



Web Filter Authentication Guide

Version 5.1.00

Publication Date: 29 April 2013

Legal Notice

Copyright © 2013 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained from:

www.trustwave.com/support/

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Part# WF-AUG-130429

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.




Format and Symbols	Meaning
<u>Blue Underline</u>	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
Code	Text in this format indicates computer code or information at a command line.
<i>Italics</i>	Italics are used to denote the name of a published work, the current document, or another document; for text emphasis; or to introduce a new term. In code examples italics indicate a placeholder for values and expressions.
[Square brackets]	In code examples, square brackets indicate optional sections or entries.
	Note: This symbol indicates information that applies to the task at hand.
	Tip: This symbol denotes a suggestion for a better or more productive way to use the product.
	Caution: This symbol highlights a warning against using the product in an unintended manner.

Table of Contents

Legal Notice	ii
Formatting Conventions	iii
1 Introduction	11
1.1 About this Guide	11
1.2 How to Use this Guide	11
1.2.1 Terminology	11
1.3 Filtering Elements	14
1.3.1 Group Types	14
1.3.1.1 Global Group	15
1.3.1.2 IP Groups	15
1.3.1.3 LDAP Domain Groups	15
1.3.2 Filtering Profile Types	16
1.3.2.1 Static Filtering Profiles	17
1.3.2.2 Active Filtering Profiles	18
1.3.3 Filtering Profile Components	18
1.3.3.1 Library Categories	19
1.3.3.2 Service Ports	19
1.3.3.3 Rules	20
1.3.3.4 Minimum Filtering Level	20
1.3.3.5 Filter Settings	20
1.3.4 Filtering Rules	21
1.4 Authentication Solutions	23
1.4.1 LDAP Authentication Protocol	23
1.4.2 Web Filter Authentication Tiers and Options	23
1.4.2.1 Web Filter authentication tiers	23
1.4.2.2 Web Filter authentication options	23
1.4.3 Authentication Solution Compatibility	23
1.4.4 Authentication System Deployment Options	24
1.4.5 Ports for Authentication System Access	24
1.4.6 Configuring Web Filter for Authentication	25
1.4.6.1 Configuration procedures	25
2 Network Setup	29
2.1 Network Requirements	29
2.2 Workstation Requirements	29
2.2.1 Administrator Workstation	29
2.2.2 End User Workstation	29
2.3 Set up the Network for Authentication	30

2.3.1 Specify the operation mode	31
2.3.1.1 Invisible, Router, or Firewall Mode	31
2.3.1.2 Bridge Mode	32
2.3.2 Specify the subnet mask, IP address(es)	32
2.3.2.1 Invisible mode	33
2.3.2.2 Router or firewall mode	33
2.3.3 Enable authentication, specify criteria	34
2.3.3.1 Net use based authentication	35
2.3.3.2 Web-based authentication.	35
2.3.4 Enter network settings for authentication.	37
2.3.5 Create an SSL certificate	38
2.3.5.1 Create, Download a Self-Signed Certificate	39
2.3.5.2 Create, Upload a Third Party Certificate	40
2.3.6 Specify block page settings	43
2.3.6.1 Block Page Authentication.	44
2.3.6.2 Common Customization	48
2.3.6.3 Authentication Form Customization	51
2.3.6.4 Block Page Customization	53
2.4 Set up Group Administrator Accounts.	55
2.4.1 Add Sub Admins to manage nodes	56
2.4.1.1 Add a group administrator account	56
2.4.1.2 Update the group administrator's password	56
2.4.1.3 Delete a group administrator account.	56
2.5 View Log Results	57
3 LDAP Authentication Setup	59
3.1 Create an LDAP Domain	59
3.1.1 Add the LDAP domain	59
3.1.2 Refresh the LDAP branch	59
3.1.3 View, modify, enter LDAP domain details.	60
3.1.3.1 Type	60
3.1.3.2 Group	61
3.1.3.3 User	62
3.1.3.4 Workstation.	63
3.1.3.5 Server.	64
3.1.3.6 SSL.	65
3.1.3.7 Account.	67
3.1.3.8 Alias List	69
3.1.4 Delete a domain	71
3.2 Set up LDAP Domain Nodes	71
3.2.1 Add nodes to the domain tree list	71
3.2.1.1 Perform a basic search	72
3.2.1.2 Options for search results	72
3.2.1.3 Apply a filtering rule to a profile.	72

3.2.1.4 Delete a rule	73
3.2.2 Specify a group's filtering profile priority	73
3.2.3 Manually add a workstation name to the tree.	74
3.2.4 Manually add a user's name to the tree	74
3.2.5 Manually add a group's name to the tree.	75
3.2.6 Upload a file of filtering profiles to the tree	76
4 Manage Nodes	79
4.1 Assign Sub Admin to an LDAP Node.	79
4.2 Create and Maintain Filtering Profiles	81
4.2.1 Add a group member to the tree list	82
4.2.2 View Container Details.	82
4.2.3 Add or maintain a node's profile	83
4.2.3.1 Category Profile	84
4.2.3.2 Redirect URL	86
4.2.3.3 Filter Options.	86
4.2.3.4 YouTube Video Control.	87
4.2.4 Add an Exception URL to the profile	89
4.2.4.1 Valid URL entries	89
4.2.4.2 Add URLs to Block URL or ByPass URL frame	90
4.2.4.3 Remove URLs from Block URL or ByPass URL frame	92
4.2.4.4 Apply settings	93
4.2.5 Create a Time Profile for the node	93
4.2.5.1 Add a Time Profile	94
4.2.6 Set Tier 2, Tier 3 timeout minutes.	97
4.2.7 Remove a node's profile from the tree.	99
4.3 Verify that an LDAP Profile is Active.	99
5 Authentication Deployment	103
5.1 Test Authentication Settings	103
5.1.1 Test Web-based authentication settings.	104
5.1.1.1 Create an IP Group, "test".	104
5.1.1.2 Create a Sub-Group, "workstation"	104
5.1.1.3 Set up "test" with a 32-bit net mask.	105
5.1.1.4 Give "workstation" a 32-bit net mask	105
5.1.1.5 Block everything for the Sub-Group	106
5.1.1.6 Use Authentication Request Page for redirect URL.	108
5.1.1.7 Disable filter options.	109
5.1.1.8 Disable YouTube Video Control	110
5.1.1.9 Attempt to access Web content	111
5.1.2 Test net use based authentication settings.	112
5.2 Activate Authentication on the Network	112
5.2.1 Activate Web-based authentication for an IP Group	113
5.2.1.1 Create a new IP Group, "webauth"	113

