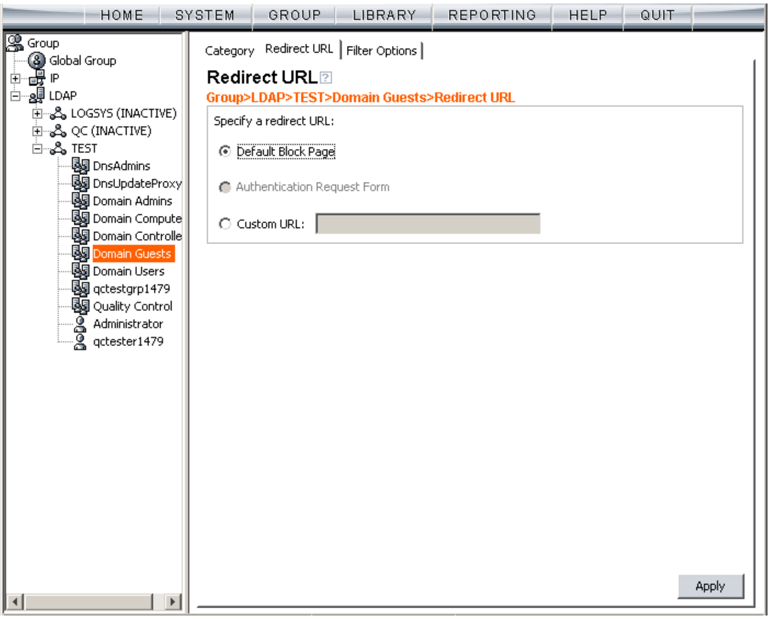
NOTE*: See the Quota Settings window in Chapter 1: System screen of the R3000 User Guide for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.*

- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned “Off”. If turned “On”, enter the number of minutes in the **Min** field to indicate when the end user’s access to passed library groups/ categories with quotas will be blocked. If the end user spends this amount of time at URLs in any quota-marked library group/category, the Overall Quota overrides the number of minutes defined for each individual quota.

5. 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:



Redirect URL

Group>LDAP>TEST>Domain Guests>Redirect URL

Specify a redirect URL:

● Default Block Page

○ Authentication Request Form

○ Custom URL:

Fig. 4-6 Group Profile window, Redirect URL tab, LDAP group

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.

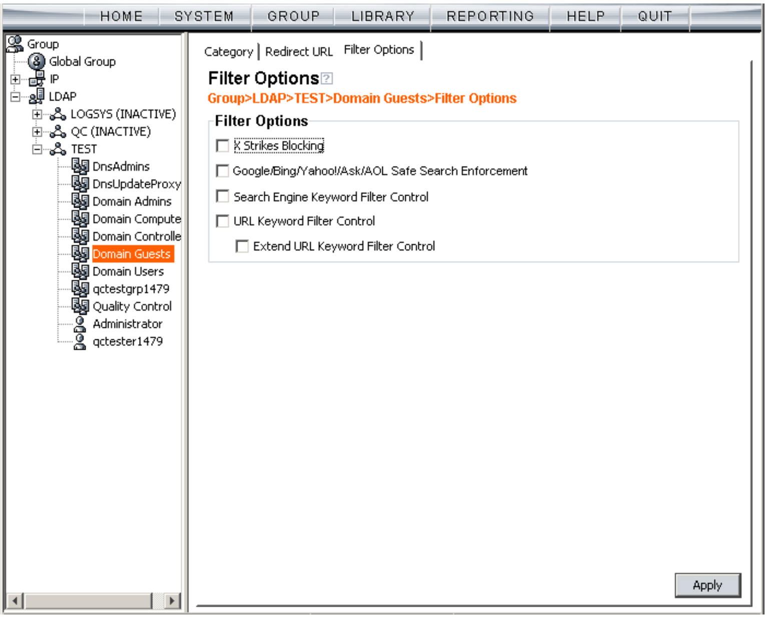
1. Specify the type of redirect URL to be used: "Default Block Page", or "Custom URL".

   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:



Filter Options

Group>LDAP>TEST>Domain Guests>Filter Options

Filter Options

□ X Strikes Blocking

□ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement

□ Search Engine Keyword Filter Control

□ URL Keyword Filter Control

□ Extend URL Keyword Filter Control

Fig. 4-7 Group Profile window, Filter Options tab, LDAP group

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

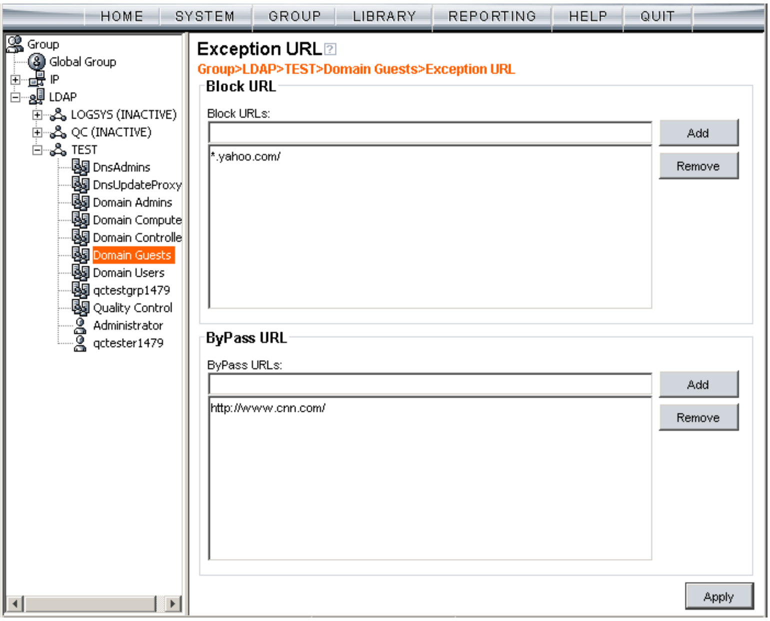
1. Click the checkbox(es) corresponding to the option(s) to be applied to the filtering profile: "X Strikes Blocking", "Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".

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

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

Add an Exception URL to the profile

From the domain, select the node and choose Exception URL from the pop-up menu to display the Exception URL window:



Exception URL

Group>LDAP>TEST>Domain Guests>Exception URL

Block URL

Block URLs:

*.yahoo.com/

ByPass URL

ByPass URLs:

http://www.cnn.com/

Fig. 4-8 Exception URL window, LDAP group

This window is used for blocking group members' access to specified URLs and/or for letting group members access specified URLs blocked at the minimum filtering level.

***NOTE**: Settings in this window work in conjunction with those made in the Minimum Filtering Level window maintained by the global administrator. See the R3000 User Guide for information on configuring and using the minimum filtering level.*

URL entries

The following types of URL entries are accepted in this window:

- formats such as: **http://www.coors.com**, **www.coors.com**, or **coors.com**
- IP address - e.g. "209.247.228.221" in http://209.247.228.221
- octal format - e.g. http://0106.0125.0226.0322
- hexadecimal short format - e.g. http://0x465596d2
- hexadecimal long format - e.g. http://0x46.0x55.0x96.0xd2
- decimal value format - e.g. http://1180014290
- escaped hexadecimal format - e.g. http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D
- query string - e.g. http://www.youtube.com/watch?v=3_Wfnj1lIMU

NOTE*: The pound sign (#) character is not allowed in this entry.*

- wildcard entry format that uses an asterisk (*) followed by a period (.) and then the URL, such as: ***.coors.com**

TIP*: The minimum number of levels that can be entered for a wildcard entry is three (e.g. *.yahoo.com) and the maximum number of levels is six (e.g. *.mail.attachments.message.yahoo .com).*

Block URL frame

To block the entity’s access to a URL:

1. In the **Block URL** field, enter the URL.
2. Click **Add** to include the URL in the Block URLs list box.

To allow the URL to be accessed by the entity again:

1. Select the URL from the Block URLs list box.
2. Click **Remove**.

ByPass URL frame

To allow a URL that is blocked at the minimum filtering level to be accessed by the entity:

1. In the **ByPass URL** field, enter the URL.
2. Click **Add** to include the URL in the ByPass URLs list box.

To block the entity’s access to the URL again:

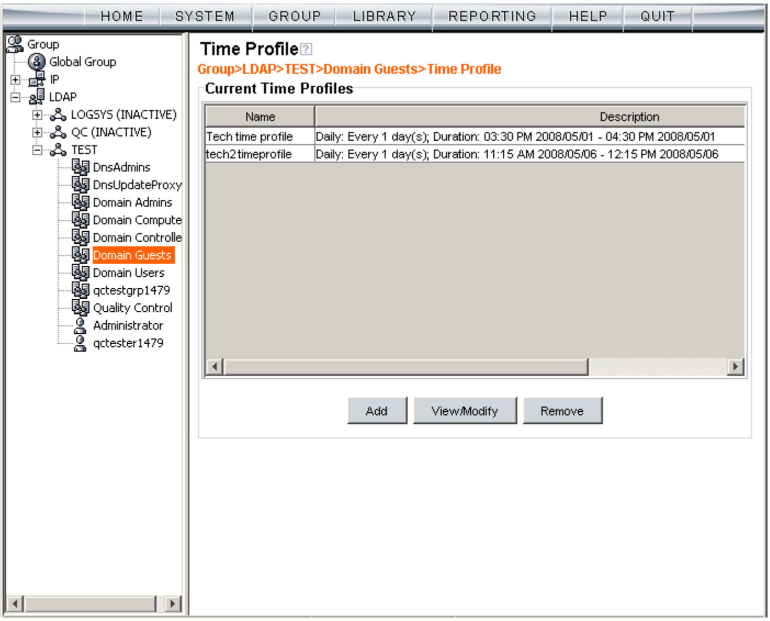
1. Select the URL from the ByPass URLs list box.
2. Click **Remove**.

Apply settings

Click **Apply** to apply your settings after adding or removing a URL.

Create a Time Profile for the node

From the domain, select the node and choose Time Profile from the pop-up menu to display the Time Profile window:



Time Profile

Group>LDAP>TEST>Domain Guests>Time Profile

Current Time Profiles

Name	Description
Tech time profile	Daily: Every 1 day(s); Duration: 03:30 PM 2008/05/01 - 04:30 PM 2008/05/01
tech2timeprofile	Daily: Every 1 day(s); Duration: 11:15 AM 2008/05/06 - 12:15 PM 2008/05/06

Fig. 4-9 Time Profile window, LDAP group

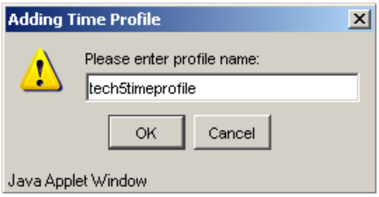
This window is used for setting up or modifying a filtering profile to be activated at a specified time.

The Current Time Profiles list box displays the Name and Description of any time profiles previously set up for the entity that are currently active.

Add a Time Profile

To create a time profile:

1. Click **Add** to open the Adding Time Profile pop-up box:



Adding Time Profile

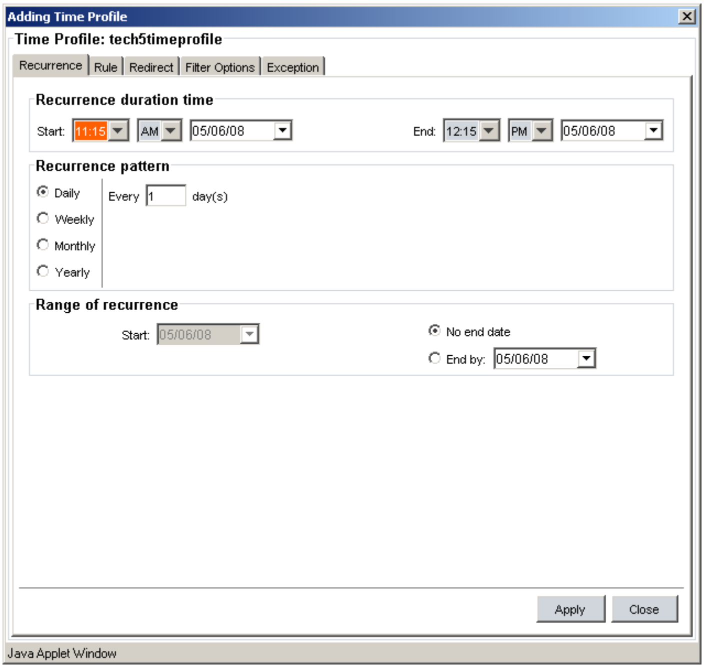
Please enter profile name:

tech5timeprofile

Fig. 4-10 Adding Time Profile

2. Type in three to 20 alphanumeric characters—the underscore (_) character can be used—for the profile name.

3. Click **OK** to close the pop-up box and to open the Adding Time Profile pop-up window that displays the name of this profile at the top of the Time Profile frame:



Adding Time Profile

Time Profile: tech5timeprofile

Recurrence duration time

Start: 11:15 AM 05/06/08 End: 12:15 PM 05/06/08

Recurrence pattern

● Daily ○ Weekly ○ Monthly ○ Yearly

Every 1 day(s)

Range of recurrence

Start: 05/06/08

● No end date

○ End by: 05/06/08

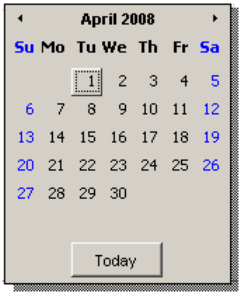
Fig. 4-11 Time Profile window Recurrence tab

4. In the Recurrence duration time frame, specify **Start** and **End** time range criteria:

a. Select from a list of time slots incremented by 15 minutes: “12:00” to “11:45”. By default, the Start field displays the closest 15-minute future time, and the End field displays a time that is one hour ahead of that time. For example, if the time is currently 11:12, “*11:15*” displays in the Start field, and “*12:15*” displays in the End field.

b. Indicate whether this time slot is “AM” or “PM”.

c. Today’s date displays using the MM/DD/YY format. To choose another date, click the arrow in the date drop-down menu to open the calendar pop-up box:



◂ April 2008 ▸

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

In this pop-up box you can do the following:

- Click the left or right arrow at the top of this box to navigate to the prior month or the next month.
- Double-click a date to select it and to close this box, populating the date field with that date.
- Click **Today** to close this box, populating the date field with today’s date.

5. In the Recurrence pattern frame, choose the frequency this time profile will be used:

- **Daily** - If this selection is made, enter the interval for the number of days this time profile will be used. By default, “*1*” displays, indicating this profile will be used each day during the specified time period.

If ***5*** is entered, this profile will be used every five days at the specified time.

- **Weekly** - If this selection is made, enter the interval for the weeks this time profile will be used, and specify the day(s) of the week (“Sunday” - “Saturday”). By default, “*1*” displays and today’s day of the week is selected. If today is Tuesday, these settings indicate this profile will be used each Tuesday during the specified time period.

  If ***2*** is entered and “Wednesday” and “Friday” are selected, this profile will be used every two weeks on Wednesday and Friday.

- **Monthly** - If this selection is made, first enter the interval for the months this time profile will be used, and next specify which day of the month:

  - If **Day** is chosen, select from “1” - “31”.
  - If a non-specific day is chosen, make selections from the two pull-down menus for the following:

    - week of the month: “First” - “Fourth”, or “Last”

    - day of the month: “Sunday” - “Saturday”, “Day”, “Weekday”, “Weekend”.

  “By default, “*1*” displays and today’s Day of the month is selected. If today is the 6th, these settings indicate this profile will be used on the 6th each month during the specified time period.

  If ***3*** is entered and the “Third” “Weekday” are selected, this profile will be used every three months on the third week day of the month. If the month begins on a Thursday (for example, May 1st), the third week day would be the following Monday (May 5th in this example).

- **Yearly** - If this selection is made, the year(s), month, and day for this time profile’s interval must be specified:

First enter the year(s) for the interval. By default "*1*" displays, indicating this time profile will be used each year.

Next, choose from one of two options to specify the day of the month for the interval:

- The first option lets you choose a specific month ("January" - "December") and day ("1" - "31"). By default the current month and day are selected.
- The second option lets you make selections from the three pull-down menus for the following:

  - week of the month: "First" - "Fourth", or "Last"

  - day of the month: "Sunday" - "Saturday", "Day", "Weekday", "Weekend"

  - month: "January" - "December".

  By default, the "First" "Sunday" of "January" are selected.

If ***2*** is entered and the "First" "Monday" of "June" are selected, this profile will be used every two years on the first Monday in June. For example, if the current month and year are May 2008, the first Monday in June this year would be the 2nd. The next time this profile would be used will be in June 2010.

6. In the Range of recurrence frame, the **Start** date displays greyed-out; this is the same date as the Start date shown in the Recurrence duration time frame. Specify whether or not the time profile will be effective up to a given date:

   - **No end date** - If this selection is made, the time profile will be effective indefinitely.

7. Click each of the tabs (Rule, Redirect, Filter Options, Exception) and specify criteria to complete the time profile. (See Category Profile, Redirect URL, Filter Options, and Exception URL in this sub-section for information on the Rule, Redirect, Filter Options, and Exception tabs.)

8. Click **Apply** to activate the time profile for the IP group at the specified time.

9. Click **Close** to close the Adding Time Profile pop-up window and to return to the Time Profile window. In this window, the Current Time Profiles list box now shows the Name and Description of the time profile that was just added.

⚠ ***WARNING**: If there is an error in a time profile, the Description for that time profile displays in red text. Select that time profile and click **View/Modify** to make any necessary corrections.*

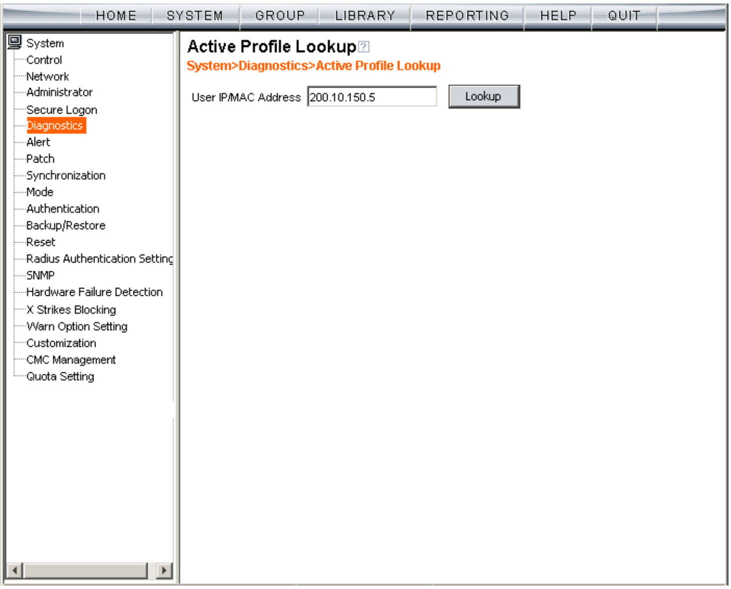
Remove a node’s profile from the tree

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

Verify that an LDAP Profile is Active

The Active Profile Lookup window is a useful tool for the global administrator to use to find out whether or not an LDAP profile is active.

1. In the System section of the user interface, select Diagnostics > Active Profile Lookup to display the Active Profile Lookup window:



Active Profile Lookup

System>Diagnostics>Active Profile Lookup

User IP/MAC Address 200.10.150.5

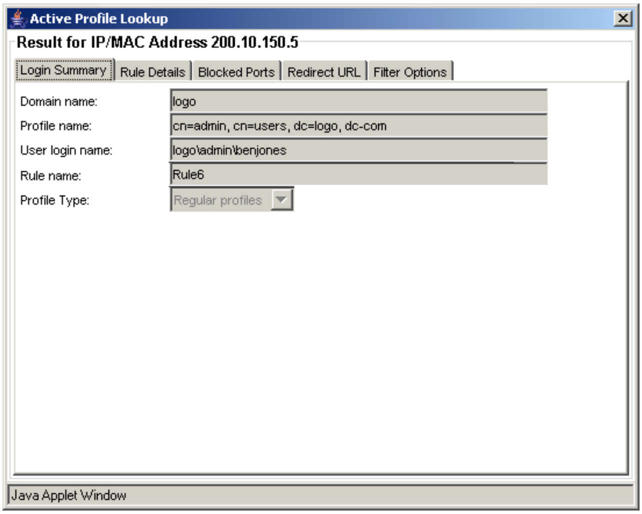
Fig. 4-12 Active Profile Lookup window

***NOTE**: Only filtering profile lookups for LDAP nodes will be addressed in this sub-section. Please refer to the R3000 User Guide for information about other looking up other types of filtering profiles. In order to use this diagnostic tool, LDAP domains and nodes must be set up in the Group section of the R3000, and each node must have a filtering profile.*

2. In the **User IP/MAC Address** field, enter the IP address or MAC address of the end user.

3. Click **Lookup** to verify whether or not an LDAP profile is active for that IP/MAC address.

   If an LDAP filtering profile is active, a pop-up box opens containing the Result frame that displays profile settings applied to the profile:



Result for IP/MAC Address 200.10.150.5

Domain name: logo
Profile name: cn=admin, cn=users, dc=logo, dc-com
User login name: logo\admin\benjones
Rule name: Rule6
Profile Type: Regular profiles

Fig. 4-13 Active Profile Lookup results

The default Login Summary tab displays the following information:

- **Domain name** - LDAP domain name.
- **Profile name** - Distinguished Name for the LDAP profile.
- **User login name** - path of the LDAP profile on the domain. For a workstation profile, this path includes the workstation name.
- **Rule name** - if this profile uses a non-custom rule, the rule number displays.
- **Profile Type** - “Regular profiles” displays greyed-out.