5.2.1.2 Set "webauth" to cover users in range	113
5.2.1.3 Create an IP Sub-Group	114
5.2.1.4 Block everything for the Sub-Group	115
5.2.1.5 Use Authentication Request Page for redirect URL	116
5.2.1.6 Disable filter options.	117
5.2.1.7 Disable YouTube Video Control	118
5.2.1.8 Set Global Group to filter unknown traffic	118
5.2.2 Activate Web-based authentication for the Global Group	121
5.2.2.1 Exclude filtering critical equipment.	121
5.2.2.2 Block Web access, logging via Range to Detect	122
5.2.2.3 Block Web access via IP Sub-Group profile	126
5.2.2.4 Modify the Global Group Profile	129
5.2.3 Add Net Use command to Login Scripts	132
5.2.3.1 Modify the 3-try login script.	132
5.2.3.2 Modify the Global Group Profile	133
Glossary	135
Appendices	141
Appendix A: Authentication Operations	141
A.0.1 Tier 1: Net use based authentication	141
A.0.2 Tier 2, Tier 3: Web-based authentication	141
A.1 Tier 1: Single Sign-On Authentication.	141
A.1.1 Net use based authentication process	141
A.1.2 Tier 1 authentication method	143
A.1.3 Name resolution methods.	143
A.1.4 Configuring the authentication server	144
A.1.5 LDAP server setup rules	145
A.2 Tier 2: Time-based, Web Authentication.	145
A.2.1 Tier 2 implementation in an environment.	146
A.3 Tier 3: Session-based, Web Authentication.	148
A.4 Authenticator.	149
A.4.1 Workstation requirements.	149
A.4.2 Enable, download Authenticator	150
A.4.3 Authenticator Deployment Kit	150
A.4.4 Work flow in environments	151
A.4.5 Download and install the Deployment Kit	152
A.4.6 Access the Deployment Tool window	154
A.4.7 Configure a New Package set	154
A.4.8 View Package Configuration contents.	158
A.4.9 Edit a Package Configuration	159
A.5 Novell eDirectory Agent	160
A.5.1 Environment requirements	160
A.5.2 Novell eDirectory setup	161
A.5.3 Web Filter setup and event logs	161
Appendix B: Obtain, Export an SSL Certificate	163
B.0.1 Verify certificate authority has been installed	163
B.0.2 Locate Certificates folder	163
B.0.3 Export the master certificate for the domain.	165
B.1 Export a Novell SSL Certificate	168
B.2 Obtain a Sun One SSL Certificate.	169
Appendix C: LDAP Server Customizations.	170

- C.1 OpenLDAP Server Scenario 170
 - C.1.1 Not all users returned in LDAP Browser window 170
- Appendix D: Profile Format and Rules 171
 - D.1 Username Formats. 171
 - D.2 Rule Criteria 171
 - D.3 File Format: Rules and Examples. 173
 - D.3.1 LDAP Profile List Format and Rules 174
 - D.3.2 LDAP Quota Format and Rules 175
- Appendix E: Override Pop-up Blockers. 177
 - E.1 Yahoo! Toolbar Pop-up Blocker 177
 - E.1.1 If pop-up blocking is enabled 177
 - E.1.2 Add override account to the white list 177
 - E.2 Google Toolbar Pop-up Blocker 178
 - E.2.1 If pop-up blocking is enabled 178
 - E.2.2 Add override account to the white list 178
 - E.3 AdwareSafe Pop-up Blocker 179
 - E.3.1 If pop-up blocking is enabled 179
 - E.3.2 Temporarily disable pop-up blocking 179
 - E.4 Mozilla Firefox Pop-up Blocker 179
 - E.4.1 Add override account to the white list 179
 - E.5 Windows XP SP2 Pop-up Blocker 180
 - E.5.1 Set up pop-up blocking. 180
 - E.5.2 Temporarily disable pop-up blocking 181
 - E.5.3 Add override account to the white list 182
- Index 195

1 Introduction

The Trustwave Web Filter Authentication Guide contains information about setting up authentication on the network.

1.1 About this Guide

This Guide addresses the network administrator designated to configure and manage the Web Filter on the network.

This section provides information on how to use this Guide, and also includes an overview of filtering components and authentication solutions.

Sections 2 and 3 describe the Web Filter Administrator console entries that must be made in order to prepare the network for using authentication for LDAP domains.



Tip: Refer to the Trustwave Web Filter Installation Guide or Trustwave WFR Installation Guide for information on installing the unit on the network. This document also provides information on how to access the Web Filter Administrator 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. Section 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.

Section 5 outlines the step you need to take to test and to activate your settings before deploying authentication on the network.

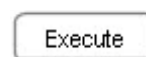
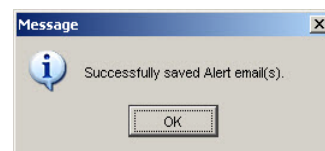
Appendices include: instructions on authentication operations; information on how to obtain or export an SSL certificate and upload it to the Web Filter; notes on customizations to make on specified LDAP servers; filtering profile file components and setup; and tips on how to override pop-up windows with pop-up blocker software installed.

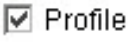
1.2 How to Use this Guide

1.2.1 Terminology

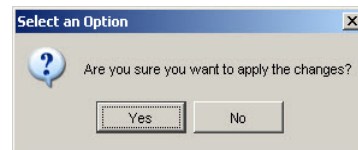
The following terms are used throughout this Guide. Sample images (not to scale) are included for each item.

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



- **check box** - a small square in a dialog box, window, or screen used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an "X" is placed, indicating that you selected the option. When this box is not checked, the option is not selected. 

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



- **field** - an area in a dialog box, window, or screen that either accommodates your data entry, or displays pertinent information. A text box is a type of field.