4. Click the following tabs to view information in that tab: Rule Details, Blocked Ports, Redirect URL, Filter Options.

   - **Rule Details** - In the Rule Details frame, the Category Groups tree displays group and library categories with filter settings that determine whether or not the end user can access URLs set up for that category group/ library category.

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.*

A check mark inside a green circle displays in the Pass, Allow, Warn, Block column for the filter setting assigned to the category group/library category for the end user. These filter settings indicate the following:

- 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.
- Quota - If a number displays in this column, the corresponding category group/library category was set up as passed but with a time limit, as defined by the number of minutes in that column. After spending 75 percent of the allotted time visiting URLs in that group/category, the user receives a quota warning message; after spending100 percent of the allotted time visiting URLs in that group/category, he/she receives a quota block page.

***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 filter 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.*

At the bottom of the Rule Details frame, Uncategorized Sites are set to “Pass”, “Warn”, or “Block”, indicating that the selected setting applies to any non-classified URL. If the Overall Quota field is enabled, the user is restricted to the number of minutes shown here for visiting URLs in all groups/categories collectively in which a quota is specified.

- **Blocked Ports** (optional) - ports that have been set up to be blocked, if established.
- **Redirect URL** (optional) - the URL that will be used for redirecting the user away from a page that is blocked, if established.
- **Filter Options** (optional) - filter options to be used in the user’s profile: “X Strikes Blocking”, “Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement”, “Search Engine Keyword Filter Control”, and/or “URL Keyword Filter Control” with/without the “Extend URL Keyword Filter Control” option selected.

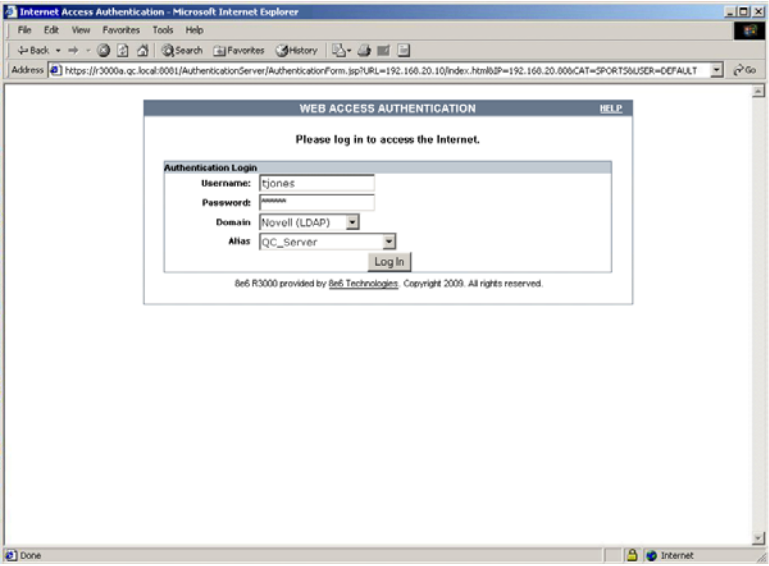
5. Click the “X” in the upper right corner of the pop-up box to close it.

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.



https://r3000a.qc.local:8081/AuthenticationServer/AuthenticationForm.jsp?URL=192.168.20.10/index.html&IP=192.168.20.80&CAT=SPORTS&USER=DEFAULT

WEB ACCESS AUTHENTICATION

Please log in to access the Internet.

Authentication Login

Username: tjones

Password: ******

Domain: Novell (LDAP)

Alias: QC_Server

8e6 R3000 provided by 8e6 Technologies. Copyright 2009. All rights reserved.

Fig. 5-1 Authentication Request Form

***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.

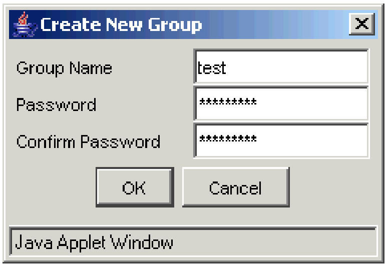
If you (the administrator) can be successfully authenticated in the domains that were set up, the test process is complete, and you are ready to activate authentication on the network (see Activate Authentication on the Network).

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:



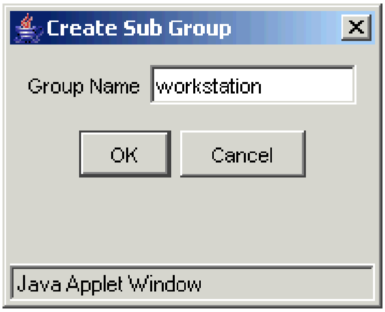
Group Name test
Password *********
Confirm Password *********

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

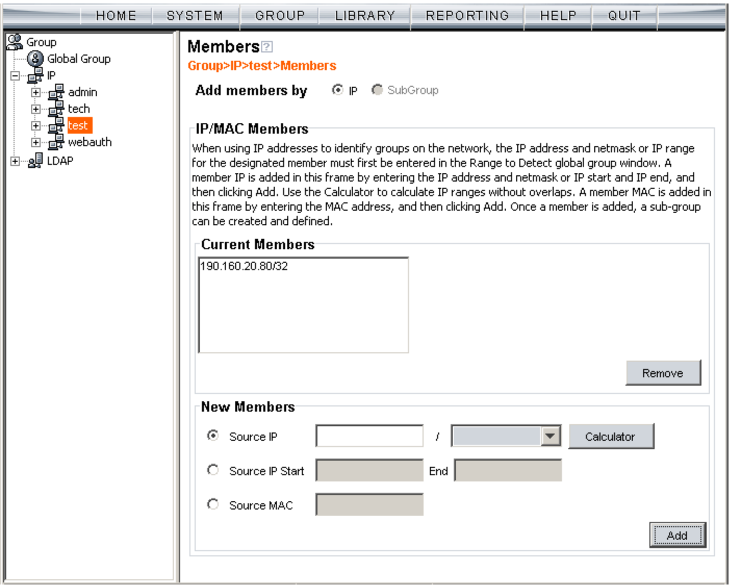
Group Name: workstation

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:



Members

Group>IP>test>Members

Add members by ● IP ○ SubGroup

IP/MAC Members

When using IP addresses to identify groups on the network, the IP address and netmask or IP range for the designated member must first be entered in the Range to Detect global group window. A member IP is added in this frame by entering the IP address and netmask or IP start and IP end, and then clicking Add. Use the Calculator to calculate IP ranges without overlaps. A member MAC is added in this frame by entering the MAC address, and then clicking Add. Once a member is added, a sub-group can be created and defined.

Current Members

190.160.20.80/32

New Members

● Source IP /

○ Source IP Start End

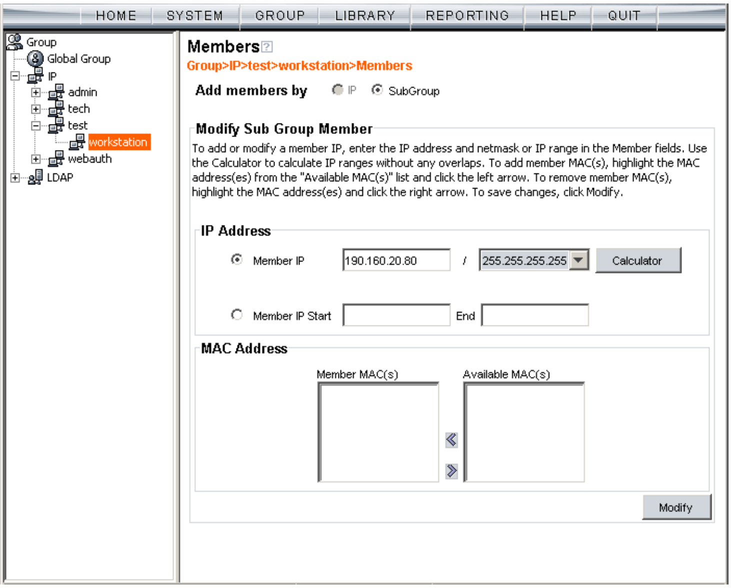
○ Source MAC

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:



Members

Group>IP>test>workstation>Members

Add members by ○ IP ● SubGroup

Modify Sub Group Member

To add or modify a member IP, enter the IP address and netmask or IP range in the Member fields. Use the Calculator to calculate IP ranges without any overlaps. To add member MAC(s), highlight the MAC address(es) from the "Available MAC(s)" list and click the left arrow. To remove member MAC(s), highlight the MAC address(es) and click the right arrow. To save changes, click Modify.

IP Address

● Member IP 190.160.20.80 / 255.255.255.255 Calculator

○ Member IP Start ____ End ____

MAC Address

Member MAC(s) Available MAC(s)

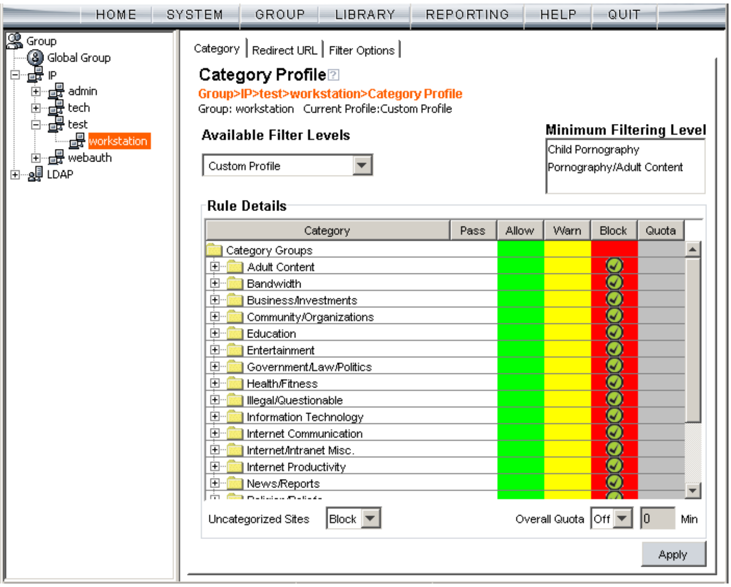
Modify

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:



Category Profile

Group>IP>test>workstation>Category Profile

Group: workstation Current Profile:Custom Profile

Available Filter Levels: Custom Profile

Minimum Filtering Level: Child Pornography, Pornography/Adult Content

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content				✓	
Bandwidth				✓	
Business/Investments				✓	
Community/Organizations				✓	
Education				✓	
Entertainment				✓	
Government/Law/Politics				✓	
Health/Fitness				✓	
Illegal/Questionable				✓	
Information Technology				✓	
Internet Communication				✓	
Internet/Intranet Misc.				✓	
Internet Productivity				✓	
News/Reports				✓	

Uncategorized Sites: Block

Overall Quota: Off 0 Min

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

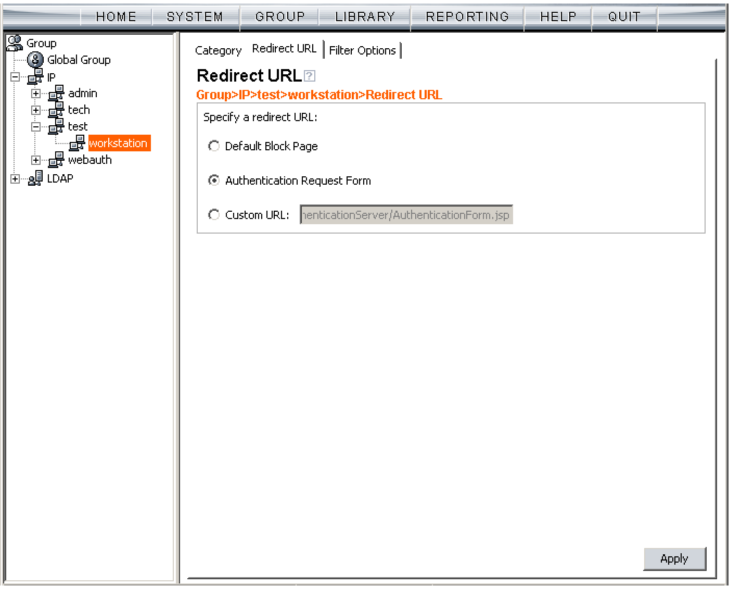
3. In the Category Profile page, select “Block All” from the **Available Filter Levels** pull-down menu.

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**, select “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:



Redirect URL

Group>IP>test>workstation>Redirect URL

Specify a redirect URL:

○ Default Block Page

● Authentication Request Form

○ Custom URL: hentication Server/AuthenticationForm.jsp

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

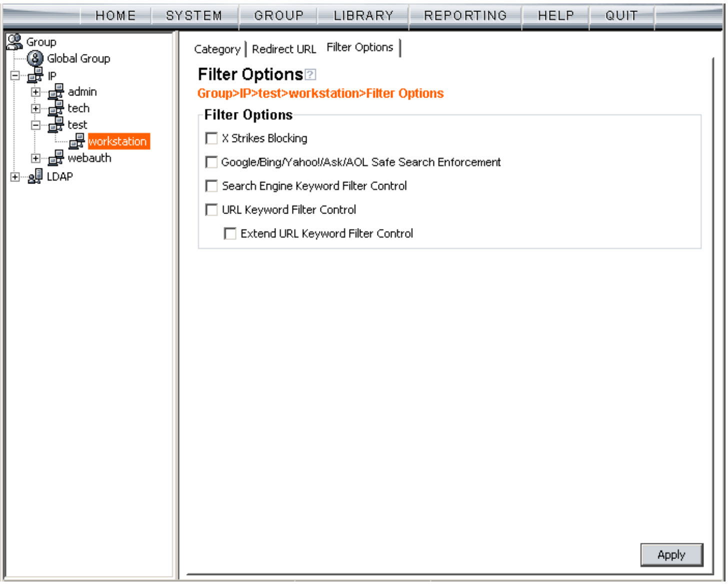
2. Select “Authentication Request Form”.

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:



Filter Options

Group>IP>test>workstation>Filter Options

Filter Options

□ X Strikes Blocking

□ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement

□ Search Engine Keyword Filter Control

□ URL Keyword Filter Control

□ Extend URL Keyword Filter Control

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

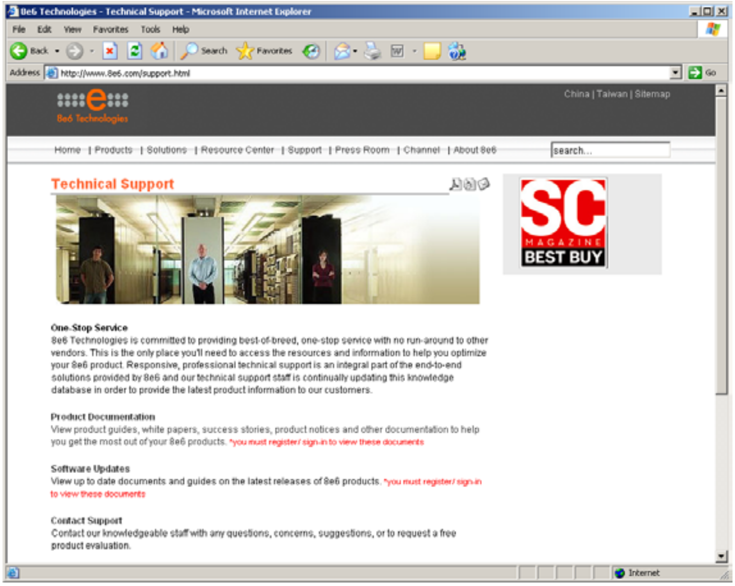
2. Uncheck all the checkboxes: “X Strikes Blocking”, “Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement”, “Search Engine Keyword Filter Control”, “URL Keyword Filter Control”, and “Extend URL Keyword Filter Control”.

3. Click **Apply**.

Step 8: Attempt to access Web content

***NOTE**: For this step, you must have your own profile set up in order to complete the test process.*

1. Launch an Internet browser window supported by the R3000:


8e6 Technologies - Technical Support - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.8e6.com/support.html
Go
8e6 Technologies
China | Taiwan | Sitemap
Home | Products | Solutions | Resource Center | Support | Press Room | Channel | About 8e6
search...
SC MAGAZINE BEST BUY
Internet

Technical Support

One-Stop Service
8e6 Technologies is committed to providing best-of-breed, one-stop service with no run-around to other vendors. This is the only place you'll need to access the resources and information to help you optimize your 8e6 product. Responsive, professional technical support is an integral part of the end-to-end solutions provided by 8e6 and our technical support staff is continually updating this knowledge database in order to provide the latest product information to our customers.

Product Documentation
View product guides, white papers, success stories, product notices and other documentation to help you get the most out of your 8e6 products. *you must register/ sign-in to view these documents

Software Updates
View up to date documents and guides on the latest releases of 8e6 products. *you must register/ sign-in to view these documents

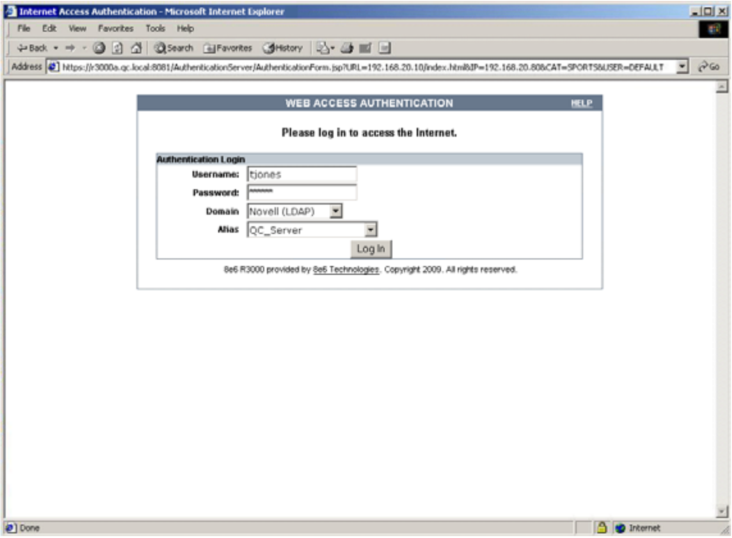
Contact Support
Contact our knowledgeable staff with any questions, concerns, suggestions, or to request a free product evaluation.

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:



https://r3000a.qc.local:8081/AuthenticationServer/AuthenticationForm.jsp?URL=192.168.20.10/index.html&IP=192.168.20.80&CAT=SPORTS&USER=DEFAULT

WEB ACCESS AUTHENTICATION HELP

Please log in to access the Internet.

Authentication Login

Username: tjones

Password: *******

Domain Novell (LDAP)

Alias QC_Server

Log In

8e6 R3000 provided by 8e6 Technologies. Copyright 2009. All rights reserved.

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 sub-section for instructions on setting up the Global Group Profile for authentication.

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

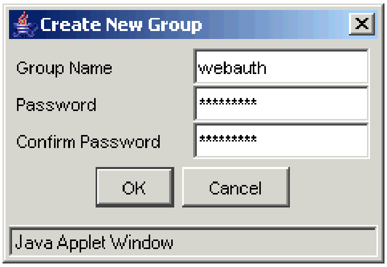
- **If Tier 1 net use based authentication will be used**: Go to the Activate net use based authentication sub-section for instructions on testing the login script and modifying the Global Group Profile for authenticating users.

Activate Web-based authentication for an IP Group

IP Group authentication is the preferred selection for Web-based 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:



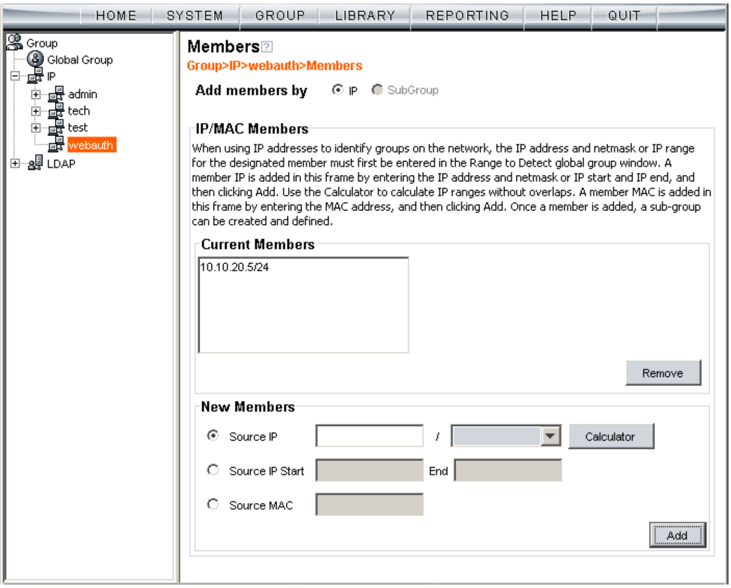
Group Name: webauth
Password: *********
Confirm Password: *********

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:



Members

Group>IP>webauth>Members

Add members by ● IP ○ SubGroup

IP/MAC Members

When using IP addresses to identify groups on the network, the IP address and netmask or IP range for the designated member must first be entered in the Range to Detect global group window. A member IP is added in this frame by entering the IP address and netmask or IP start and IP end, and then clicking Add. Use the Calculator to calculate IP ranges without overlaps. A member MAC is added in this frame by entering the MAC address, and then clicking Add. Once a member is added, a sub-group can be created and defined.

Current Members

10.10.20.5/24

New Members

● Source IP /

○ Source IP Start End

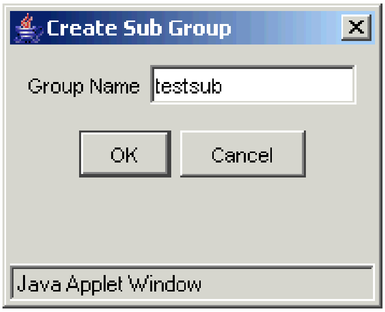
○ Source MAC

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

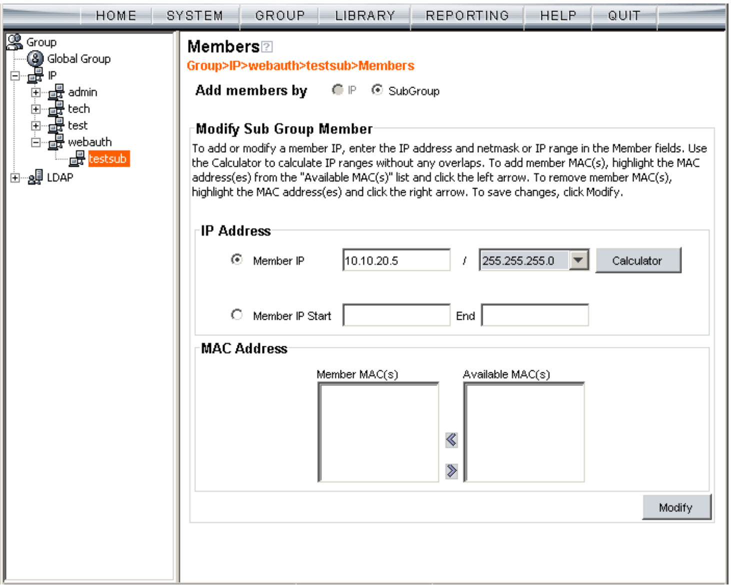
1. Select the IP Group “webauth” from the tree.
2. Click Add Sub Group in the pop-up menu to open the Create Sub Group dialog box:



Group Name: testsub

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:



Members

Group>IP>webauth>testsub>Members

Add members by ○ IP ● SubGroup

Modify Sub Group Member

To add or modify a member IP, enter the IP address and netmask or IP range in the Member fields. Use the Calculator to calculate IP ranges without any overlaps. To add member MAC(s), highlight the MAC address(es) from the "Available MAC(s)" list and click the left arrow. To remove member MAC(s), highlight the MAC address(es) and click the right arrow. To save changes, click Modify.

IP Address

● Member IP 10.10.20.5 / 255.255.255.0

○ Member IP Start End

MAC Address

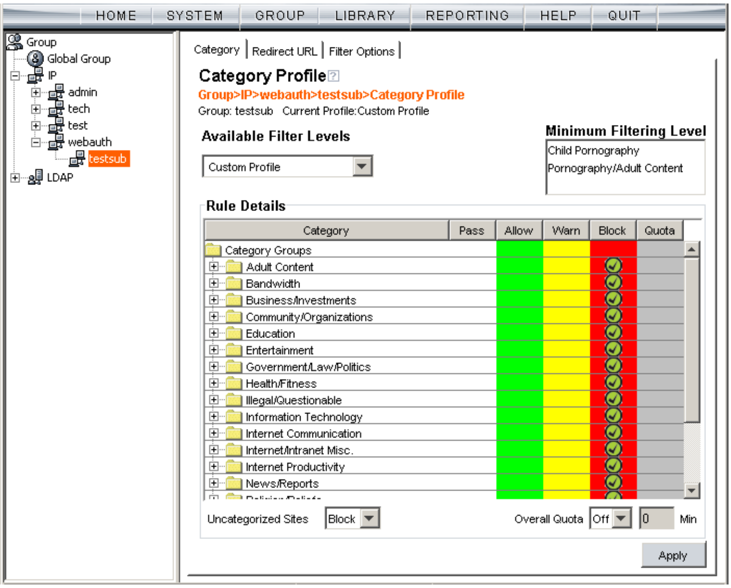
Member MAC(s) Available MAC(s)

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:



Category Profile

Group>IP>webauth>testsub>Category Profile

Group: testsub Current Profile:Custom Profile

Available Filter Levels: Custom Profile

Minimum Filtering Level: Child Pornography, Pornography/Adult Content

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content				✓	
Bandwidth				✓	
Business/Investments				✓	
Community/Organizations				✓	
Education				✓	
Entertainment				✓	
Government/Law/Politics				✓	
Health/Fitness				✓	
Illegal/Questionable				✓	
Information Technology				✓	
Internet Communication				✓	
Internet/Intranet Misc.				✓	
Internet Productivity				✓	
News/Reports				✓	

Uncategorized Sites: Block

Overall Quota: Off 0 Min

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

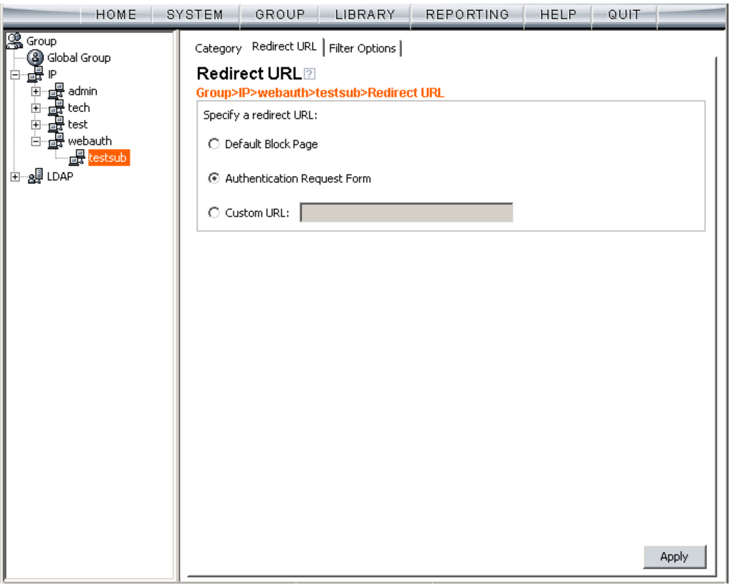
3. In the Category Profile page, select “Block All” from the **Available Filter Levels** pull-down menu.

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**, select “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:



Redirect URL

Group>IP>webauth>testsub>Redirect URL

Specify a redirect URL:

○ Default Block Page

● Authentication Request Form

○ Custom URL:

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

2. Select “Authentication Request Form”.

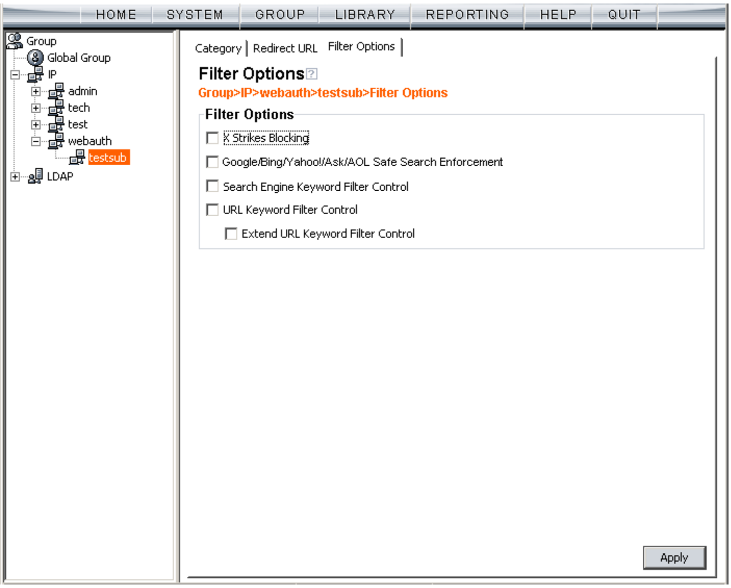
NOTE: *Since the Authentication Request Form radio button selection uses the host name of the server—not the IP address—be sure there is a DNS resolution for the host name.*

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:



Filter Options

Group>IP>webauth>testsub>Filter Options

Filter Options

□ X Strikes Blocking

□ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement

□ Search Engine Keyword Filter Control

□ URL Keyword Filter Control

□ Extend URL Keyword Filter Control

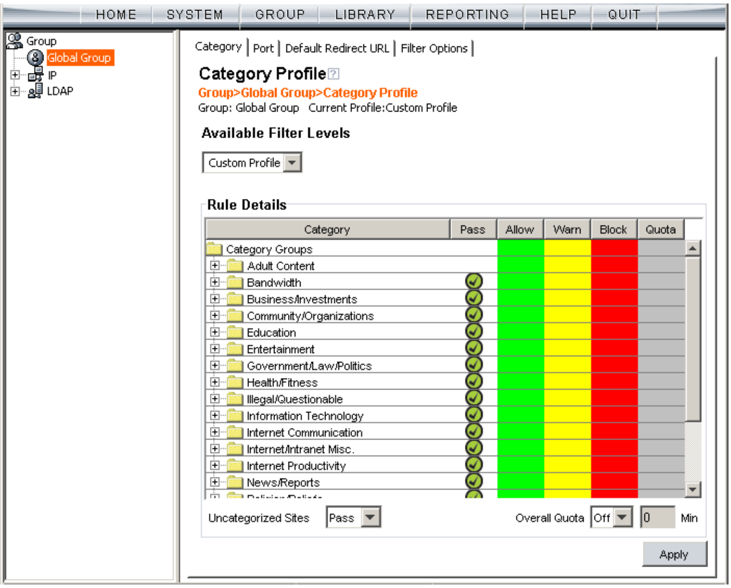
Fig. 5-17 Sub Group Profile window, Filter Options tab

2. Uncheck all the checkboxes: “X Strikes Blocking”, “Google/Bing/Yahoo!/Ask/AOL 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:



Category Profile

Group>Global Group>Category Profile

Group: Global Group   Current Profile:Custom Profile

Available Filter Levels

Custom Profile

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups		🟩	🟨	🟥	
Adult Content		🟩	🟨	🟥	
Bandwidth	✓	🟩	🟨	🟥	
Business/Investments	✓	🟩	🟨	🟥	
Community/Organizations	✓	🟩	🟨	🟥	
Education	✓	🟩	🟨	🟥	
Entertainment	✓	🟩	🟨	🟥	
Government/Law/Politics	✓	🟩	🟨	🟥	
Health/Fitness	✓	🟩	🟨	🟥	
Illegal/Questionable	✓	🟩	🟨	🟥	
Information Technology	✓	🟩	🟨	🟥	
Internet Communication	✓	🟩	🟨	🟥	
Internet/Intranet Misc.	✓	🟩	🟨	🟥	
Internet Productivity	✓	🟩	🟨	🟥	
News/Reports	✓	🟩	🟨	🟥	

Uncategorized Sites: Pass

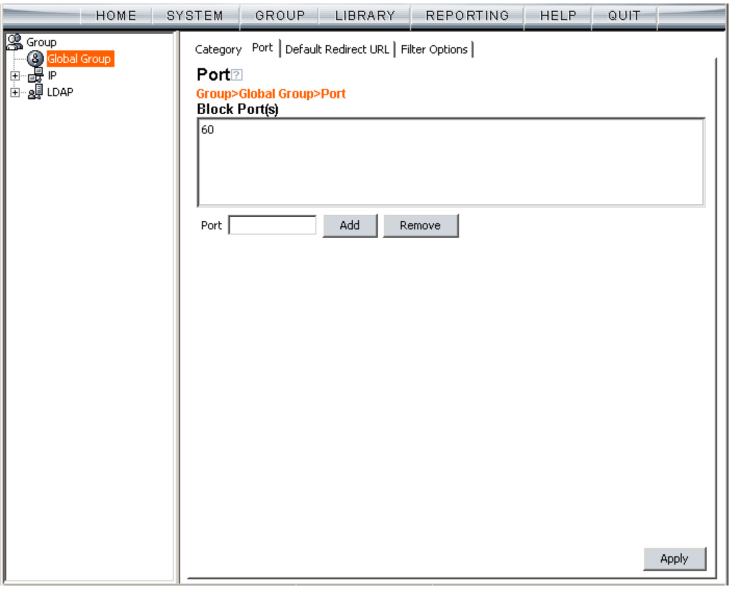
Overall Quota: Off 0 Min

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, trigger a warn message for the end user, or be blocked.

b. Click **Apply**.

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



60

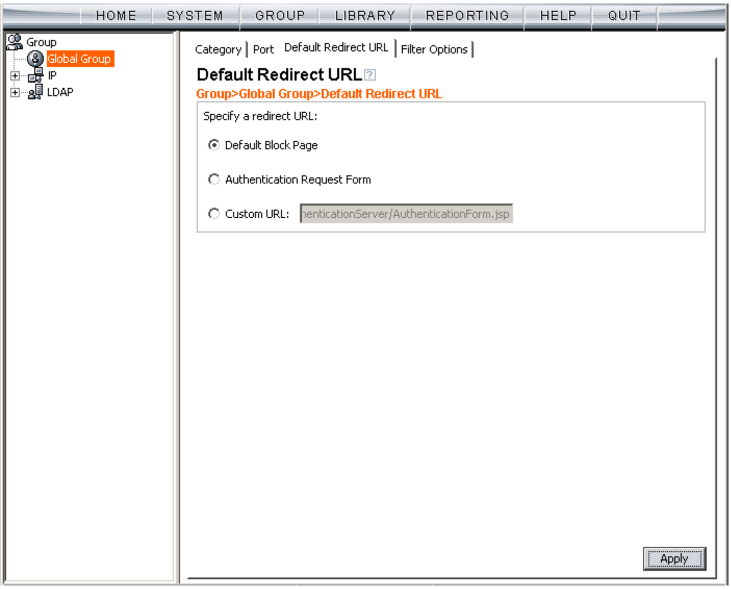
Fig. 5-19 Global Group Profile window, Port tab

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:



Default Redirect URL

Group>Global Group>Default Redirect URL

Specify a redirect URL:

● Default Block Page

○ Authentication Request Form

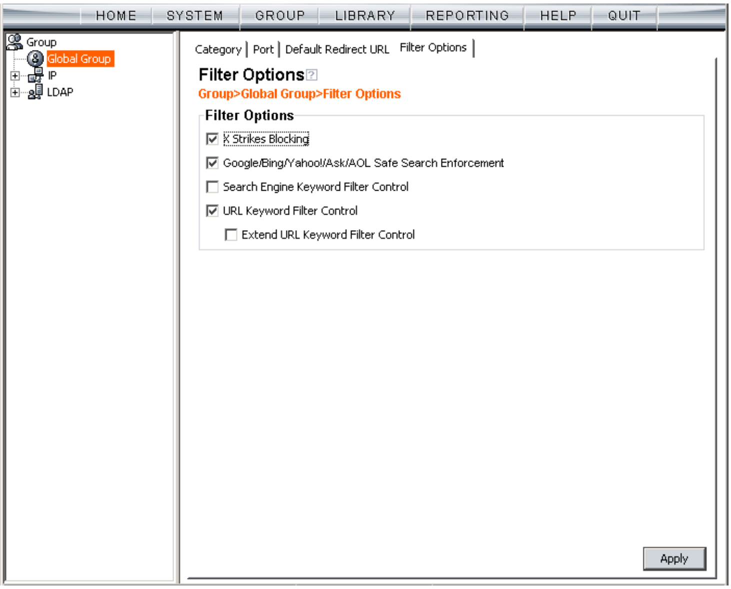
○ Custom URL: hentication Server/AuthenticationForm.jsp

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:



Filter Options

Group>Global Group>Filter Options

Filter Options

☑ X Strikes Blocking

☑ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement

□ Search Engine Keyword Filter Control

☑ URL Keyword Filter Control

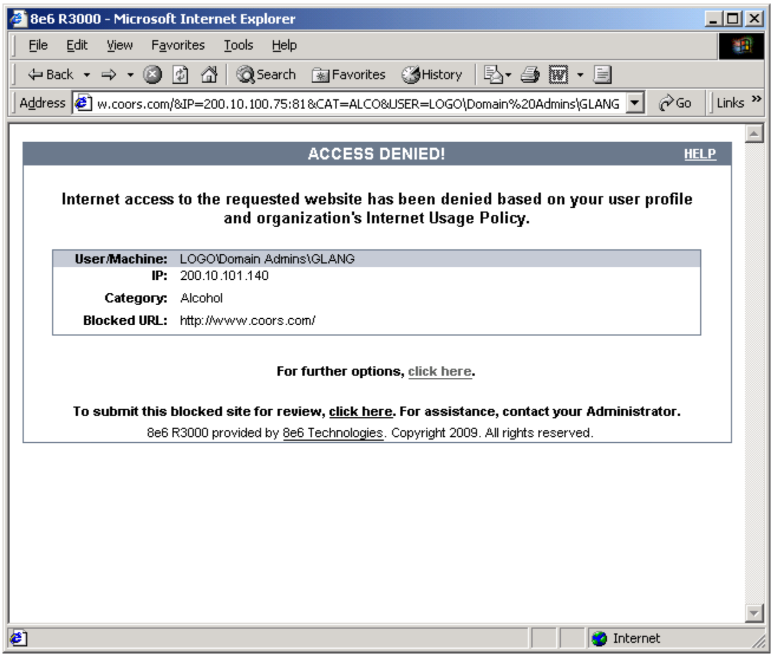
□ Extend URL Keyword Filter Control

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
File Edit View Favorites Tools Help
Back Search Favorites History
Address w.coors.com/&IP=200.10.100.75:81&CAT=ALCO&USER=LOGO\Domain%20Admins\GLANG
Go Links
Internet

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
Blocked URL:	http://www.coors.com/

For further options, click here.

To submit this blocked site for review, click here. For assistance, contact your Administrator.

8e6 R3000 provided by 8e6 Technologies. Copyright 2009. All rights reserved.

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:

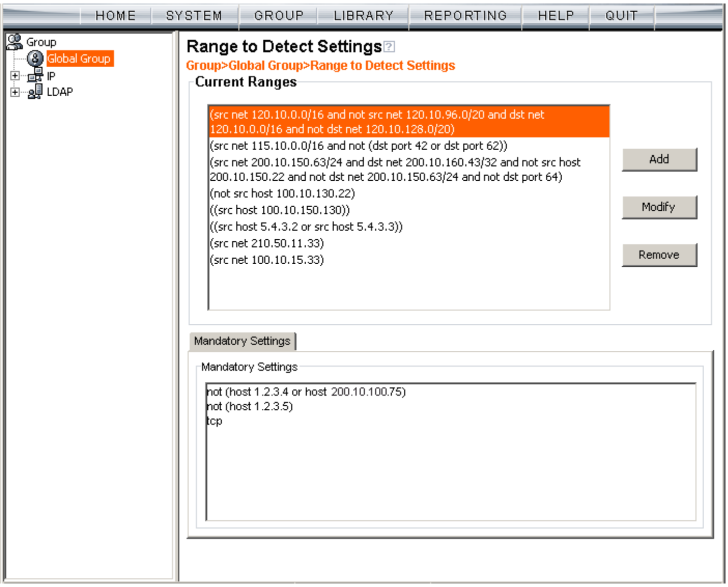
- **Block Web access only** – Select this option if you do not want to log traffic for a machine that you set up to be excluded from filtering on the network. Using this option, you exclude the IP address of a machine via the Range to Detect window. If you select this option, go to Step 1A.
- **Block 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:



Range to Detect Settings

Group>Global Group>Range to Detect Settings

Current Ranges

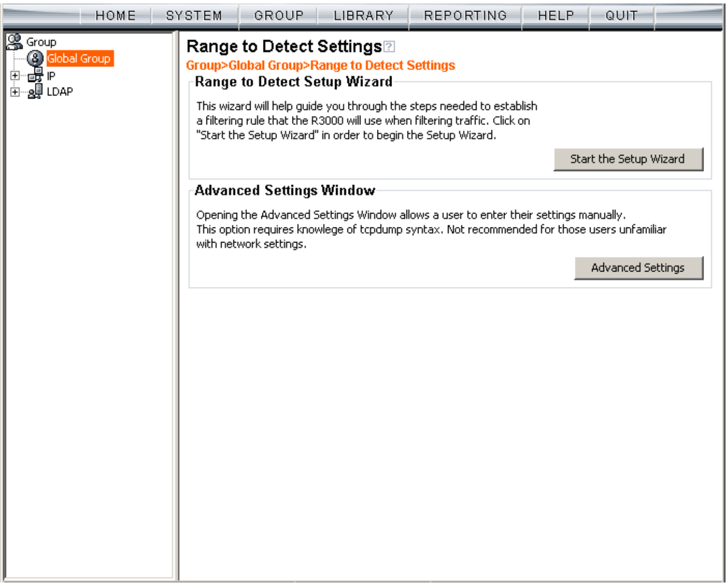
```
(src net 120.10.0.0/16 and not src net 120.10.96.0/20 and dst net
120.10.0.0/16 and not dst net 120.10.128.0/20)
(src net 115.10.0.0/16 and not (dst port 42 or dst port 62))
(src net 200.10.150.63/24 and dst net 200.10.160.43/32 and not src host
200.10.150.22 and not dst net 200.10.150.63/24 and not dst port 64)
(not src host 100.10.130.22)
((src host 100.10.150.130))
((src host 5.4.3.2 or src host 5.4.3.3))
(src net 210.50.11.33)
(src net 100.10.15.33)
```

Mandatory Settings

```
not (host 1.2.3.4 or host 200.10.100.75)
not (host 1.2.3.5)
tcp
```

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:



Range to Detect Settings

Group>Global Group>Range to Detect Settings

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. Click on "Start the Setup Wizard" in order to begin the Setup Wizard.