Short Name

- **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 Administrator 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

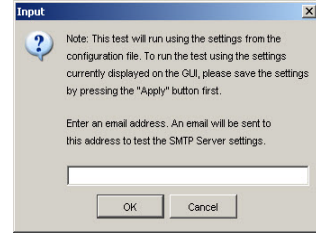
- **list box** - an area in a dialog box, window, or screen that accommodates and/or displays entries of items that can be added or removed.



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



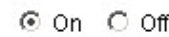
- **pop-up box** or **pop-up window** - a box or window that opens after you click a button in a dialog box, window, or screen. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.



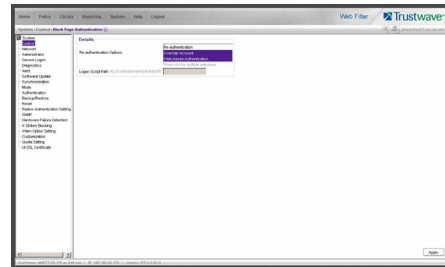
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down-arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.



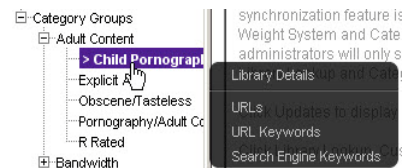
- **radio button** - a small, circular object in a dialog box, window, or screen used for selecting an option. This object allows you to toggle between two choices. By clicking a radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option 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.

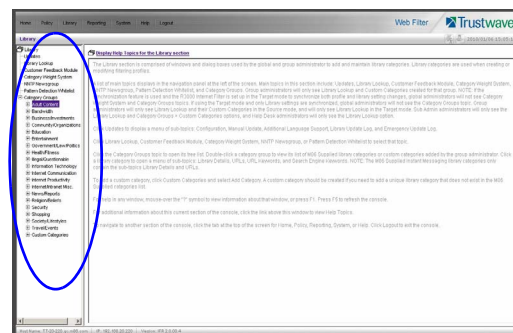


- **sub-topic** - a subset of a main topic that displays as a menu item for the topic. The menu of sub-topics opens when a pertinent topic link in the left panel—the navigation panel—of a screen is clicked. If a sub-topic is selected, the window for that sub-topic displays in the right panel of the screen, or a pop-up window or an alert box opens, as appropriate.

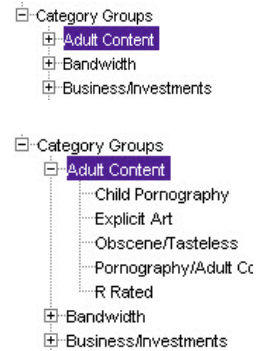


- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See "field".)

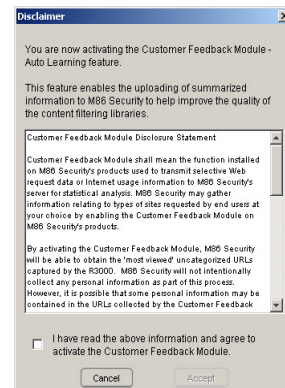
- **topic** - a topic displays as a link in the left panel—the navigation panel—of a screen. By clicking the link for a topic, the window for that topic displays in the right panel of the screen, or a menu of sub-topics opens.



- **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, check boxes, 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.



1.3 Filtering Elements

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

1.3.1 Group Types

In the Policy 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





Note: If authentication is enabled, the global administrator—who has all rights and permissions on the Web Filter—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.

1.3.1.1 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.

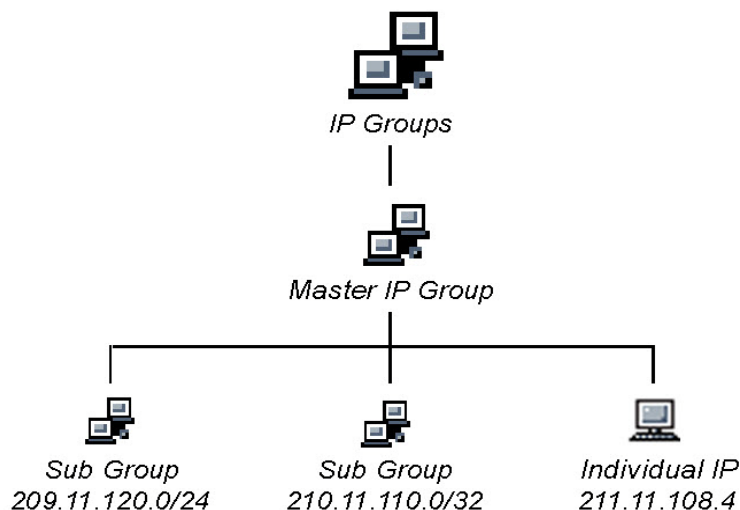
1.3.1.2 IP Groups

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.

Figure 1: IP diagram with a sample master IP group and its members



1.3.1.3 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






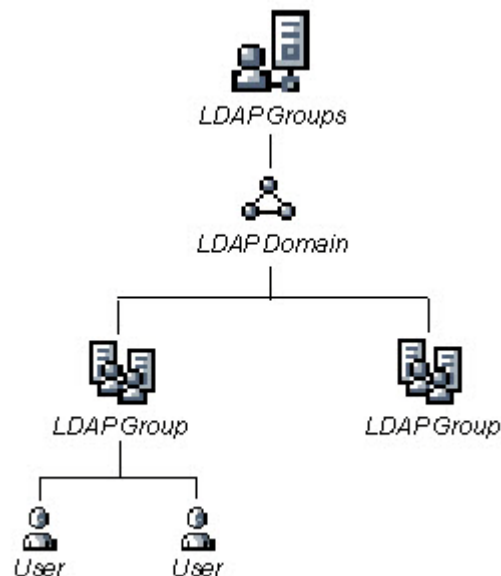
groups , workstations , users , or containers . For Open Directory, nodes include groups and users. For Novell eDirectory, Sun One, Sun IPlanet, or Netscape Directory server types, these nodes also include dynamic groups . If users belong to more than one group, the global administrator sets the priority for group filtering.

Figure 2: LDAP domain diagram, with sample groups and members



1.3.2 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 Policy 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 Web Filter Administrator 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 Web Filter and the Radius authentication feature enabled.
- TAR profile - used if a Trustwave Security Reporter (SR) or Trustwave Threat Analysis Reporter (TAR) is connected to the Web Filter and an end user is locked out by the TAR module when attempting to access blocked content in a library category.