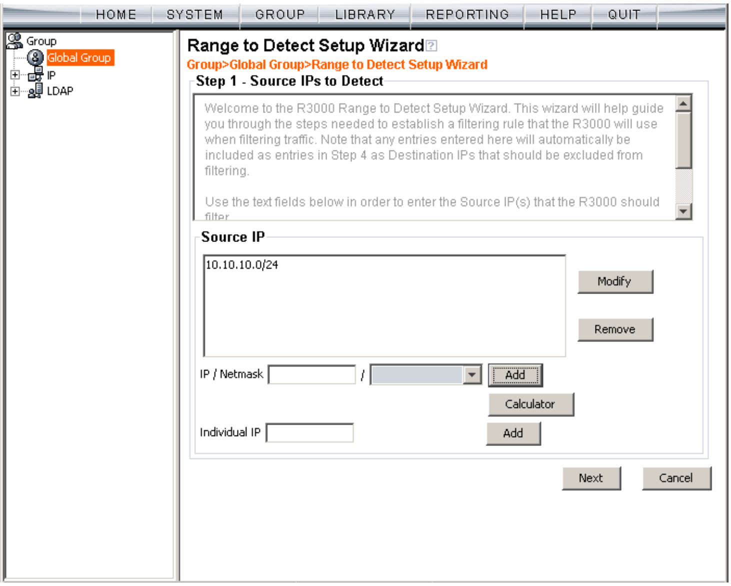
Advanced Settings Window

Opening the Advanced Settings Window allows a user to enter their settings manually. This option requires knowlege of tcpdump syntax. Not recommended for those users unfamiliar with network settings.

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



Range to Detect Setup Wizard

Group>Global Group>Range to Detect Setup Wizard

Step 1 - Source IPs to Detect

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

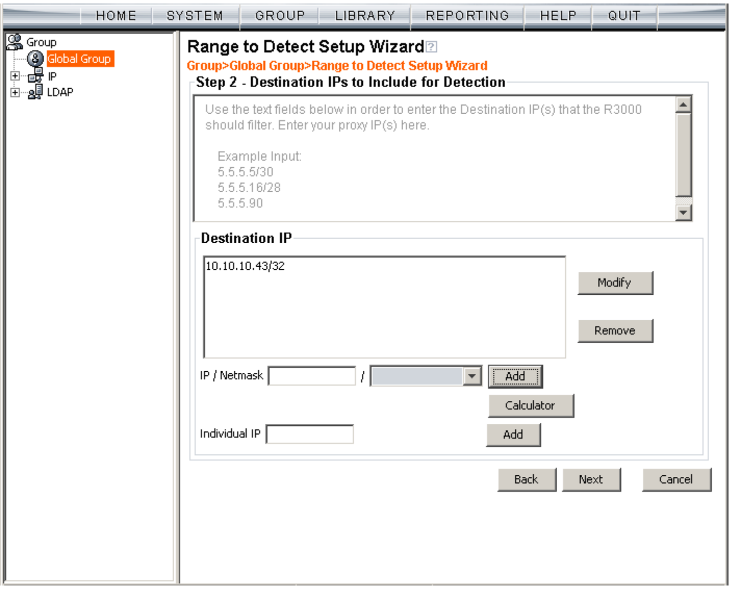
10.10.10.0/24

IP / Netmask /

Individual IP

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:



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:
5.5.5.5/30
5.5.5.16/28
5.5.5.90

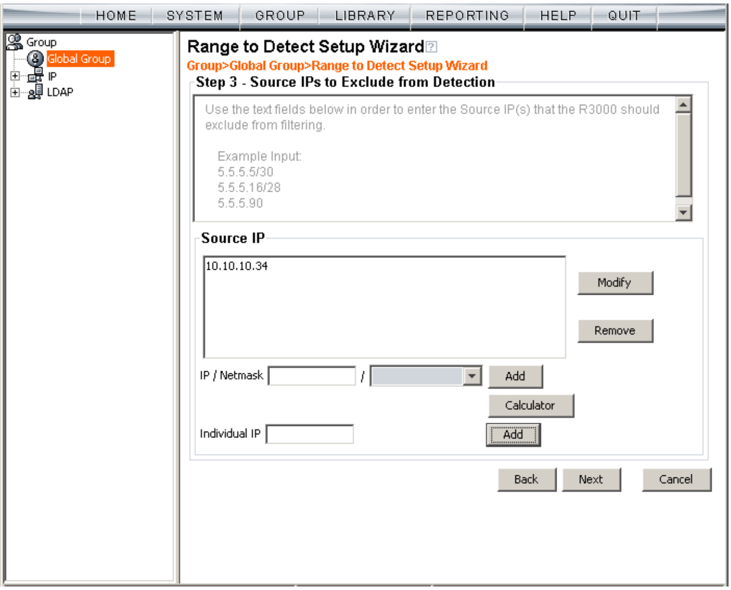
Destination IP

10.10.10.43/32

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

3. 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:



Range to Detect Setup Wizard

Group>Global Group>Range to Detect Setup Wizard

Step 3 - Source IPs to Exclude from Detection

Use the text fields below in order to enter the Source IP(s) that the R3000 should exclude from filtering.

Example Input:
5.5.5.5/30
5.5.5.16/28
5.5.5.90

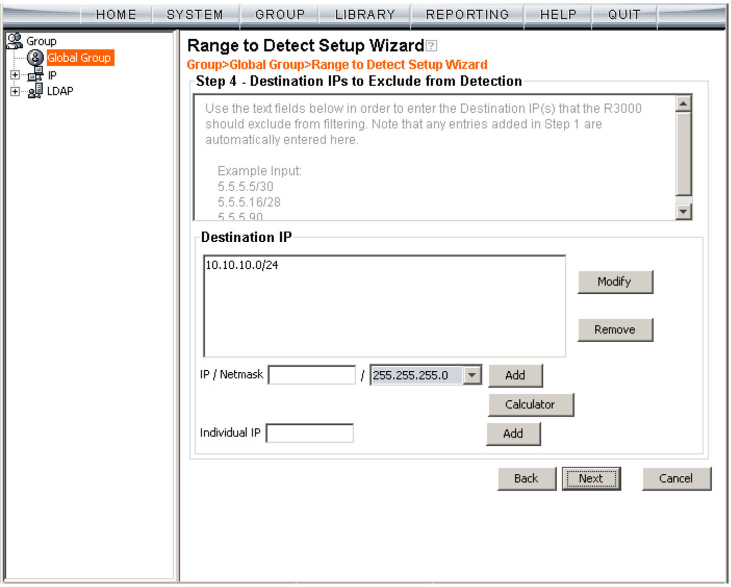
Source IP

10.10.10.34

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

5. 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:



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 R3000 should exclude from filtering. Note that any entries added in Step 1 are automatically entered here.

Example Input:
5.5.5.5/30
5.5.5.16/28
5.5.5.90

Destination IP

10.10.10.0/24

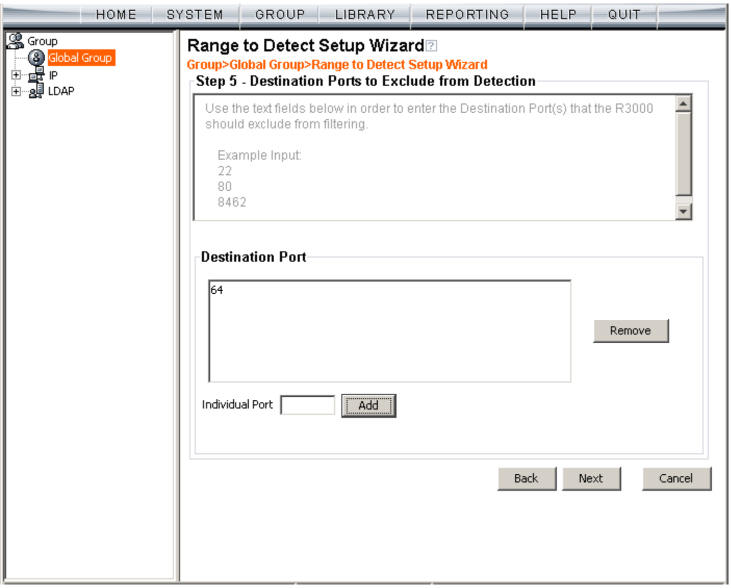
IP / Netmask / 255.255.255.0

Individual IP

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

7. 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:



Range to Detect Setup Wizard

Group>Global Group>Range to Detect Setup Wizard

Step 5 - Destination Ports to Exclude from Detection

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

Destination Port

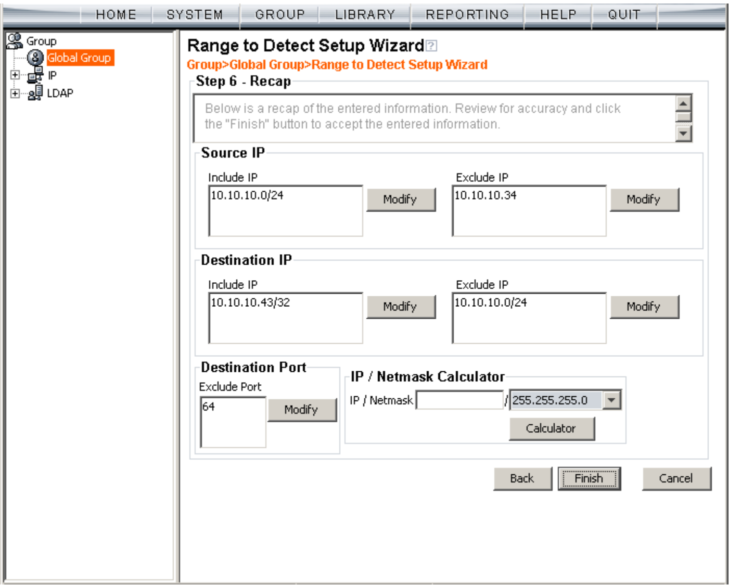
64

Individual Port

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:



Range to Detect Setup Wizard

Group>Global Group>Range to Detect Setup Wizard

Step 6 - Recap

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: 10.10.10.0/24

Exclude IP: 10.10.10.34

Destination IP

Include IP: 10.10.10.43/32

Exclude IP: 10.10.10.0/24

Destination Port

Exclude Port: 64

IP / Netmask Calculator

IP / Netmask: / 255.255.255.0

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.

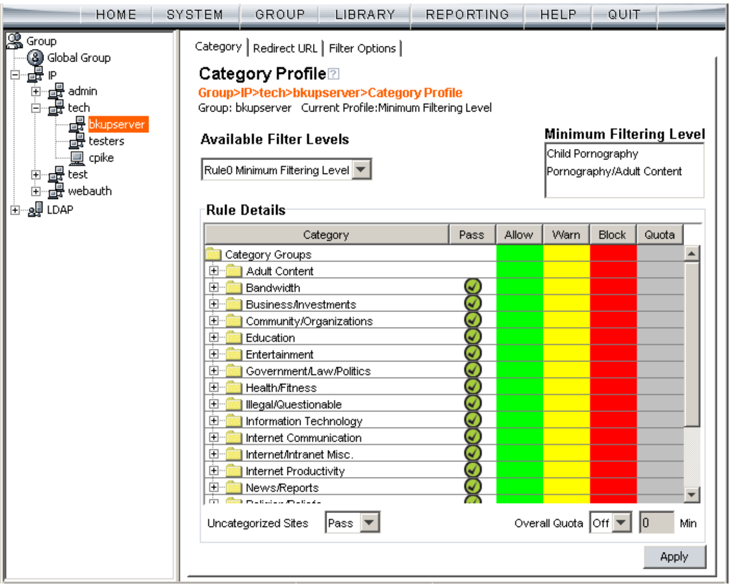
As a result of these entries, the IP address(es) specified to be excluded will not be logged or filtered on the network.

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:



Category Profile

Group>IP>tech>bkupserver>Category Profile

Group: bkupserver Current Profile:Minimum Filtering Level

Available Filter Levels

Rule0 Minimum Filtering Level

Minimum Filtering Level

Child Pornography
Pornography/Adult Content

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups		🟩	🟨	🟥	
Adult Content		🟩	🟨	🟥	
Bandwidth	✓	🟩	🟨	🟥	
Business/Investments	✓	🟩	🟨	🟥	
Community/Organizations	✓	🟩	🟨	🟥	
Education	✓	🟩	🟨	🟥	
Entertainment	✓	🟩	🟨	🟥	
Government/Law/Politics	✓	🟩	🟨	🟥	
Health/Fitness	✓	🟩	🟨	🟥	
Illegal/Questionable	✓	🟩	🟨	🟥	
Information Technology	✓	🟩	🟨	🟥	
Internet Communication	✓	🟩	🟨	🟥	
Internet/Intranet Misc.	✓	🟩	🟨	🟥	
Internet Productivity	✓	🟩	🟨	🟥	
News/Reports	✓	🟩	🟨	🟥	

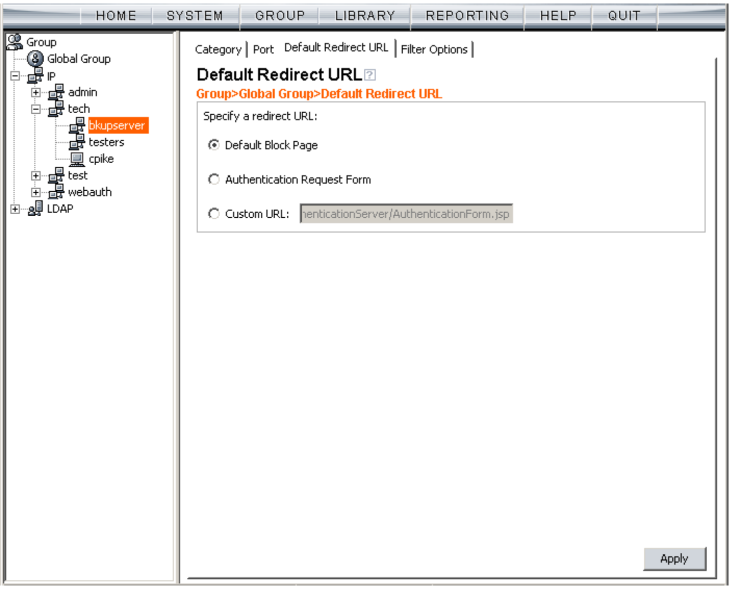
Uncategorized Sites: Pass

Overall Quota: Off 0 Min

Apply

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, trigger a warn message for the end user, or be blocked.
4. Click **Apply**.
5. Click the Redirect URL tab to display the Redirect URL page:



Default Redirect URL

Group>Global Group>Default Redirect URL

Specify a redirect URL:

● Default Block Page

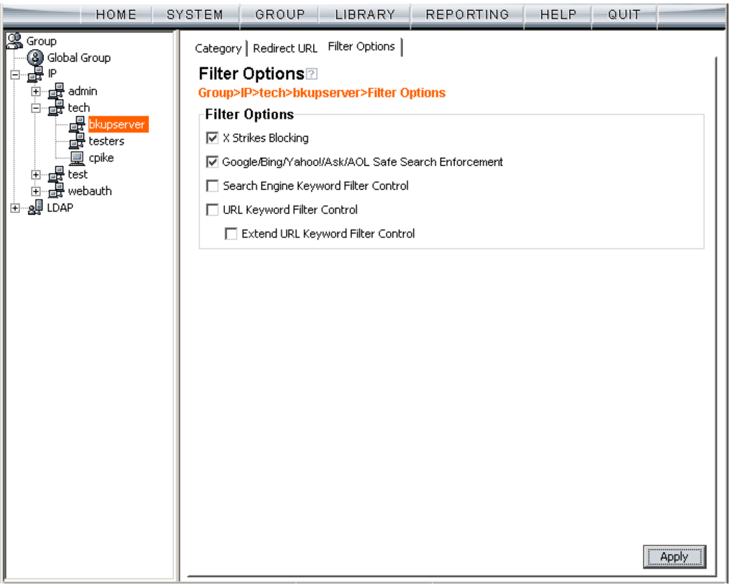
○ Authentication Request Form

○ Custom URL: henticationServer/AuthenticationForm.jsp

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:



Filter Options

Group>IP>tech>bkupserver>Filter Options

Filter Options

☑ X Strikes Blocking

☑ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement

☐ Search Engine Keyword Filter Control

☐ URL Keyword Filter Control

☐ Extend URL Keyword Filter Control

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

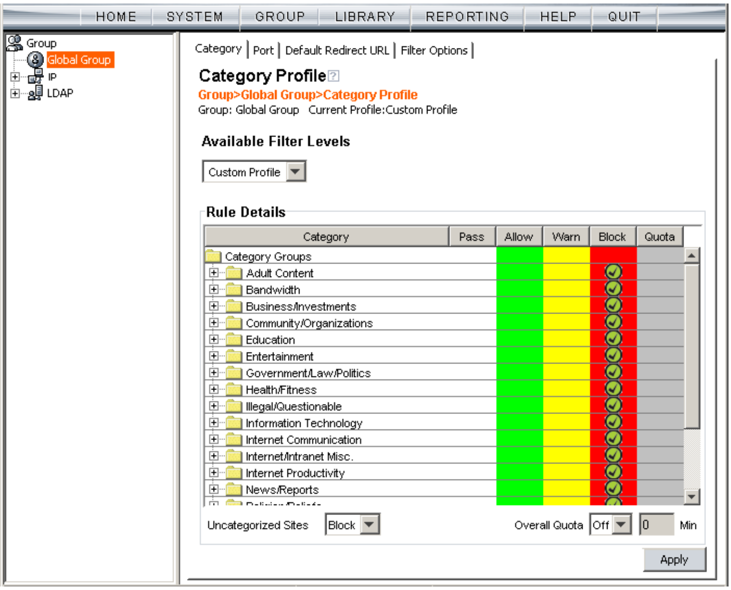
8. Select filter options to be enabled, and click **Apply**.

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:



Category Profile

Group>Global Group>Category Profile

Group: Global Group Current Profile:Custom Profile

Available Filter Levels

Custom Profile

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content				✓	
Bandwidth				✓	
Business/Investments				✓	
Community/Organizations				✓	
Education				✓	
Entertainment				✓	
Government/Law/Politics				✓	
Health/Fitness				✓	
Illegal/Questionable				✓	
Information Technology				✓	
Internet Communication				✓	
Internet/Intranet Misc.				✓	
Internet Productivity				✓	
News/Reports				✓	

Uncategorized Sites: Block

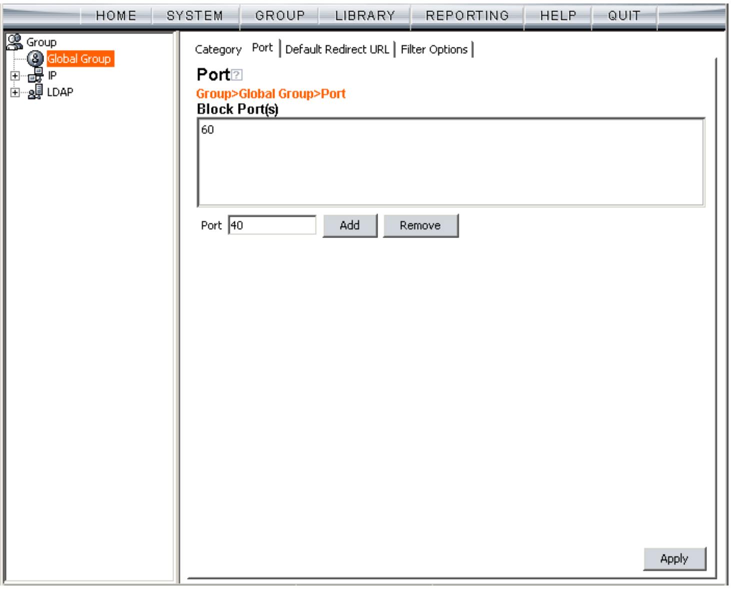
Overall Quota: Off 0 Min

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:



Port

Group>Global Group>Port

Block Port(s)

60

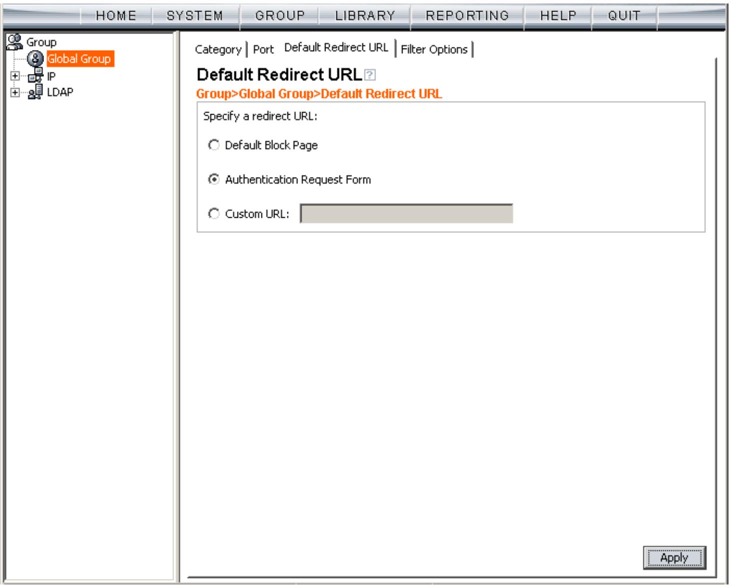
Port 40

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:



Default Redirect URL

Group>Global Group>Default Redirect URL

Specify a redirect URL:

○ Default Block Page

● Authentication Request Form

○ Custom URL:

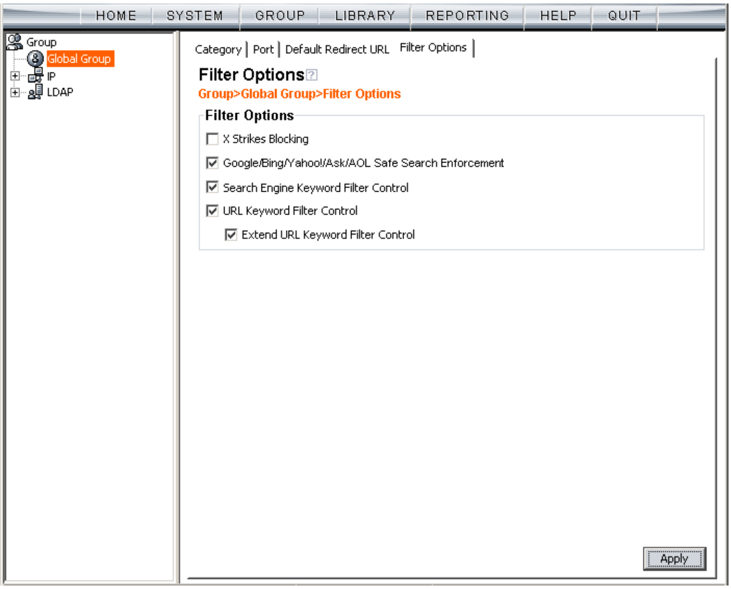
Fig. 5-36 Global Group Profile window, Redirect URL tab

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:



Filter Options

Group>Global Group>Filter Options

Filter Options

☐ X Strikes Blocking

☑ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement

☑ Search Engine Keyword Filter Control

☑ URL Keyword Filter Control

☑ Extend URL Keyword Filter Control

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.