1.3.2.1 Static Filtering Profiles

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

1.3.2.1.1 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.

1.3.2.1.2 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.

1.3.2.1.3 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.

1.3.2.2 Active Filtering Profiles

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

1.3.2.2.1 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.

1.3.2.2.2 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.

1.3.2.2.3 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.

1.3.2.2.4 Time Profile

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

1.3.2.2.5 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 Trustwave Web Filter Administrator Guide, or the Web Filter portion of the Trustwave WFR Administrator Guide for additional information on the Override Account Profile, Time Profile, and Lock Profile.

1.3.3 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

1.3.3.1 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.

1.3.3.1.1 Trustwave Supplied Categories

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

1.3.3.1.2 Custom Categories

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



Note: Trustwave cannot provide updates to custom categories. Maintaining the list of URLs and keywords is the responsibility of the global or group administrator.

1.3.3.2 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 Web Filter), 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).

1.3.3.3 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.

1.3.3.4 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.

If an override account is established at the IP group level for a member of a master IP group, filtering settings made for that end user will override the minimum filtering level if the global administrator sets the option to allow the minimum filtering level to be bypassed. An override account established at the global group level will automatically bypass the minimum filtering level.

1.3.3.5 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

1.3.4 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 container time profile takes precedence over a domain time profile, and a group time profile takes precedence over a container time profile. An individual time profile takes precedence over a group 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.

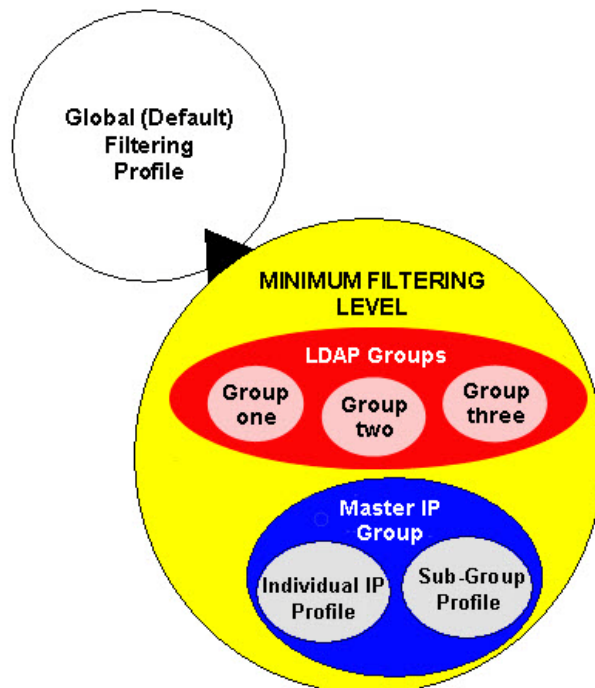
7. A Threat Analysis Reporter (TAR) profile is a type of lockout profile. If using a Security Reporter or TAR with a Web Filter, the TAR low level lockout profile takes precedence over an authentication profile or a time profile, locking out the end user from library categories specified in the lockout profile in TAR.
8. An override account profile takes precedence over a TAR lockout 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 Web Filter Administrator console takes precedence over an override account set up in the global group section of the console.

9. An X Strikes lockout profile takes precedence over all filtering profiles. This profile is set up under Filter Options, by enabling the X Strikes Blocking feature.

Figure 3: Sample filtering hierarchy diagram



1.4 Authentication Solutions

1.4.1 LDAP Authentication Protocol

The Web Filter 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.

1.4.2 Web Filter Authentication Tiers and Options

1.4.2.1 Web Filter authentication tiers

The Web Filter authentication architecture for the LDAP authentication protocol is comprised of three tiers. When using LDAP authentication with the Web Filter, 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.

1.4.2.2 Web Filter authentication options

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

1.4.3 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	Authenticator	eDirectory Agent
Tier 1	--	Yes	Yes	N/R	N/A
Tier 2	Yes	--	Yes *	Yes	Yes
Tier 3	Yes	Yes *	--	Yes	Yes
Authenticator	N/R	Yes	Yes	--	N/R
eDirectory Agent	N/A	Yes	Yes	N/R	--

KEY:

- * = Time-based option is available for Tier 3
- N/A = Not Applicable
- N/R = Not Recommended

1.4.4 Authentication System Deployment Options

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

Authentication System	Single Sign-On (SSO)	Force Authentication
Sun One OpenLDAP CommuniGate Pro (Stalker)	None	Tier 2 or Tier 3
Windows 2000/2003 Server (both Mixed and Native modes) NOTE: Windows 2008 also can be used with Authenticator	Tier 1 "net use" Authenticator for Windows	Tier 2 or Tier 3
Novell eDirectory	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 NOTE: Windows 2008 also can be used with Authenticator	Authenticator for Windows Novell eDirectory Agent	Tier 2 or Tier 3
Open Directory	Authenticator for Apple (Macintosh)	Tier 2 or Tier 3

1.4.5 Ports for Authentication System Access

The following ports should be used for authentication system access:

Type	Port number	Function
TCP	8081	Used between the Web Filter's transmitting interface and the SSL block page for Tier 2 or Tier 3 authentication.
TCP	836	Used between the Web Filter's Virtual IP address and Java applet for Tier 3 authentication.
TCP	139	Used between the Web Filter and workstations requiring Tier 1 or Tier 3 authentication.
TCP/UDP	137	Used between the Web Filter 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.

Type	Port number	Function
LDAPS	636	Used for communicating with domain controllers in order to bind with them so that user/group information can be queried/accessed.

1.4.6 Configuring Web Filter for Authentication

1.4.6.1 Configuration procedures

When configuring the Web Filter for authentication, settings must be made in System and Policy 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 Web Filter resides.
- The entries described in this section represent entries to be made on a typical network.

1.4.6.1.1 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 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.

- a. In the Listening Device frame, set the Listening Device to "LAN1".
- b. 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 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 menu.

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

- Tier 1: Choose this tier if you will only be using net use based authentication for Active Directory servers.
- Tier 2: Choose this tier if you wish to use timed Web-based authentication for LDAP domains. This tier 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 tier if you wish to use persistent Web-based authentication for LDAP domains. This tier gives the user a persistent network connection via a Java applet window that keeps the user's session open until the window is closed, so the user does not have to log in repeatedly.

For end users with Android or iOS-based devices that do not permit the Java applet to launch, an option in this tier provides end users a timed session for their Internet access, in this scenario.

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: Authenticator, and/or Novell eDirectory Agent.

4. Select "Authentication" from the navigation panel, and then select "Authentication Settings" from the menu.
 - a. In the Settings frame, enter general configuration settings for the Web Filter such as IP address entries.
 - b. 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 menu. This option should be used if Web-based authentication will be deployed on the Web Filter. 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 Web Filter as a valid server with which they can communicate.
6. Select "Control" from the navigation panel, and then select "Block Page Authentication" from the 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 Web Filter 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 Policy tree.

1.4.6.1.2 Policy section

In the Policy 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 Web Filter.



Note: If the network has more than one domain, the first one you add should be the domain on which the Web Filter 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.

2 Network Setup

2.1 Network Requirements

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

2.2 Workstation Requirements

2.2.1 Administrator Workstation

System requirements for the administrator's workstation include the following:

Client OS	IE version	Firefox version	Chrome version	Safari version
Windows XP	8	16	23	N/A
Windows Vista	9	16	23	N/A
Windows 7	9	16	23	N/A
Macintosh 10.6 (Snow Leopard)	N/A	17	23	5
Macintosh 10.7 (Lion)	N/A	17	23	6
Macintosh 10.8 (Mountain Lion)	N/A	16	N/A	6

- JavaScript enabled
- Java Virtual Machine
- Java Plug-in (use the version specified for the Web Filter software version)
- Java Runtime Environment, if using Tier 3 authentication
- Pop-up blocking software, if installed, must be disabled



Note: Web Filter administrators must be set up with software installation privileges in order to install Java used for accessing the user interface.

2.2.2 End User Workstation

System requirements for the end user's workstation include the following:

- JavaScript enabled

Client OS	IE version	Firefox version	Chrome version	Safari version
Windows XP	8	16	23	N/A
Windows Vista	9	16	23	N/A
Windows 7	9	16	23	N/A
Macintosh 10.6 (Snow Leopard)	N/A	17	23	5
Macintosh 10.7 (Lion)	N/A	17	23	6
Macintosh 10.8 (Mountain Lion)	N/A	16	23	6

- Java Runtime Environment, if using Tier 3 authentication
- Pop-up blocking software, if installed, must be disabled

The following features are available for these supported tablets:

Client OS	Auth Form	Block Page	Safe Search	You Tube for Schools	VuSafe	HTTPS
iPad1 (iOS 5.5)	Y	Y	Y	N	Y	Y
iPad2 (iOS 6)	Y*	Y	Y	N	Y	Y
Galaxy Tab 7.0 (Android 2.2, Froyo)	Y	Y	Y	Y	Y	Y
Kindle Fire Gen. 1 (Android 2.3 Gingerbread OS)	Y	Y**	N*	N	Y	Y
Nexus 7 (Android 4.1.1)	Y	Y**	N*	N	Y	Y

KEY - Functionality with the following exceptions:

- Y* = CA certificate must be imported to the browser
- Y** = No keyword blocking for Google and Bing
- N* = SafeSearch works for Yahoo! but not Google and Bing

2.3 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.

2.3.1 Specify the operation mode

Click Mode and select Operation Mode from the menu to display the Operation Mode window.

Figure 4: Operation Mode window and non-WFR Web Filter

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

In the Mode frame, select the mode to be used: "Invisible", "Router", "Firewall", or "Bridge".



Note: See the Trustwave Mobile Security Client Guide for information about configuring and using the mobile mode option.

2.3.1.1 Invisible, Router, or Firewall Mode

1. In the Listening Device frame, set the **Device** to "LAN1".
2. 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 Web Filter 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 Web Filter 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.

3. Click **Apply**.

2.3.1.2 Bridge Mode

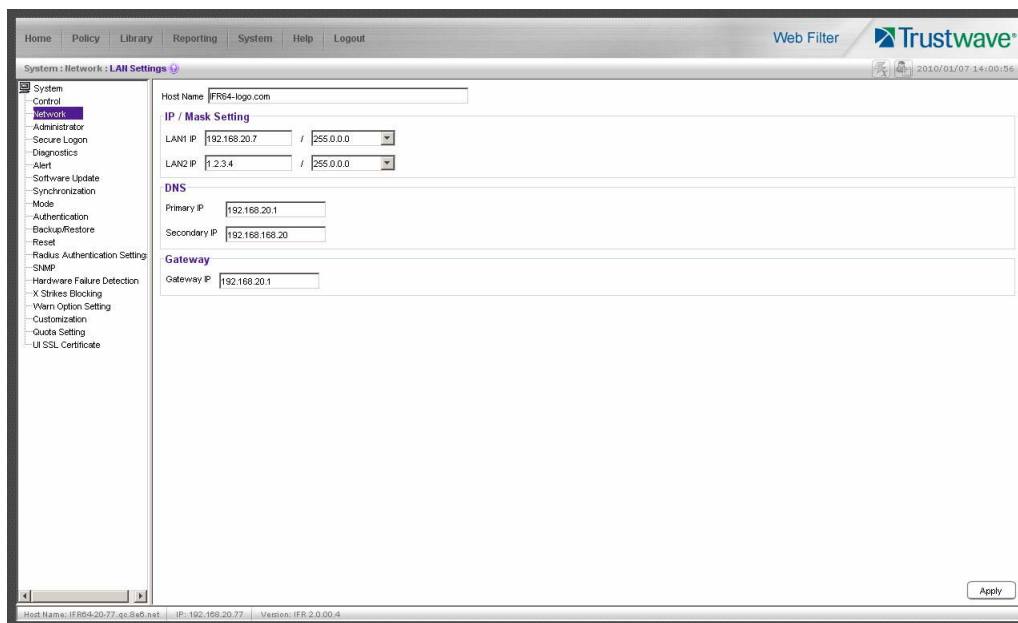
In the Bridge Settings frame:

1. In the IP Address field, specify the IP address of the Bridge interface.
2. IN the Subnet mask field, specify the mask for the subnet of the Bridge interface.
3. In the Default gateway field, specify the gateway for the subnet.