Add Net Use command to Login Scripts

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, trigger a warn message for the end user, 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.m86security.com/support/** or contact us by phone, by e-mail, or in writing.

For troubleshooting tips, visit **http://www.m86security.com/software/8e6/ts/r3000.html**

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 3*

International

1. Call **+1-714-282-6111**
2. Select *option 3*

E-Mail

For non-emergency assistance, e-mail us at **support@m86security.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

7 Fl., No. 1, Sec. 2, Ren-Ai Rd.
Taipei 10055
Taiwan, R.O.C.

Taipei Local	:	2397-0300
Fax	:	2397-0306
Domestic Taiwan	:	02-2397-0300
International	:	886-2-2397-0300

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 NetBIOS:

- Windows 2000 or 2003 Server in mixed/legacy mode

Using LDAP:

- Microsoft Active Directory Mixed Mode
- Microsoft Active Directory Native Mode

Tier 2, Tier 3: Web-based authentication

Using an LDAP domain:

- Windows Active Directory 2002 and 2003
- Novell eDirectory
- SunONE directory server
- Open 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:

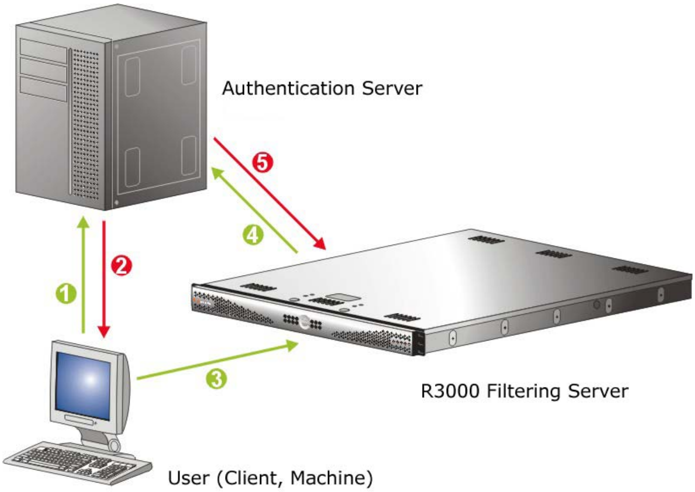


Fig. A-1 Net use based authentication module diagram

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.
3. 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.

6. 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.*

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 re-authenticate 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 method

Tier 1 supports the LDAP authentication method. 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 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.

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 the following location on the 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

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.

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:

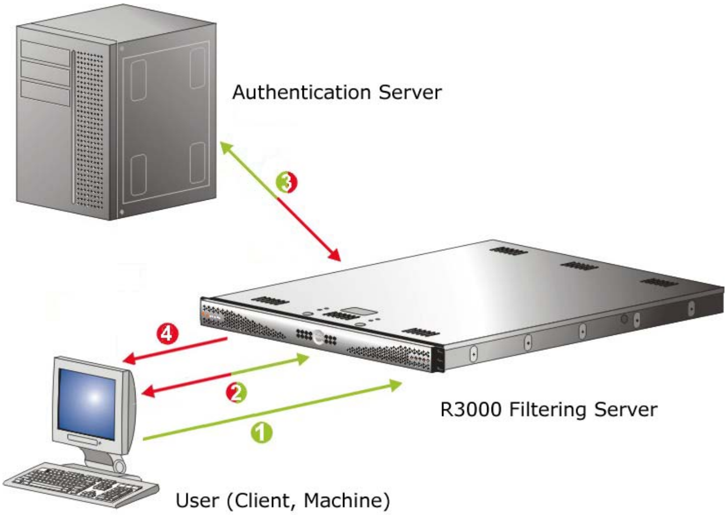


Fig. A-2 Web-based authentication module diagram

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.)*

On a Macintosh, the 8e6 Authenticator client (Authenticator) should be installed on the client machine so that it will automatically launch when the end user logs in.

***NOTES**: Most Apple shops use Apple Remote Desktop to deploy files in bulk, rather than posting each individual download on a file server.*

The Marshal8e6 Authenticator Deployment Kit is designed for the Macintosh and contains the Authenticator executable, along with some support files. When installing the Marshal8e6 Authenticator Deployment Kit on a Macintosh, the informational Authenticator Basics.pdf document launches. Please review this document before installing the Authenticator.

Environment requirements

Windows 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 Windows 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 El Torito specification
- USB or PS/2* mouse

Macintosh minimum system requirements

The following minimum server components are required when using a Macintosh:

- OS X 10.5
- Intel processor
- Super VGA display adapter
- One network board
- CD drive

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
- Windows Vista (all editions except Home)
- Macintosh OS X 10.5

NOTE*: Windows XP Home and Vista Home Editions 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 environments

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), 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.*

Macintosh environment

1. The administrator installs a LaunchAgent on the client machine.
2. Using a Macintosh machine, an end user logs on the domain and launches the LaunchAgent.
3. The end user’s launchd process invokes Authenticator on login.
4. The 8e6 Authenticator client identifies the end user by using the OS X Directory Services, then retrieves the username and domain name, and sends this information (LOGON event) to the R3000.
5. The R3000 looks up the groups to which the end user belongs, 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.

8e6 Authenticator configuration priority

The source and order in which parameters are received and override one another are described below.

***NOTES**: The RA[] parameter for the R3000 IP address is the only parameter that must be configured.*

Any parameter set at the end of the list will override any parameter that was previously set.

Windows

1. **Compiled Defaults**: Given no parameters at all, the client will try to execute using the default compilation.
2. **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.

Macintosh

1. **Compiled Defaults**: Given no parameters at all, the client will try to execute using the default compilation.
2. **Configuration File** (optional): The default configuration file name is “8e6Authenticator.conf”. The path can be specified on the command line with the CF[] parameter. Review the ++ comment following Table 1 for more information. If the path is not specified, the following directories are searched, in this order:

   a. current working directory (i.e. the directory from which the program was launched)

   b. “.8e6Authenticator/.8e6Authenticator.conf” file in the user’s HOME folder (if present)

   c. 8e6Authenticator.conf file in the path containing the Authenticator executable, if present
3. **Command Line** (optional): Options on the command line will override compiled defaults and the configuration file. The command line can be left blank.

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 }
```

***NOTE**: On a Macintosh, the LF[] parameter is ignored. Log files are always placed in the user’s home folder under ~/Library/Logs/8e6authenticator.log. To view the logs, either the OS X Console application or the UNIX “tail” command can be used.*

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 = Novell)	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 Support 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 output 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;3.3.3.3:222)]
  ```

  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 102.108.2.15 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 3: 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 Directory-based 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 running on a 32-bit platform
- 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

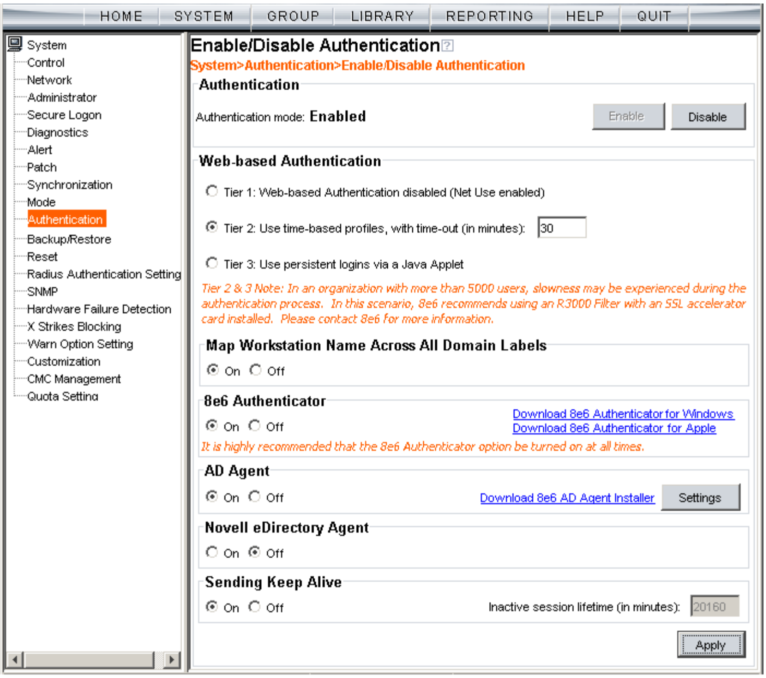
Work flow in a Windows environment

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:



Enable/Disable Authentication

System>Authentication>Enable/Disable Authentication

Authentication

Authentication mode: **Enabled**

Web-based Authentication

○ Tier 1: Web-based Authentication disabled (Net Use enabled)

● Tier 2: Use time-based profiles, with time-out (in minutes): 30

○ Tier 3: Use persistent logins via a Java Applet

Tier 2 & 3 Note: 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.

Map Workstation Name Across All Domain Labels

● On ○ Off

8e6 Authenticator

● On ○ Off

Download 8e6 Authenticator for Windows
Download 8e6 Authenticator for Apple

It is highly recommended that the 8e6 Authenticator option be turned on at all times.

AD Agent

● On ○ Off

Download 8e6 AD Agent Installer

Novell eDirectory Agent

○ On ● Off

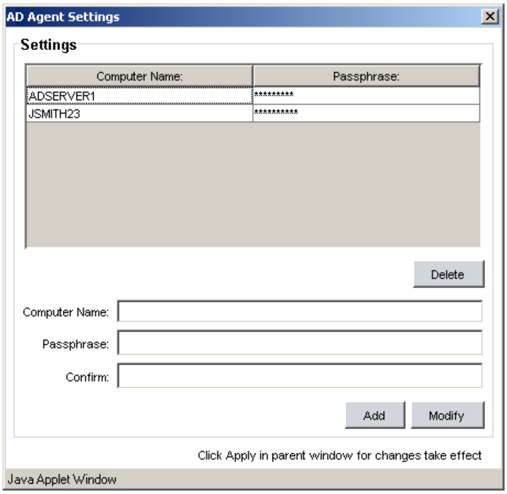
Sending Keep Alive

● On ○ Off

Inactive session lifetime (in minutes): 20160

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:



Computer Name:	Passphrase:
ADSERVER1	*********
JSMITH23	**********

Computer Name:

Passphrase:

Confirm:

Click Apply in parent window for changes take effect

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

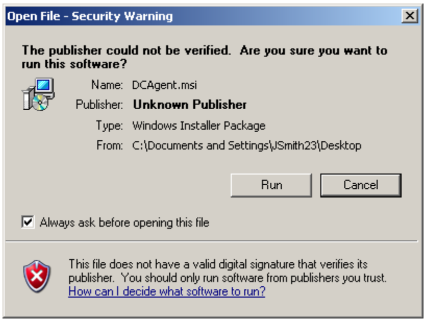
The steps in this section provide instructions for setting up and running AD Agent on a simple, single-domain network.

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:



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: DCAgent.msi

Publisher: **Unknown Publisher**

Type: Windows Installer Package

From: C:\Documents and Settings\JSmith23\Desktop

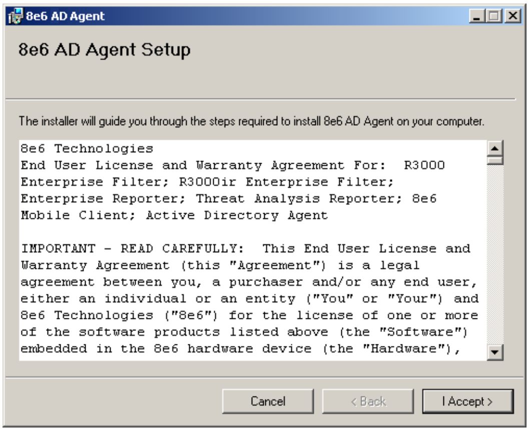
☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

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:



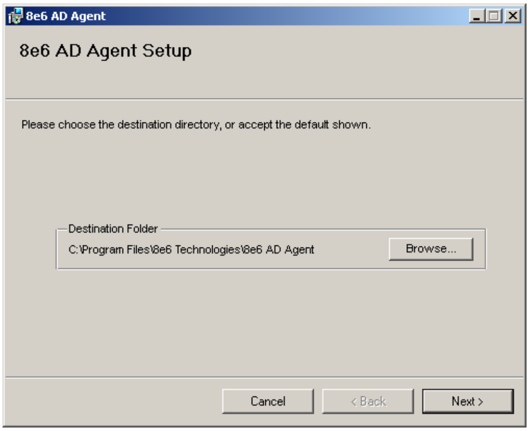
The installer will guide you through the steps required to install 8e6 AD Agent on your computer.

```
8e6 Technologies
End User License and Warranty Agreement For:  R3000
Enterprise Filter; R3000ir Enterprise Filter;
Enterprise Reporter; Threat Analysis Reporter; 8e6
Mobile Client; Active Directory Agent

IMPORTANT - READ CAREFULLY:  This End User License and
Warranty Agreement (this "Agreement") is a legal
agreement between you, a purchaser and/or any end user,
either an individual or an entity ("You" or "Your") and
8e6 Technologies ("8e6") for the license of one or more
of the software products listed above (the "Software")
embedded in the 8e6 hardware device (the "Hardware"),
```

Fig. A-6 AD Agent EULA

3. After reading the EULA, click **Accept** to proceed with specifying the destination folder for installing the AD Agent:

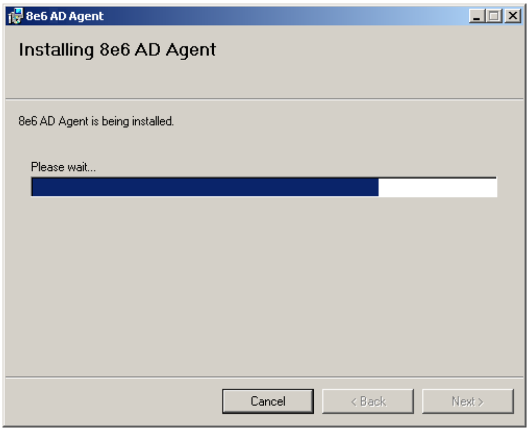


Please choose the destination directory, or accept the default shown.

Destination Folder
C:\Program Files\8e6 Technologies\8e6 AD Agent

Fig. A-7 Specify installation setup destination

4. After specifying the destination folder for installing the AD Agent, click **Next** to begin the installation setup process:



8e6 AD Agent

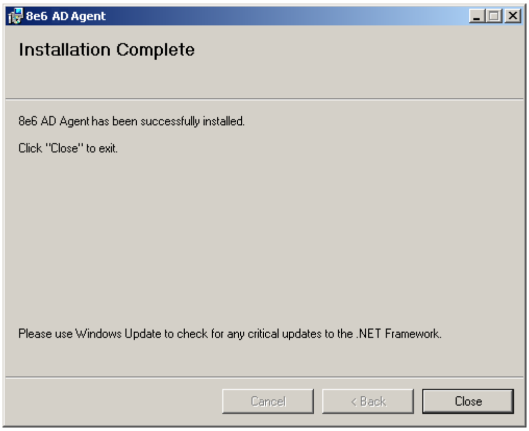
Installing 8e6 AD Agent

8e6 AD Agent is being installed.

Please wait...

Fig. A-8 AD Agent installation

5. When the AD Agent installation setup process has successfully finished, completion information displays:



8e6 AD Agent

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.

Fig. A-9 Installation Complete

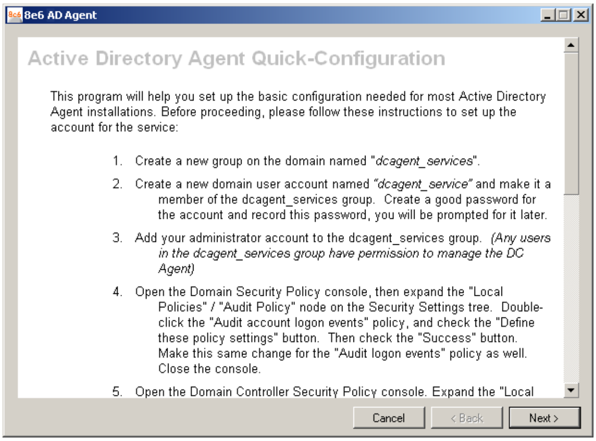
Click **Close** to close the installation setup window and to open the AD Agent configuration wizard window (see Fig. A-10). The configuration wizard can be completed now or at a later point in time.

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:



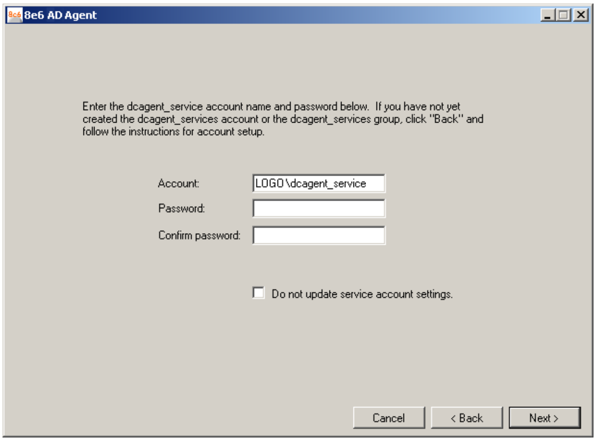
Active Directory Agent Quick-Configuration

This program will help you set up the basic configuration needed for most Active Directory Agent installations. Before proceeding, please follow these instructions to set up the account for the service:

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. Create a good password for the account and record this password, you will be prompted for it later.
3. Add your administrator account to the dcagent_services group. *(Any users in the dcagent_services group have permission to manage the DC Agent)*
4. Open the Domain Security Policy console, then expand the "Local Policies" / "Audit Policy" node on the Security Settings tree. Double-click the "Audit account logon events" policy, and check the "Define these policy settings" button. Then check the "Success" button. Make this same change for the "Audit logon events" policy as well. Close the console.
5. Open the Domain Controller Security Policy console. Expand the "Local

Fig. A-10 AD Agent configuration wizard, preliminary instructions

Click **Next** to go to the account and password page:



Enter the dcagent_service account name and password below. If you have not yet created the dcagent_services account or the dcagent_services group, click "Back" and follow the instructions for account setup.

Account: LOGO\dcagent_service

Password:

Confirm password:

□ Do not update service account settings.

Fig. A-11 Account and password information

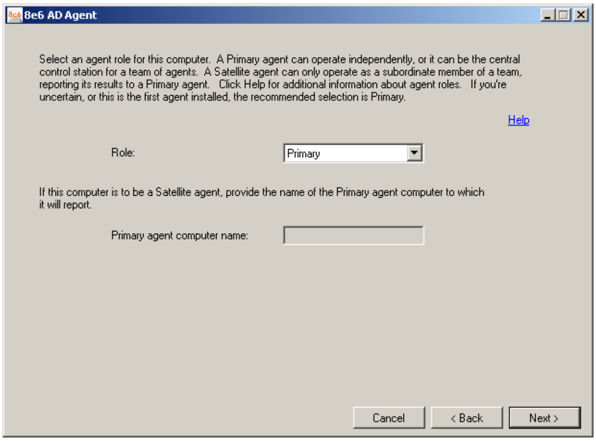
2. By default, the Account field is populated with the path of the dcagent_service account.

   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

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 uncertain, or this is the first agent installed, the recommended selection 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:

Fig. A-12 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-13).

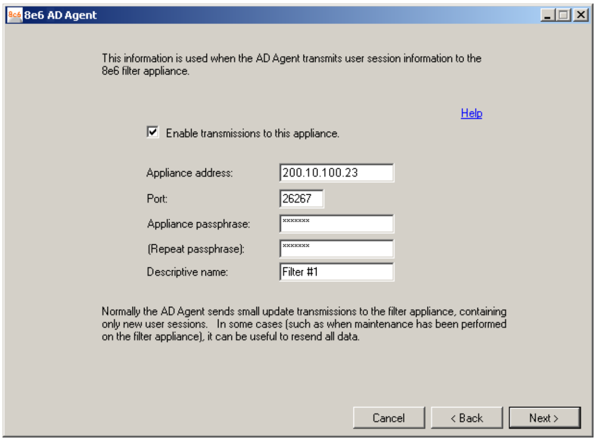
   - If the role of this AD Agent is “Satellite” - Do the following:

     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-14).