2.3.2 Specify the subnet mask, IP address(es)

Click Network and select LAN Settings from the menu to display the LAN Settings window.

Figure 5: LAN Settings window



The entries made in this window will vary depending on whether you are using the invisible mode, router or firewall mode. Bridge mode settings are configured on the Mode screen (see above)



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

2.3.2.1 Invisible mode

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

2.3.2.2 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.

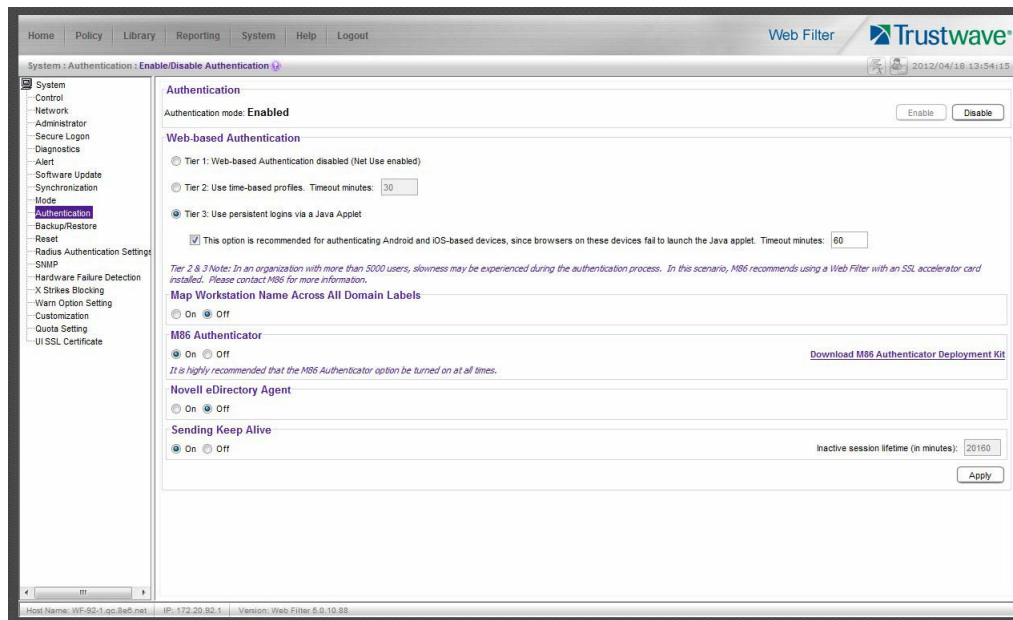
2. Click **Apply** to apply your settings.



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

2.3.3 Enable authentication, specify criteria

1. Click Authentication and select Enable/Disable Authentication from the 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:



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 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 Web Filter 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 Authenticator frame, be sure the Authenticator is "On"—unless the Novell eDirectory Agent option will be used instead. Enabling the Authenticator option, and then downloading, installing, and configuring the Authenticator Deployment Kit on a Windows machine results in the deployment of a platform-specific package that can be installed on a network share accessible by an Active Directory domain controller, a Novell eDirectory server, or on a Windows or Macintosh workstation joined to a domain via Active Directory or OpenDirectory. When installed on a workstation, the Authenticator automatically authenticates the end user when the user logs into the workstation. If installing the deployment kit in a Macintosh environment, 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 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 Policy tree.



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

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**.

2.3.3.1 Net use based authentication

2.3.3.1.1 Tier 1: Web-based Authentication disabled

Choose Tier 1 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.

2.3.3.2 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, Trustwave recommends using a Web Filter with an SSL accelerator card installed. Please contact Trustwave for more information.

2.3.3.2.1 Tier 2: Use time-based profiles

Choose this tier 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 Web Filter.

1. Click "Tier 2".
2. In the **Timeout minutes** field, enter a whole number for the duration of time the user will retain his/her Internet connection; 30 minutes displays by default.

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



Note: See Set Tier 2, Tier 3 timeout minutes in Chapter 4 if you wish to define a customized number of timeout minutes for a domain, group, or user authentication profile.

2.3.3.2.2 Tier 3: Use persistent logins via a Java Applet

Choose this tier 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:



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 Web Filter will allow the JRE download at the time of login. However some operating systems may require this action to be performed manually.

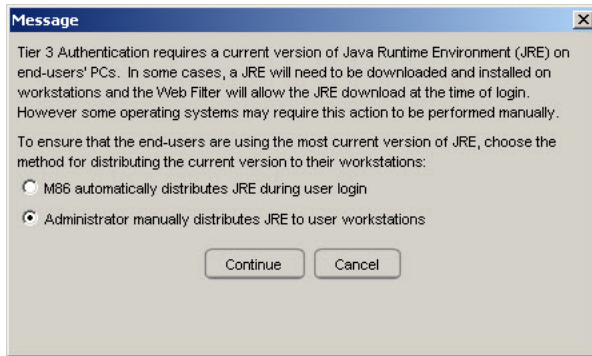
If the user's browser fails to launch the Java applet, an option is available for that user to have a time-based authentication profile activated for a set number of minutes.

1. Click "Tier 3".
2. If any users have Android or iOS-based devices such as iPad tablets, click the check box corresponding to the option: "Enable time-based profiles if browsers fail to launch the Java Applet," and specify the number of **Timeout minutes** users will retain their Internet connections; 1 minute displays by default.



Note: See Set Tier 2, Tier 3 timeout minutes in Chapter 4 if you wish to define a customized number of timeout minutes for a domain, group, or user authentication profile.

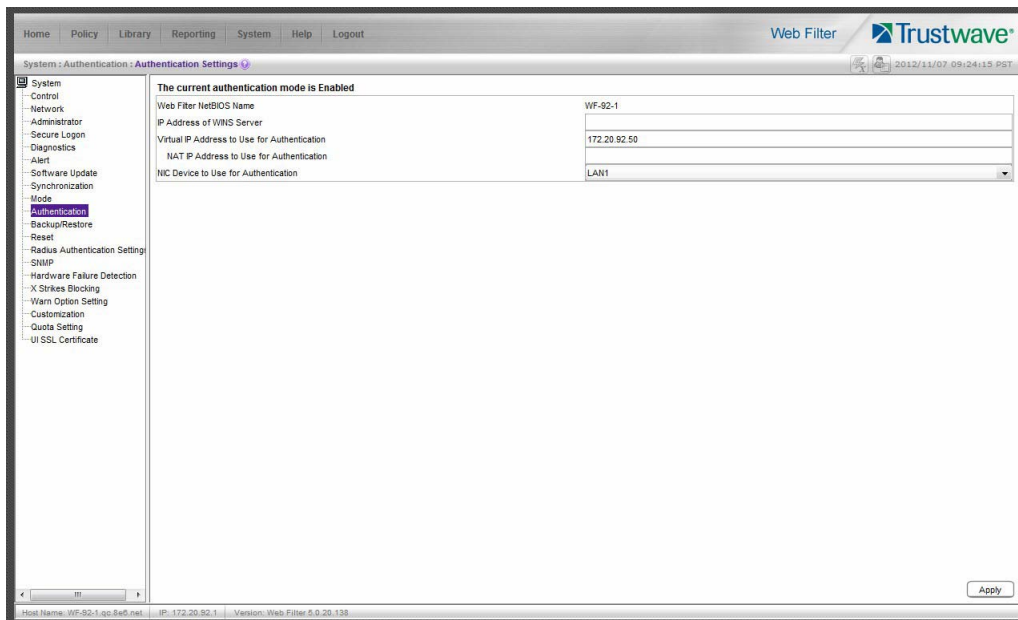
3. Click **Apply** to open the dialog box that informs you about the requirement of a current Java Runtime Environment (JRE) to be installed on each end user's workstation:



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

2.3.4 Enter network settings for authentication

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



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

3. 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 Web Filter, with a space between each IP address.
4. 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 Web Filter and the PDC. This must be an IP address that is not being used, on the same segment of the network as the Web Filter.



Caution: If the IP address entered here is not in the same subnet as this Web Filter, the net use connection will fail.

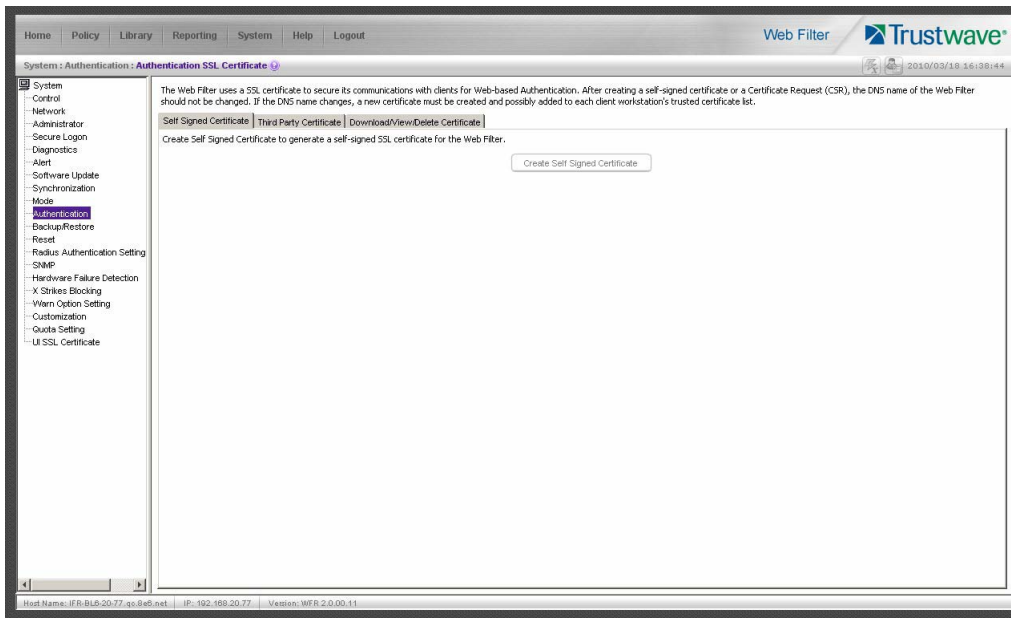
5. Enter the **NAT IP Address to Use for Authentication** if the Web Filter is configured behind the NAT router.
6. From the **NIC Device to Use for Authentication** pull-down menu:
 - if using the invisible mode, select "LAN2" for sending traffic on the network—in particular, for transferring authentication data.
 - if using the router or firewall mode, select "LAN1".
7. Click **Apply** to apply your settings.

2.3.5 Create an SSL certificate

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

Click Authentication and select Authentication SSL Certificate from the menu to display the Authentication SSL Certificate window.

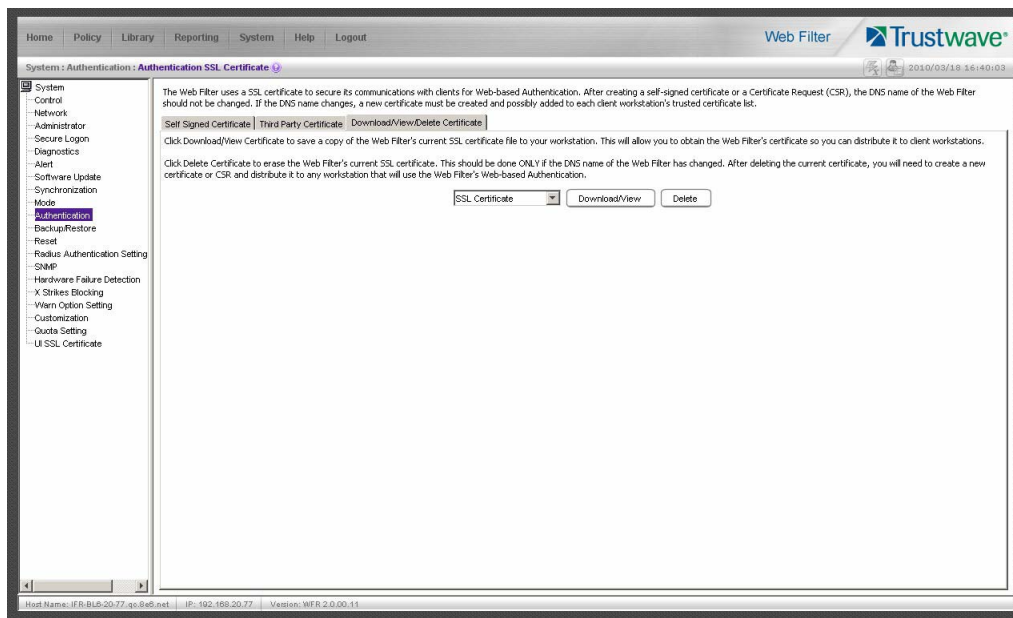
Figure 6: Authentication SSL Certificate window



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.