4. If configuring a primary AD Agent, make the following entries in the appropriate fields:



This information is used when the AD Agent transmits user session information to the 8e6 filter appliance.

☑ Enable transmissions to this appliance.

Appliance address: 200.10.100.23

Port: 26267

Appliance passphrase: *******

(Repeat passphrase): *******

Descriptive name: Filter #1

Normally the AD Agent sends small update transmissions to the filter appliance, containing only new user sessions. In some cases (such as when maintenance has been performed on the filter appliance), it can be useful to resend all data.

Fig. A-13 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.

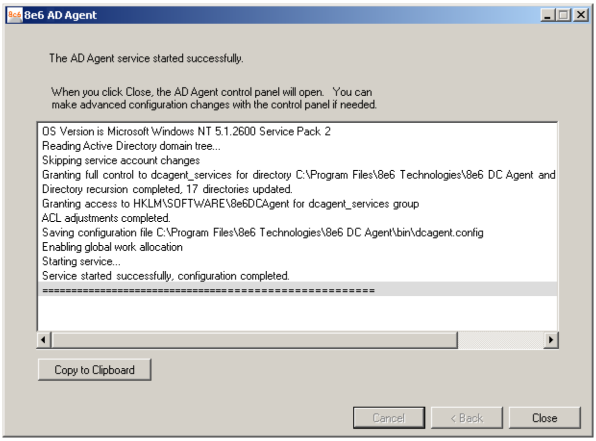
c. **Port** - By default, “26267” displays for the R3000’s port. This port number should only be changed if the R3000 is using a different port number.

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.

5. 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:



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
Granting full control to dcagent_services for directory C:\Program Files\8e6 Technologies\8e6 DC Agent and
Directory recursion completed, 17 directories updated.
Granting access to HKLM\SOFTWARE\8e6DCAgent for dcagent_services group
ACL adjustments completed.
Saving configuration file C:\Program Files\8e6 Technologies\8e6 DC Agent\bin\dcagent.config
Enabling global work allocation
Starting service...
Service started successfully, configuration completed.
======================================================
```

Fig. A-14 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.*

6. 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-15).

***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.*

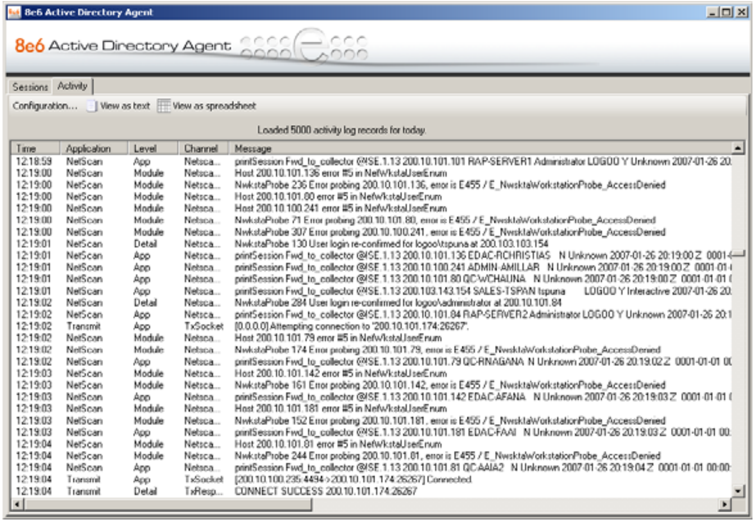
Use the Active Directory Agent console

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:



Loaded 5000 activity log records for today.

```
Time      Application  Level   Channel   Message
12:18:59  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.101 RAP-SERVER1 Administrator LOGOO Y Unknown 2007-01-26 20.
12:19:00  NetScan      Module  Netsca...  Host 200.10.101.136 error #5 in NetWkstaUserEnum
12:19:00  NetScan      Module  Netsca...  NwkstaProbe 236 Error probing 200.10.101.136, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
12:19:00  NetScan      Module  Netsca...  Host 200.10.101.80 error #5 in NetWkstaUserEnum
12:19:00  NetScan      Module  Netsca...  Host 200.10.100.241 error #5 in NetWkstaUserEnum
12:19:00  NetScan      Module  Netsca...  NwkstaProbe 71 Error probing 200.10.101.80, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
12:19:00  NetScan      Module  Netsca...  NwkstaProbe 307 Error probing 200.10.100.241, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
12:19:01  NetScan      Detail  Netsca...  NwkstaProbe 130 User login re-confirmed for logoo\tspuna at 200.103.103.154
12:19:01  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.136 EDAC-RCHRISTIAS   N Unknown 2007-01-26 20:19:00Z  0001-(
12:19:01  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.100.241 ADMIN-AMILLAR   N Unknown 2007-01-26 20:19:00Z  0001-01-(
12:19:01  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.80 QC-WCHAUNA   N Unknown 2007-01-26 20:19:00Z  0001-01-01 (
12:19:01  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.103.143.154 SALES-TSPAN tspuna      LOGOO Y Interactive 2007-01-26 20.
12:19:02  NetScan      Detail  Netsca...  NwkstaProbe 284 User login re-confirmed for logoo\administrator at 200.10.101.84
12:19:02  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.84 RAP-SERVER2 Administrator LOGOO Y Unknown 2007-01-26 20:1
12:19:02  Transmit     App     TxSocket   [0.0.0.0] Attempting connection to "200.10.101.174:26267".
12:19:02  NetScan      Module  Netsca...  Host 200.10.101.79 error #5 in NetWkstaUserEnum
12:19:02  NetScan      Module  Netsca...  NwkstaProbe 174 Error probing 200.10.101.79, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
12:19:02  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.79 QC-RNAGANA  N Unknown 2007-01-26 20:19:02Z  0001-01-01 00
12:19:03  NetScan      Module  Netsca...  Host 200.10.101.142 error #5 in NetWkstaUserEnum
12:19:03  NetScan      Module  Netsca...  NwkstaProbe 161 Error probing 200.10.101.142, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
12:19:03  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.142 EDAC-AFANA   N Unknown 2007-01-26 20:19:03Z  0001-01-01 (
12:19:03  NetScan      Module  Netsca...  Host 200.10.101.181 error #5 in NetWkstaUserEnum
12:19:03  NetScan      Module  Netsca...  NwkstaProbe 152 Error probing 200.10.101.181, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
12:19:03  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.181 EDAC-FAAI   N Unknown 2007-01-26 20:19:03Z  0001-01-01 00:
12:19:04  NetScan      Module  Netsca...  Host 200.10.101.81 error #5 in NetWkstaUserEnum
12:19:04  NetScan      Module  Netsca...  NwkstaProbe 244 Error probing 200.10.101.81, error is E455 / E_NwsktaWorkstationProbe_AccessDenied
12:19:04  NetScan      App     Netsca...  printSession Fwd_to_collector @!SE.1.13 200.10.101.81 QC-AAIA2   N Unknown 2007-01-26 20:19:04Z  0001-01-01 00:00:
12:19:04  Transmit     App     TxSocket   [200.10.100.235:4494->200.10.101.174:26267] Connected.
12:19:04  Transmit     Detail  TxResp...  CONNECT SUCCESS 200.10.101.174:26267
```

Fig. A-15 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, right-click 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.

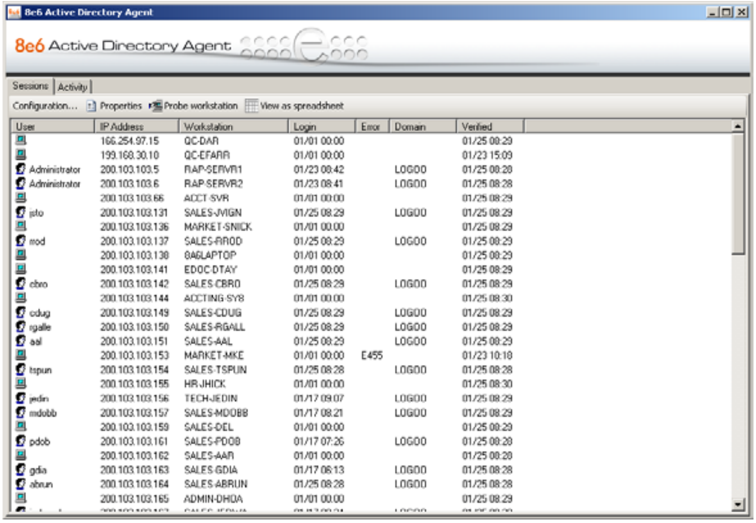
***NOTE**: Any record that displays in red text indicates an error on the server. All errors reported in this log will be sent in a daily email message to the designated administrator (see the Notifications page Active Directory Agent Configuration window).*

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:



User	IP Address	Workstation	Login	Error	Domain	Verified
	166.254.97.15	QC-DAR	01/01 00:00			01/25 08:29
	199.168.30.10	QC-EFARR	01/01 00:00			01/23 15:09
Administrator	200.103.103.5	RAP-SERVR1	01/23 08:42		LOGOO	01/25 08:28
Administrator	200.103.103.6	RAP-SERVR2	01/23 08:41		LOGOO	01/25 08:28
	200.103.103.66	ACCT-SVR	01/01 00:00			01/25 08:29
jsto	200.103.103.131	SALES-JVIGN	01/25 08:29		LOGOO	01/25 08:29
	200.103.103.136	MARKET-SNICK	01/01 00:00			01/25 08:29
rrod	200.103.103.137	SALES-RROD	01/25 08:29		LOGOO	01/25 08:29
	200.103.103.138	8AGLAPTOP	01/01 00:00			01/25 08:29
	200.103.103.141	EDOC-DTAY	01/01 00:00			01/25 08:29
cbro	200.103.103.142	SALES-CBRO	01/25 08:29		LOGOO	01/25 08:29
	200.103.103.144	ACCTING-SY8	01/01 00:00			01/25 08:30
cdug	200.103.103.149	SALES-CDUG	01/25 08:29		LOGOO	01/25 08:29
rgalle	200.103.103.150	SALES-RGALL	01/25 08:29		LOGOO	01/25 08:29
aal	200.103.103.151	SALES-AAL	01/25 08:29		LOGOO	01/25 08:29
	200.103.103.153	MARKET-MKE	01/01 00:00	E455		01/23 10:18
tspun	200.103.103.154	SALES-TSPUN	01/25 08:28		LOGOO	01/25 08:28
	200.103.103.155	HR-JHICK	01/01 00:00			01/25 08:30
jedin	200.103.103.156	TECH-JEDIN	01/17 09:07		LOGOO	01/25 08:29
mdobb	200.103.103.157	SALES-MDOBB	01/17 08:21		LOGOO	01/25 08:29
	200.103.103.159	SALES-DEL	01/01 00:00			01/25 08:29
pdob	200.103.103.161	SALES-PDOB	01/17 07:26		LOGOO	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		LOGOO	01/25 08:28
abrun	200.103.103.164	SALES-ABRUN	01/25 08:28		LOGOO	01/25 08:28
	200.103.103.165	ADMIN-DHDA	01/01 00:00			01/25 08:29

Fig. A-16 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.m86security.com/software/8e6/hlp/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:

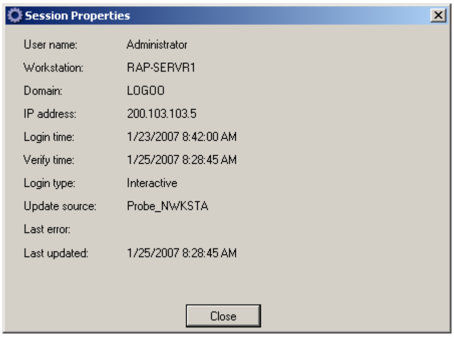
   - Double-click the record in the session table to open the Session Properties pop-up window

     or

   - Click the record in the session table, and then click the **Properties** button to open the Session Properties pop-up 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:



User name: Administrator
Workstation: RAP-SERVR1
Domain: LOGOO
IP address: 200.103.103.5
Login time: 1/23/2007 8:42:00 AM
Verify time: 1/25/2007 8:28:45 AM
Login type: Interactive
Update source: Probe_NWKSTA
Last error:
Last updated: 1/25/2007 8:28:45 AM

Fig. A-17 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.

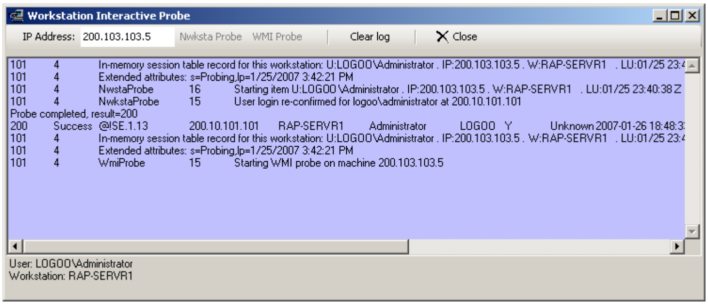
Workstation Interactive Probe window

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 Address: 200.103.103.5

```
101     4       In-memory session table record for this workstation: U:LOGOO\Administrator . IP:200.103.103.5 . W:RAP-SERVR1   . LU:01/25 23:4
101     4       Extended attributes: s=Probing,lp=1/25/2007 3:42:21 PM
101     4       NwstaProbe      16      Starting item U:LOGOO \Administrator . IP:200.103.103.5 . W:RAP-SERVR1   . LU:01/25 23:40:38 Z
101     4       NwkstaProbe     15      User login re-confirmed for logoo\administrator at 200.10.101.101
Probe completed, result=200
200     Success @!SE.1.13       200.10.101.101   RAP-SERVR1      Administrator       LOGOO   Y        Unknown 2007-01-26 18:48:3
101     4       In-memory session table record for this workstation: U:LOGOO\Administrator . IP:200.103.103.5 . W:RAP-SERVR1   . LU:01/25 23:4
101     4       Extended attributes: s=Probing,lp=1/25/2007 3:42:21 PM
101     4       WmiProbe        15      Starting WMI probe on machine 200.103.103.5
```

User: LOGOO\Administrator
Workstation: RAP-SERVR1

Fig. A-18 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.

1. Click **Configuration** on either the Session tab or Activity tab to open the Active Directory Agent Configuration window:

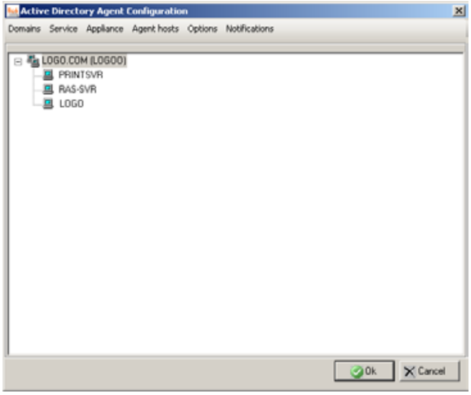


Fig. A-19 Primary host Configuration, Domains

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.*

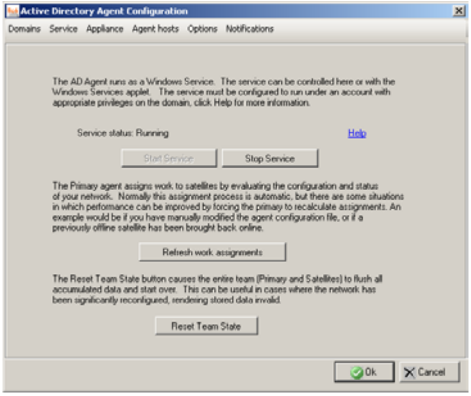
For satellite hosts, fields in all pages display greyed-out. The following message displays at the bottom of the window on all pages except the Service page: "These settings cannot be modified because the service mode for this machine is set to 'satellite'. The primary server (server name) can be used to make team-wide configuration".

3. 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:



The AD Agent runs as a Windows Service. The service can be controlled here or with the Windows Services applet. The service must be configured to run under an account with appropriate privileges on the domain, click Help for more information.

Service status: Running

The Primary agent assigns work to satellites by evaluating the configuration and status of your network. Normally this assignment process is automatic, but there are some situations in which performance can be improved by forcing the primary to recalculate assignments. An example would be if you have manually modified the agent configuration file, or if a previously offline satellite has been brought back online.

The Reset Team State button causes the entire team (Primary and Satellites) to flush all accumulated data and start over. This can be useful in cases where the network has been significantly reconfigured, rendering stored data invalid.

Fig. A-20 Primary host Configuration, Service

The Server status displays to indicate the status of AD Agent on the current machine: Running, StopPending, Stop, StartPending.

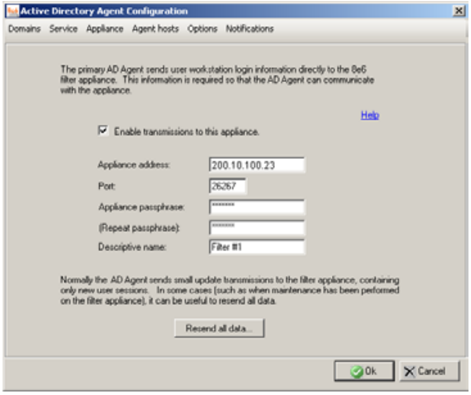
2. Perform any of the following actions:

- **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:



The primary AD Agent sends user workstation login information directly to the 8e6 filter appliance. This information is required so that the AD Agent can communicate with the appliance.

☑ Enable transmissions to this appliance.

Appliance address: 200.10.100.23
Port: 26267
Appliance passphrase: ********
(Repeat passphrase): ********
Descriptive name: Filter #1

Normally the AD Agent sends small update transmissions to the filter appliance, containing only new user sessions. In some cases (such as when maintenance has been performed on the filter appliance), it can be useful to resend all data.

Fig. A-21 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.

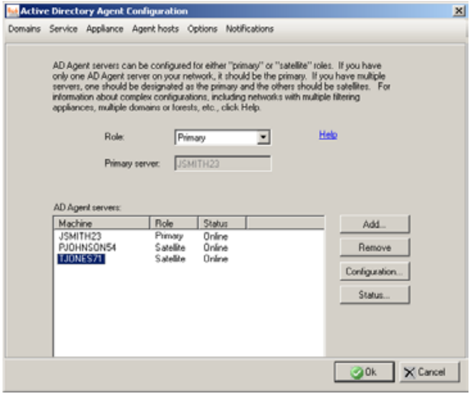
2. If necessary, click the following objects on a primary host to perform the specified actions:

   - “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:



AD Agent servers can be configured for either "primary" or "satellite" roles. If you have only one AD Agent server on your network, it should be the primary. If you have multiple servers, one should be designated as the primary and the others should be satellites. For information about complex configurations, including networks with multiple filtering appliances, multiple domains or forests, etc., click Help.

Role: Primary

Primary server: JSMITH23

AD Agent servers:

Machine	Role	Status
JSMITH23	Primary	Online
PJOHNSON54	Satellite	Online
TJONES71	Satellite	Online

Fig. A-22 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:

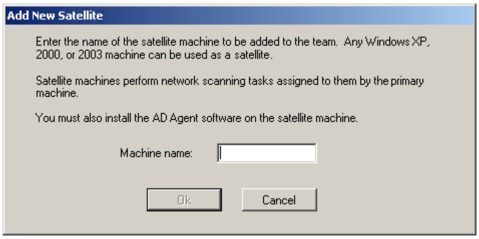
   - **Add** - On a primary host server, clicking this button opens a dialog box in which a new satellite is set up and added to the list box.
   - **Remove** - On a primary host server, selecting a satellite in the AD Agent servers list box and clicking this activated button removes the satellite from 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:

Fig. A-23 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

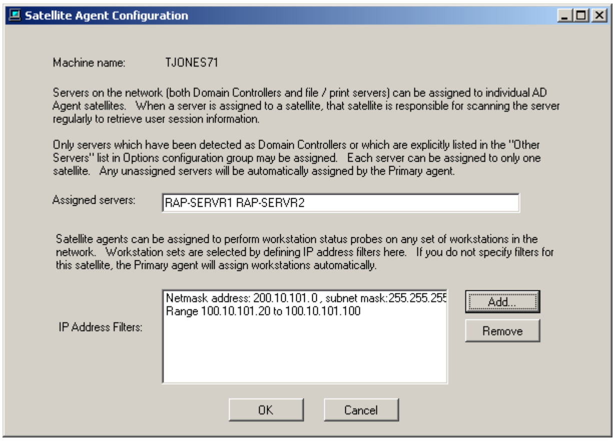
On a primary host server:

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:



Satellite Agent Configuration

Machine name: TJONES71

Servers on the network (both Domain Controllers and file / print servers) can be assigned to individual AD Agent satellites. When a server is assigned to a satellite, that satellite is responsible for scanning the server regularly to retrieve user session information.

Only servers which have been detected as Domain Controllers or which are explicitly listed in the "Other Servers" list in Options configuration group may be assigned. Each server can be assigned to only one satellite. Any unassigned servers will be automatically assigned by the Primary agent.

Assigned servers: RAP-SERVR1 RAP-SERVR2

Satellite agents can be assigned to perform workstation status probes on any set of workstations in the network. Workstation sets are selected by defining IP address filters here. If you do not specify filters for this satellite, the Primary agent will assign workstations automatically.

IP Address Filters:
Netmask address: 200.10.101.0 , subnet mask:255.255.255
Range 100.10.101.20 to 100.10.101.100

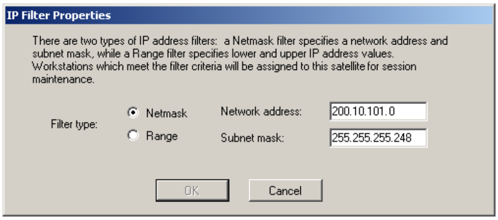
Fig. A-24 Satellite Agent Configuration

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:



There are two types of IP address filters: a Netmask filter specifies a network address and subnet mask, while a Range filter specifies lower and upper IP address values. Workstations which meet the filter criteria will be assigned to this satellite for session maintenance.

Filter type: ● Netmask ○ Range

Network address: 200.10.101.0

Subnet mask: 255.255.255.248

Fig. A-25 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:

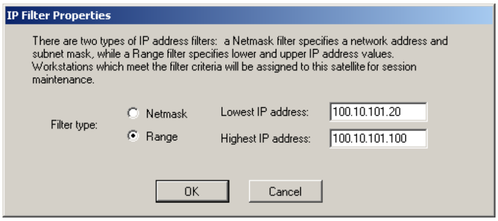
   - To specify a subnet to scan, choose the default “Netmask” and make the following entries:

     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:



There are two types of IP address filters: a Netmask filter specifies a network address and subnet mask, while a Range filter specifies lower and upper IP address values. Workstations which meet the filter criteria will be assigned to this satellite for session maintenance.

Filter type: ○ Netmask ● Range

Lowest IP address: 100.10.101.20

Highest IP address: 100.10.101.100

Fig. A-26 IP Filter Properties dialog box, Range

a. Enter the **Lowest IP address** in the range.

b. Enter the **Highest IP address** in the range.

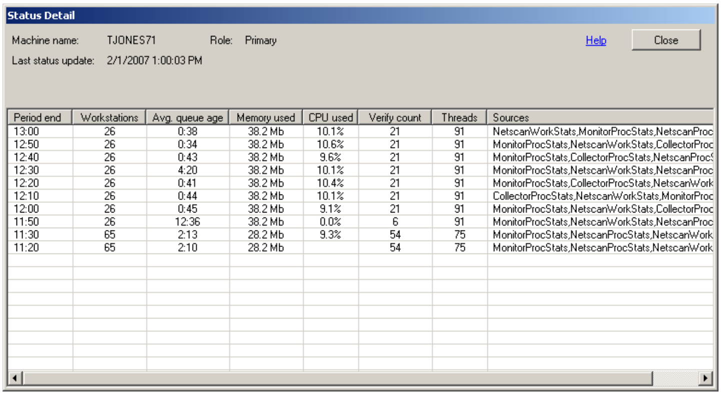
c. Click **OK** to close the dialog box and to display your entries in the IP Address Filters list box of the Satellite Agent Configuration dialog box.

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:



Machine name: TJONES71 Role: Primary

Last status update: 2/1/2007 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,NetscanProc
12:50	26	0:34	38.2 Mb	10.6%	21	91	MonitorProcStats,NetscanWorkStats,CollectorProc
12:40	26	0:43	38.2 Mb	9.6%	21	91	MonitorProcStats,CollectorProcStats,NetscanProcS
12:30	26	4:20	38.2 Mb	10.1%	21	91	MonitorProcStats,NetscanWorkStats,NetscanProc
12:20	26	0:41	38.2 Mb	10.4%	21	91	MonitorProcStats,CollectorProcStats,NetscanWork
12:10	26	0:44	38.2 Mb	10.1%	21	91	CollectorProcStats,NetscanWorkStats,MonitorProc
12:00	26	0:45	38.2 Mb	9.1%	21	91	MonitorProcStats,NetscanWorkStats,CollectorProc
11:50	26	12:36	38.2 Mb	0.0%	6	91	MonitorProcStats,NetscanWorkStats,NetscanProc
11:30	65	2:13	28.2 Mb	9.3%	54	75	MonitorProcStats,NetscanProcStats,NetscanWork
11:20	65	2:10	28.2 Mb		54	75	MonitorProcStats,NetscanProcStats,NetscanWork

Fig. A-27 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:

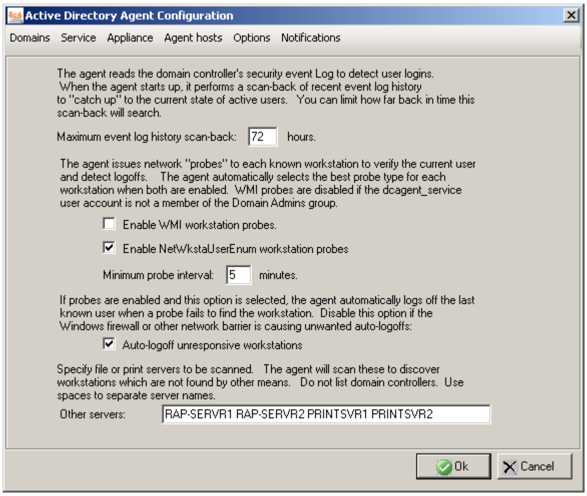
- Period end - the time period (using the HH:MM military time format) of each 10-minute interval in which servers/machines were scanned. The most recent 10-minute interval displays as the first record among the rows of records.
- Workstations - the number of workstations included in the local session 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 five-minute 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:



The agent reads the domain controller's security event Log to detect user logins. When the agent starts up, it performs a scan-back of recent event log history to "catch up" to the current state of active users. You can limit how far back in time this scan-back will search.

Maximum event log history scan-back: 72 hours.

The agent issues network "probes" to each known workstation to verify the current user and detect logoffs. The agent automatically selects the best probe type for each workstation when both are enabled. WMI probes are disabled if the dcagent_service user account is not a member of the Domain Admins group.

☐ Enable WMI workstation probes.

☑ Enable NetWkstaUserEnum workstation probes

Minimum probe interval: 5 minutes.

If probes are enabled and this option is selected, the agent automatically logs off the last known user when a probe fails to find the workstation. Disable this option if the Windows firewall or other network barrier is causing unwanted auto-logoffs:

☑ Auto-logoff unresponsive workstations

Specify file or print servers to be scanned. The agent will scan these to discover workstations which are not found by other means. Do not list domain controllers. Use spaces to separate server names.

Other servers: RAP-SERVR1 RAP-SERVR2 PRINTSVR1 PRINTSVR2

Fig. A-28 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.*

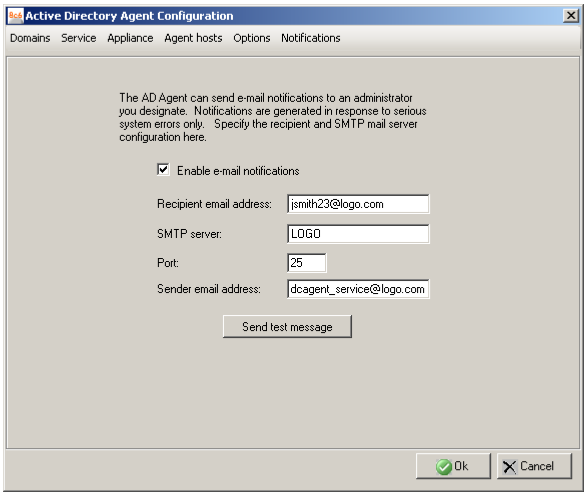
- “Enable NetWkstaUserEnum workstation probes”: By default, this probe process is selected to run.
- **Minimum probe interval**: By default, *5* minutes displays as the interval of time in which the selected probe type(s) will probe workstations.
- “Auto-logoff unresponsive workstations”: By default, 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:



The AD Agent can send e-mail notifications to an administrator you designate. Notifications are generated in response to serious system errors only. Specify the recipient and SMTP mail server configuration here.

☑ Enable e-mail notifications

Recipient email address: jsmith23@logo.com

SMTP server: LOGO

Port: 25

Sender email address: dcagent_service@logo.com

Fig. A-29 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: 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

1. From the console of the LDAP server, go to Start > Programs > Administrative Tools > Certification Authority to open the Certification Authority window:

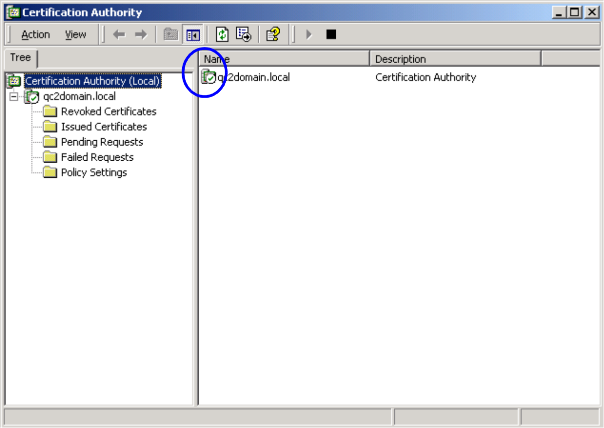
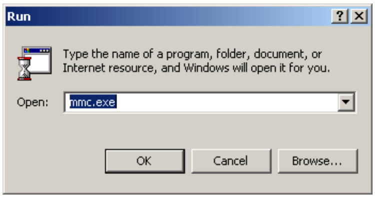


Fig. B-1 Certfication Authority window

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. B-1).

Locate Certificates folder

1. 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:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc.exe

Fig. B-2 Run dialog box

2. Click **OK** to open the Console window:

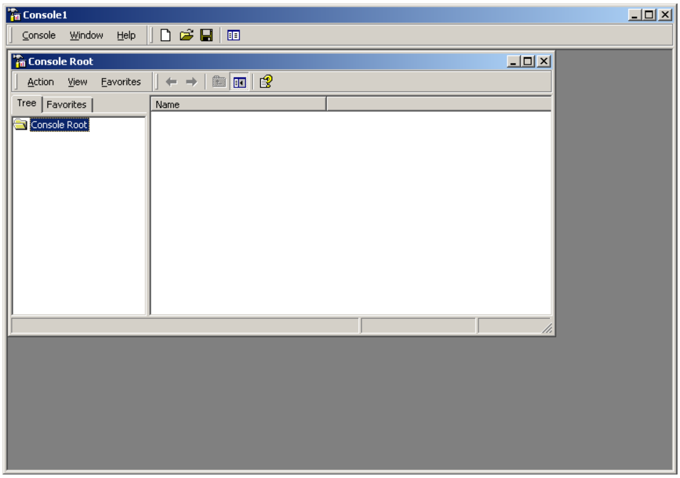
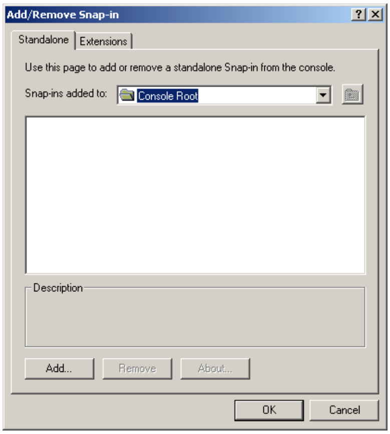


Fig. B-3 Microsoft Console window

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:

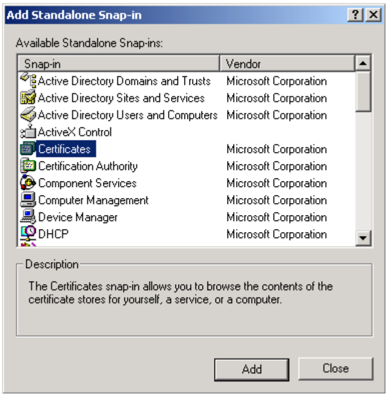


Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Fig. B-4 Add/Remove Snap-in

4. Click **Add** to open the Add Standalone Snap-in dialog box:



Available Standalone Snap-ins:

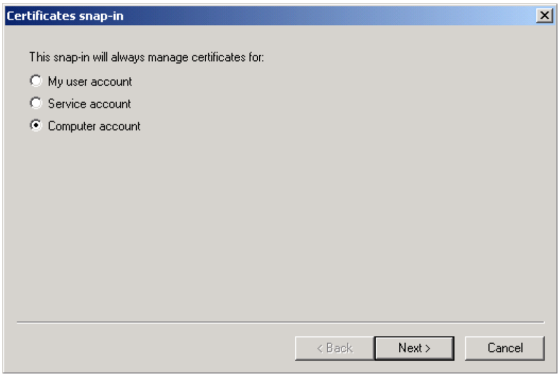
Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
DHCP	Microsoft Corporation

Description

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Fig. B-5 Add Standalone Snap-in

5. Select Certificates, and click **Add** to open the Certificates snap-in wizard dialog box:



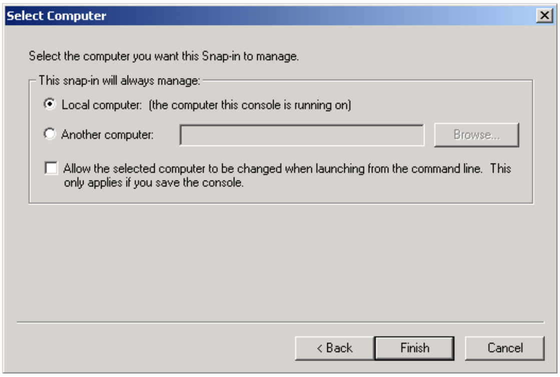
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Fig. B-6 Certificates snap-in dialog box

6. Choose “Computer account”, and click **Next** to go to the Select Computer wizard page:



Select Computer

Select the computer you want this Snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)
○ Another computer:

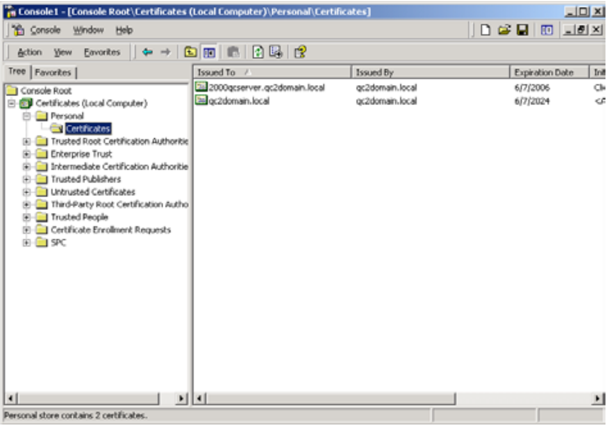
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Fig. B-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.

8. 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:



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued By	Expiration Date	Int
2000qcserver.qc2domain.local	qc2domain.local	6/7/2006	Cl
qc2domain.local	qc2domain.local	6/7/2024	<A

Personal store contains 2 certificates.

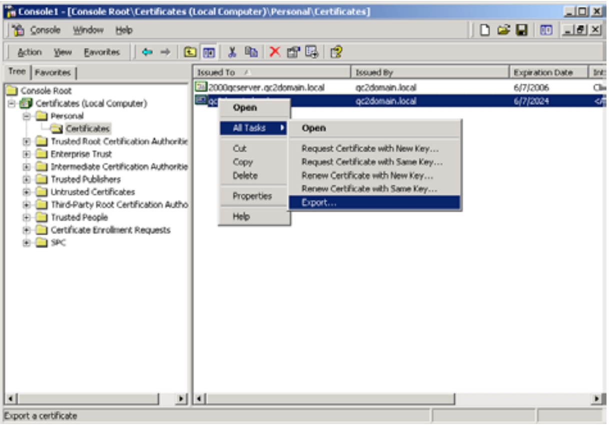
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authoritie
Enterprise Trust
Intermediate Certification Authoritie
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Autho
Trusted People
Certificate Enrollment Requests
SPC

Fig. B-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:



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

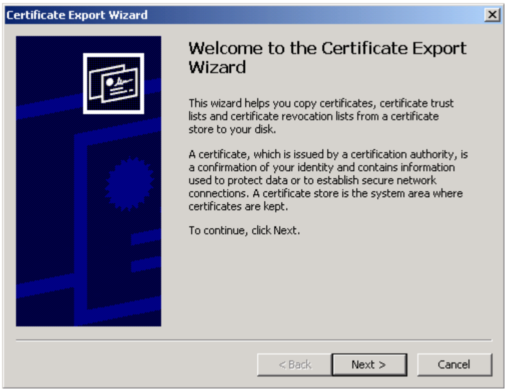
Issued To	Issued By	Expiration Date	Int
2000qcserver.qc2domain.local	qc2domain.local	6/7/2006	Cl
qc	qc2domain.local	6/7/2024	<A

Export a certificate

Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authoritie
Enterprise Trust
Intermediate Certification Authoritie
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Autho
Trusted People
Certificate Enrollment Requests
SPC
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Request Certificate with Same Key...
Renew Certificate with New Key...
Renew Certificate with Same Key...
Export...

Fig. B-9 Select the certificate to be exported

This action launches the Certificate Export Wizard:



Welcome to the Certificate Export Wizard

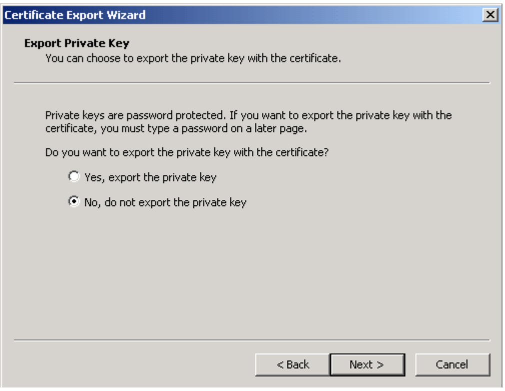
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Fig. B-10 Certificate Export Wizard

3. Click **Next** to go to the Export Private Key page of the wizard:



Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

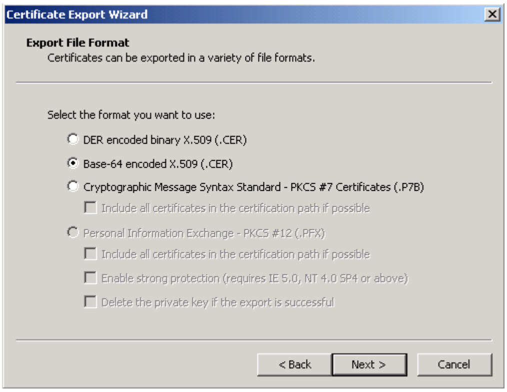
Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Fig. B-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:



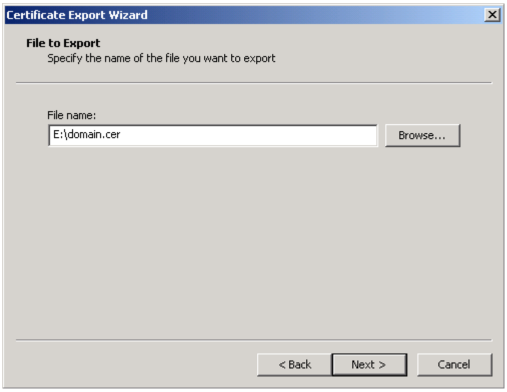
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ 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. B-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:

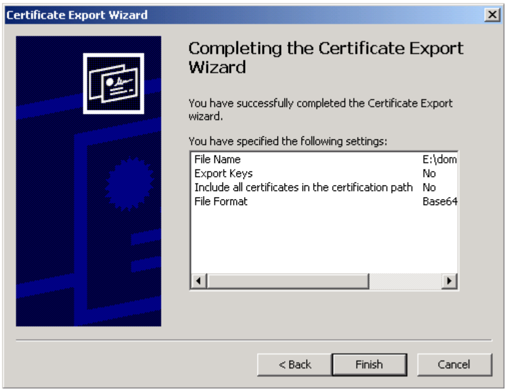


File to Export
Specify the name of the file you want to export

File name:
E:\domain.cer

Fig. B-13 File to Export

6. 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:



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	E:\dom
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

Fig. B-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):

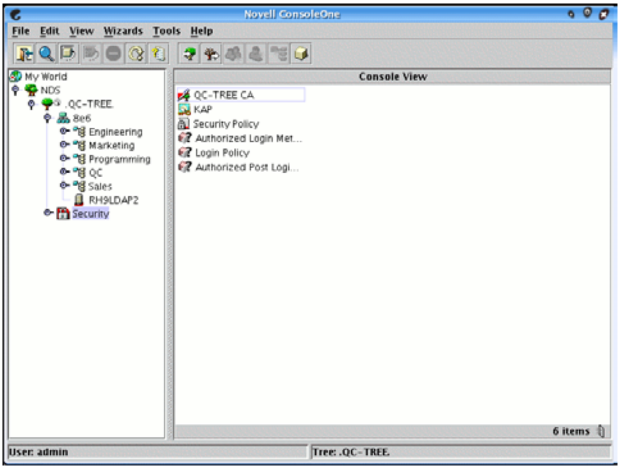
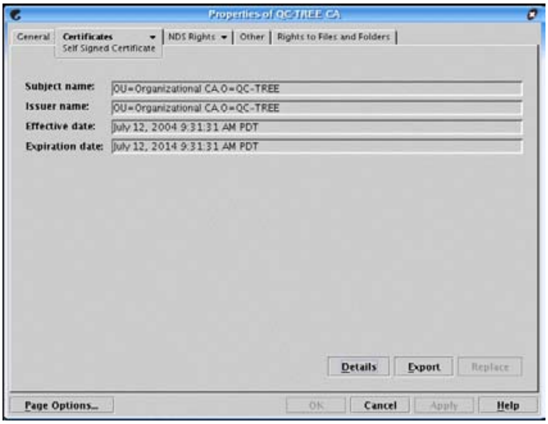


Fig. B-15 Novell Console window

2. Find the tree's folder and right-click it to open the pop-up menu. Select Properties to open the Properties dialog box:

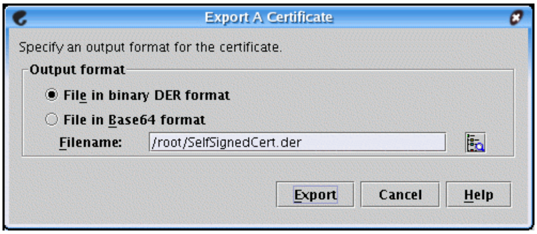


Subject name: OU=Organizational CA.O=QC-TREE
Issuer name: OU=Organizational CA.O=QC-TREE
Effective date: July 12, 2004 9:31:31 AM PDT
Expiration date: July 12, 2014 9:31:31 AM PDT

Fig. B-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:



Export A Certificate

Specify an output format for the certificate.

Output format

● File in binary DER format

○ File in Base64 format

Filename: /root/SelfSignedCert.der

Fig. B-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 C: 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 LDAP Browser window

In this scenario, a query is performed in the LDAP 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/ ldapgroup**
2. Find the subdirectory bearing the name of the LDAP domain, and change the current directory to that subdirectory.
3. Open the file ”ldapobjectdef.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 D: PROFILE FORMAT AND RULES

The file with filtering profiles you upload to the server must be set up in a specified format, with one complete profile per line. This format will differ depending on the type of profiles in the file: Workstation, user, group, container, or quota.

Each non-quota filtering profile in the file must contain the following items:

1. The workstation name, username, group name, or container 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).

An LDAP quota filtering profile is set up in the following format:

1. Enter the workstation name, username, group name, or container name.
2. Press the Tab key on your keyboard to leave a space.
3. Enter the quota string.

Username Formats

NOTE*: For examples of valid username entries, see File Format: Rules and Examples in this appendix, or go to* ***http://www.m86security.com/software/8e6/hlp/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)
  M= Set the defined port number(s) to trigger a warn message
  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:**

  Category command codes must be entered in the following order: J, R, M, I. “PASSED” should either be entered after J, R, or M, or after a string of category codes following J, R, or M.

  J = Positioned before the category/categories defined as "always allowed."

  R = Positioned before the category/categories defined as "blocked."

  M = Positioned before the category/categories defined as containing URLs potentially against the organization’s policies, and accompanied by a warning message.

  I = Positioned at the end of a profile string, indicating that all other categories should “pass.”

  PASSED = When positioned at the end of a string of categories or after a category command code, this code indicates that unidentified categories will follow suit with categories defined by that code: J (pass), R (block), or M (receive warning message).

- **Category Codes:**

  For the list of category codes (short names) and their corresponding descriptions (long names), go to **http://www.m86security.com/software/8e6/hlp/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.m86security.com/resources/database-categories.asp

- **Filter Option codes:**

  - 0x1 = Exception URL Query (always enabled)
  - 0x2 = X Strikes Blocking
  - 0x4 = Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement
  - 0x100 = Search Engine Keyword
  - 0x200 = URL Keyword
  - 0x1000=Extend URL Keyword Filter Control

***NOTE**: To enable multiple filter codes, add the codes together—i.e. 1 + 2 + 4 + 100 + 200 + 1000 = 1307—which means that **0x1307** should be entered at the end of the profile string. To disable all filter codes, enter **0x1** at the end of the profile string.*

- **Quota format**

  A separate file—apart from the LDAP profile file—must be used in order to include quotas in the LDAP group/ user profile. In this file, each quota profile must be entered on a separate line in the following manner:

  1. Type in the username.
  2. Press the Tab key on your keyboard to leave a space.
  3. Type in the quota string using this format: Overall Quota minutes, a comma (**,**), the first library category code, a colon (**:**), the number of quota minutes, and a comma between each quota.

***NOTE**: See **http://www.m86security.com/software/8e6/hlp/r3000help/files/2group_textfile_format_ldap.html** for examples of LDAP filtering profile entries. Quota profile entries are included in these pages.*

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 “0x1” if no filter options will be enabled.
- If quotas are to be used in filtering profiles, these must be entered in a separate file from the LDAP profile file.

LDAP Profile List Format and Rules

When setting up the “ldapwrkstnprofile.conf” file, “ldapuserprofile.conf” file, “ldapgroupprofile.conf” file, or “ldapcontainerprofile.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 (,). “0x1” should be placed at the end of a profile string without any filter options enabled.

Workstation profile list format

Here are examples of workstation profile entries in an ldapwrkstnprofile.conf file:

```
CN=R3KWRK1, CN=Computers, DC=logo, DC=net; R
      21 A, J R KDPORN GPORN M PASSED I,1, , 0x1
CN=WIN2000-79AHM, OU=Domain Controllers,
      DC=logo, DC=net; Rule0, , 0x1306
```

***NOTE**: The DN format must contain the workstation name and LDAP 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:

- profile for a workstation named “R3KWRK1”, LDAP group “Computers”, domain “logo”, DNS suffix “.net”: Block port 21 and Filter all other ports, Block Child

Pornography and Pornography/Adult Content, Warn on Uncategorized URLs, and Pass all other categories, use filter mode 1, use redirect URL http://www.cnn.com in place of the standard block page, no filter options enabled.

- profile for a workstation named “WIN2000-79AHM”, organizational unit “Domain Controllers”, domain “logo”, DNS suffix “.net”: Block all ports, use minimum filtering level, use filter mode 1, use standard block page, enable all filter options.

User profile list format

Here are examples of user profile entries in an ldapuserprofile.conf file:

```
CN=Jane Doe, CN=Users, DC=qc, DC=local; R 21 A, J
      R KDPORN GPORN M PASSED I,1, , 0x1
CN=Public\, Joe Q., OU=Users, OU=Sales, DC=qc,
      DC=local; Rule0, , 0x1306
```

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:

- profile for a user with username “Jane Doe”, user group “Users”, domain “qc”, DNS suffix “.local”: Block port 21 and Filter all other ports, Block Child Pornography and Pornography/Adult Content, Warn on Uncategorized URLs, and Pass all other categories, use filter mode 1, use redirect URL http://www.cnn.com in place of the standard block page, no filter options enabled.

- profile for a user with username “Public\, Joe Q.”, organizational units “Users” and “Sales”, domain “qc”, DNS suffix “.local”: Block all ports, use minimum filtering level, use filter mode 1, use standard block page, enable all filter options.

Group profile list format

Here is an example of a group profile entry in an ldapgroupprofile.conf file:

CN=Sales, CN=Users, DC=qc, DC=local; Rule1, 1, http://www.cnn.com, 0x1

***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:

- 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, no filter options enabled.

Container profile list format

A container profile entry in an ldapcontainerprofile.conf file will be similar to entries made in workstation, user, and group profile files, however the Distinguished Name will be slightly different, based on how containers are set up in your organization.

LDAP Quota Format and Rules

When setting up the “quota.conf” file, each entry must consist of the Distinguished Name (DN), a Tab space, and quota criteria. A zero (0) should be used if no Overall Quota minutes are included. For example:

```
CN=Admin, CN=Users, DC=tc, DC=local    0,
   PARNML:15, RELIG:15
CN=Sales, CN=Reps, DC=tc, DC=local    10,
   GNEWS:5, SPORTS:5, TRAFIC:10
```

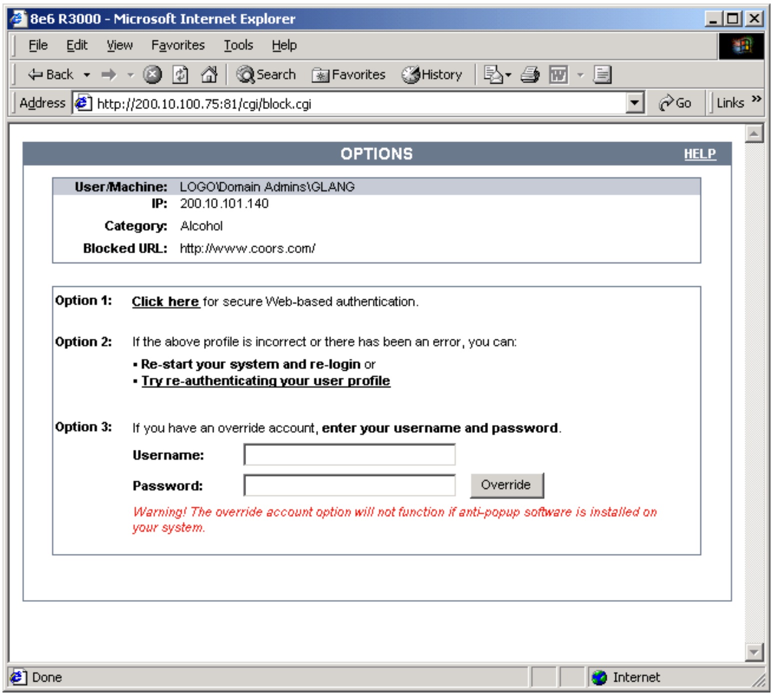
NOTE*: The DN format must contain the group name—and, if applicable—user group "CN" ("common name") attribute type, and the domain and DNS suffix "DC" ("domain component") attribute type. The "OU" ("organizational unit") attribute type also can be included. Each attribute type should be followed by an equals sign (=), and separated by a comma (,).*

When translated, these strings of code mean:

- quota profile for “Admin”, user group “Users”, domain “tc”, DNS suffix “.local”: No Overall Quota minutes, and 15 quota minutes for each category listed.
- quota profile for “Sales”, user group “Reps”, domain “tc”, DNS suffic “.local”: 10 Overall Quota minutes, 5 quota minutes for the first two categories listed, and 10 quota minutes for the last category listed.

APPENDIX E: 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:


8e6 R3000 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://200.10.100.75:81/cgi/block.cgi
Go Links
Done
Internet

OPTIONS HELP

User/Machine: LOGO\Domain Admins\GLANG
IP: 200.10.101.140
Category: Alcohol
Blocked URL: http://www.coors.com/

Option 1: Click here 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
- Try re-authenticating your user profile

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.

Fig. E-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. E-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:

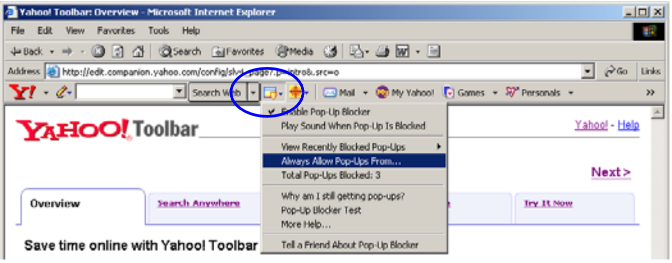
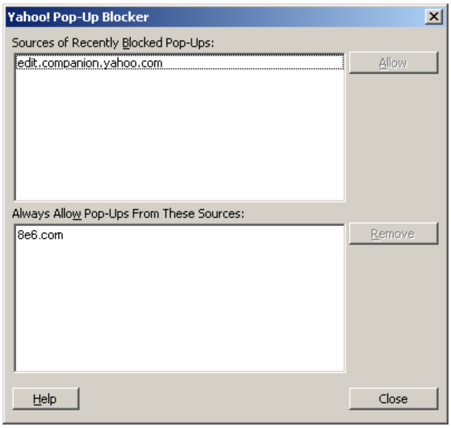

Yahoo! Toolbar: Overview - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://edit.companion.yahoo.com/config/slv4_page?.p=intro&.src=o
Go Links
Search Web
Mail My Yahoo! Games Personals
✓ Enable Pop-Up Blocker
Play Sound When Pop-Up Is Blocked
View Recently Blocked Pop-Ups
Always Allow Pop-Ups From...
Total Pop-Ups Blocked: 3
Why am I still getting pop-ups?
Pop-Up Blocker Test
More Help...
Tell a Friend About Pop-Up Blocker
YAHOO! Toolbar
Yahoo! - Help
Next >
Overview
Search Anywhere
Try It Now
Save time online with Yahoo! Toolbar

Fig. E-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:



Sources of Recently Blocked Pop-Ups:
edit.companion.yahoo.com

Always Allow Pop-Ups From These Sources:
8e6.com

Fig. E-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.

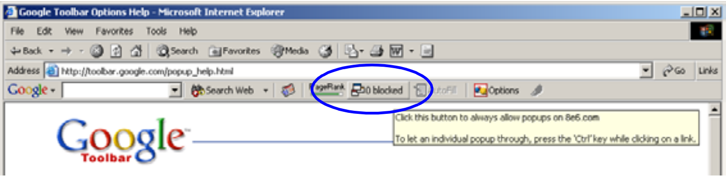
Google Toolbar Pop-up Blocker

If pop-up blocking is enabled

1. In the Options page (see Fig. E-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:

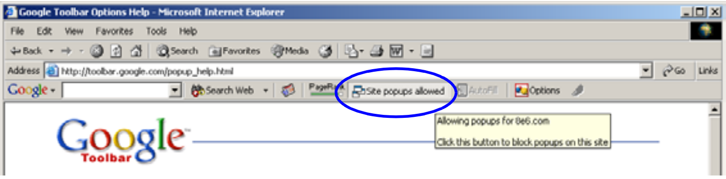


Click this button to always allow popups on 8e6.com

To let an individual popup through, press the 'Ctrl' key while clicking on a link.

Fig. E-4 # blocked icon enabled

Clicking this icon toggles to the Site pop-ups allowed icon, adding the override account window to your white list:



Allowing popups for 8e6.com

Click this button to block popups on this site

Fig. E-5 Site pop-ups allowed icon enabled

AdwareSafe Pop-up Blocker

If pop-up blocking is enabled

1. In the Options page (see Fig. E-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

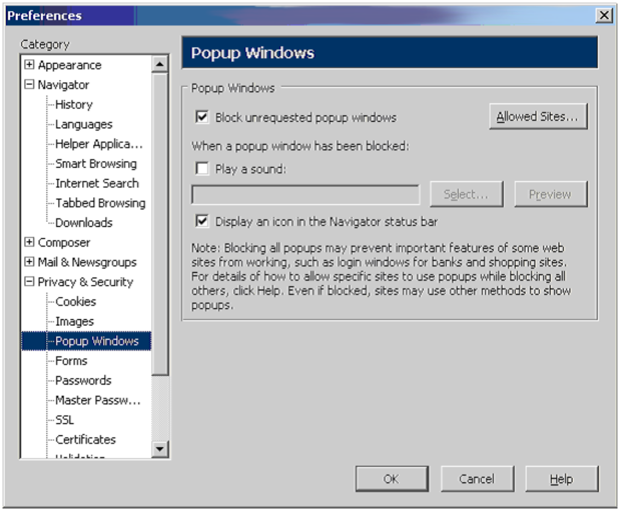
AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

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. E-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:



Popup Windows

Popup Windows

☑ Block unrequested popup windows

When a popup window has been blocked:

□ Play a sound:

☑ Display an icon in the Navigator status bar

Note: Blocking all popups may prevent important features of some web sites from working, such as login windows for banks and shopping sites. For details of how to allow specific sites to use popups while blocking all others, click Help. Even if blocked, sites may use other methods to show popups.

Fig. E-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.

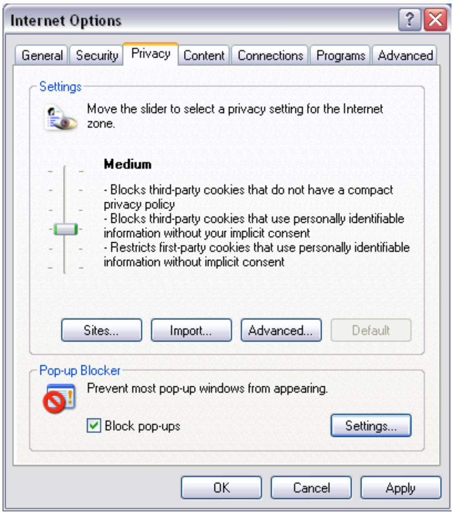
Windows XP SP2 Pop-up Blocker

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:



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☑ Block pop-ups

Fig. E-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 > Pop-up Blocker > Turn On Pop-up Blocker:

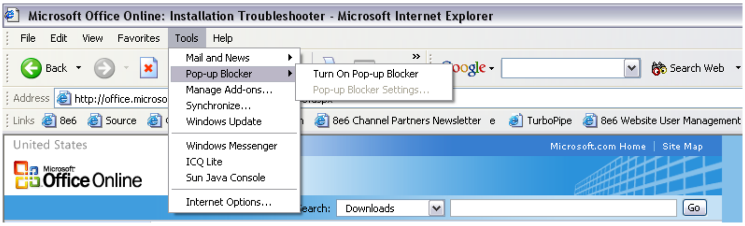


Fig. E-8 Toolbar setup

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

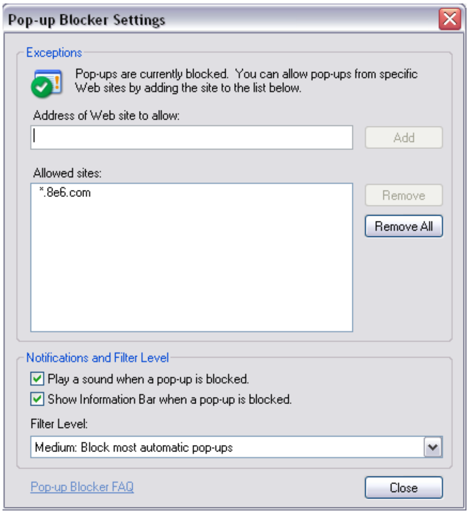
1. In the Options page (see Fig. E-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

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

1. 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:



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:

Allowed sites:
*.8e6.com

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level:
Medium: Block most automatic pop-ups

Fig. E-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. E-1), enter your **Username** and **Password**.
4. Click the **Override** button to open the override account pop-up window.

Use the Information Bar

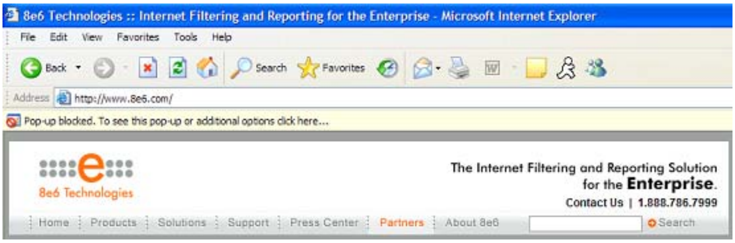
With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

Set up the Information Bar

1. 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. E-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. E-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...”:



8e6 Technologies :: Internet Filtering and Reporting for the Enterprise - Microsoft Internet Explorer

Pop-up blocked. To see this pop-up or additional options click here...

Fig. E-10 Information Bar showing blocked pop-up status

3. Click the Information Bar for settings options:

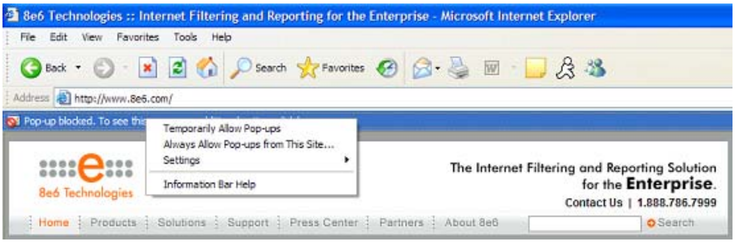
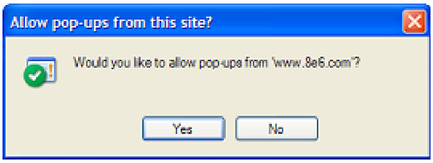

8e6 Technologies :: Internet Filtering and Reporting for the Enterprise - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.8e6.com/
Pop-up blocked. To see this
Temporarily Allow Pop-ups
Always Allow Pop-ups from This Site...
Settings
Information Bar Help
8e6 Technologies
The Internet Filtering and Reporting Solution for the Enterprise.
Contact Us | 1.888.786.7999
Home Products Solutions Support Press Center Partners About 8e6
Search

Fig. E-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 pop-ups from this site?

Would you like to allow pop-ups from 'www.8e6.com'?

Fig. E-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. E-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 F: 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. LDAP is the method used by the R3000.

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 user-name 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 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, LDAP domains, and each member's associated filtering profile. The global administrator configures the R3000, sets up master IP groups and LDAP domains, and performs routine maintenance on the server.

group administrator - An authorized administrator of the network who maintains a master IP group or LDAP domain/group, and sets up and manages members within the group/domain. This administrator also adds and maintains customized library categories for group/domain members.

group name - The name of a group set up for a domain on an Windows Active Directory 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 - The authentication method protocol 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. If the minimum filtering level is set up to block a library category, this setting will override an always allowed setting for that category in a user’s profile. Minimum filtering level settings can be overridden by profile settings made in override accounts, exception URL settings, and use of the “bypass all” Rule setting.

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 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. An override account will bypass settings made in the minimum filtering level.

PDC - A Primary Domain Controller functions as the authentication server on a Windows Active Directory 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 is a type of authentication method protocol.

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.

quota - The number of minutes configured for a passed library category in an end user’s profile that lets him/her access URLs for a specified time before being blocked from further access to that category.

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).

static group - An LDAP group that contains names of its members. (See also “dynamic group”.)

Sub Admin - An LDAP group administrator assigned to a specific domain, group, workstation, member, or container. This group administrator manages the profiles of entities (nodes) assigned to him/her.

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 the LDAP authentication method to give a user a time limit on his/her Internet access to specified library categories.

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 LDAP. Tier 2 uses time-based profiles for the LDAP authentication method, and Tier 3 uses persistent login connections for the LDAP authentication method.

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 or uncategorized URLs when creating a rule, or when setting up a filtering profile. This designation indicates URLs in the library category or uncategorized URLs 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 or an uncategorized URL is requested.

Web-based - An authentication method that uses time-based profiles or persistent login connections.

white list - A list of approved library categories for a specified entity’s filtering profile.

INDEX