2.3.5.1 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:



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.

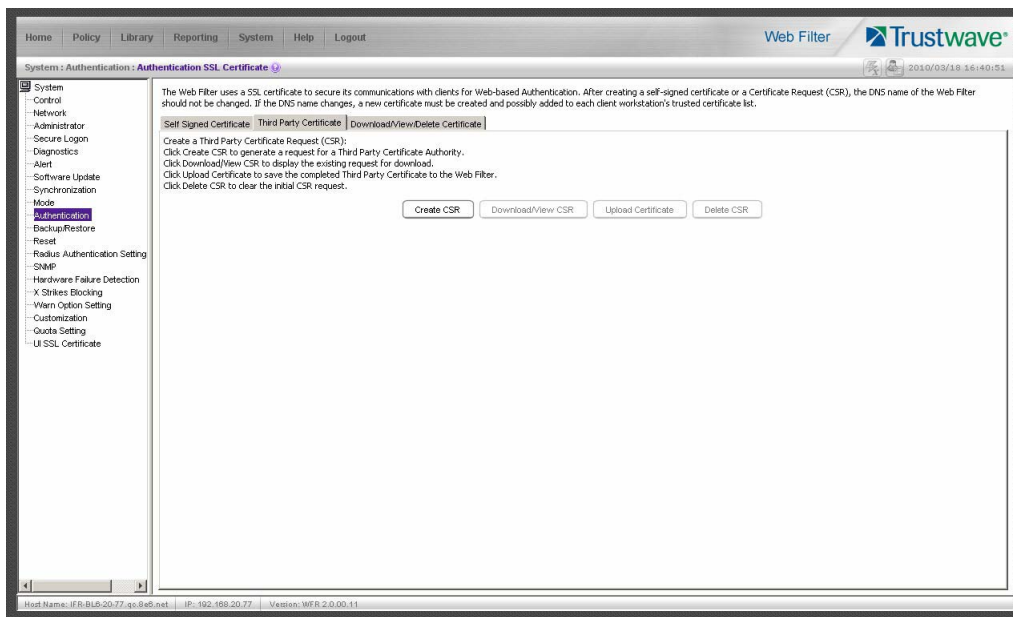


Tip: Click **Delete Certificate** to remove the certificate from the server.

2.3.5.2 Create, Upload a Third Party Certificate

2.3.5.2.1 Create a Third Party Certificate

1. Click the 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 window:



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

Buttons: Create, Cancel

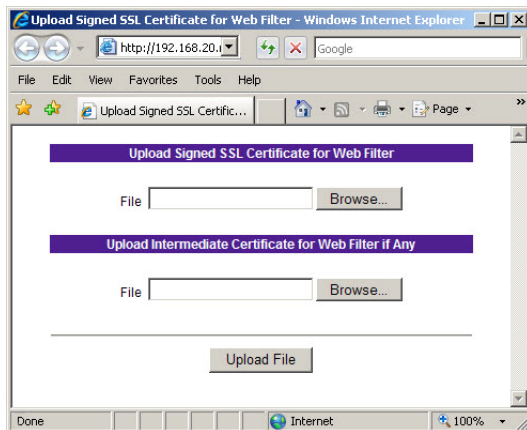
3. The **Common Name (Host Name)** field should automatically be populated with the host name. This field can be edited, if necessary.
4. Enter your **Email Address**.
5. Enter the name of your **Organization**, such as Trustwave .
6. Enter an **Organizational Unit** code set up on your server, such as Corp.
7. Enter **Locality** information such as the name of your city or principality.
8. Enter the **State or Province** name in its entirety, such as Ca l i f o r n i a.
9. Enter the two-character **Country** code, such as US .
10. 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.

2.3.5.2.2 Upload a Third Party Certificate

1. In the Third Party Certificate tab, click **Upload Certificate** to open the Upload Signed SSL Certificate for Web Filter window:



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.



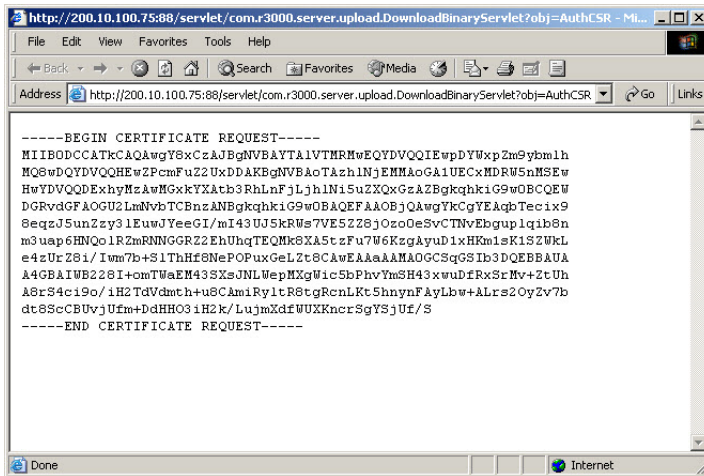
Tip: Click **Cancel** in the dialog box to cancel the procedure.

2. In the Upload Signed SSL Certificate for Web Filter window, do one of the following, as appropriate:
 - Click **Browse...** in the Upload Signed SSL Certificate for Web Filter section if the certificate to be uploaded is an SSL certificate.
 - Click **Browse...** in the Upload Intermediate Certificate for Web Filter if Any, 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 Web Filter.
5. Click **OK** in the Message dialog box to confirm the upload and to close the dialog box.

2.3.5.2.3 Download a Third Party Certificate

1. In the Third Party Certificate tab, choose either "SSL Certificate" or "Intermediate Certificate."

2. Click **Download/View CSR** to open a window containing the contents of the certificate request:



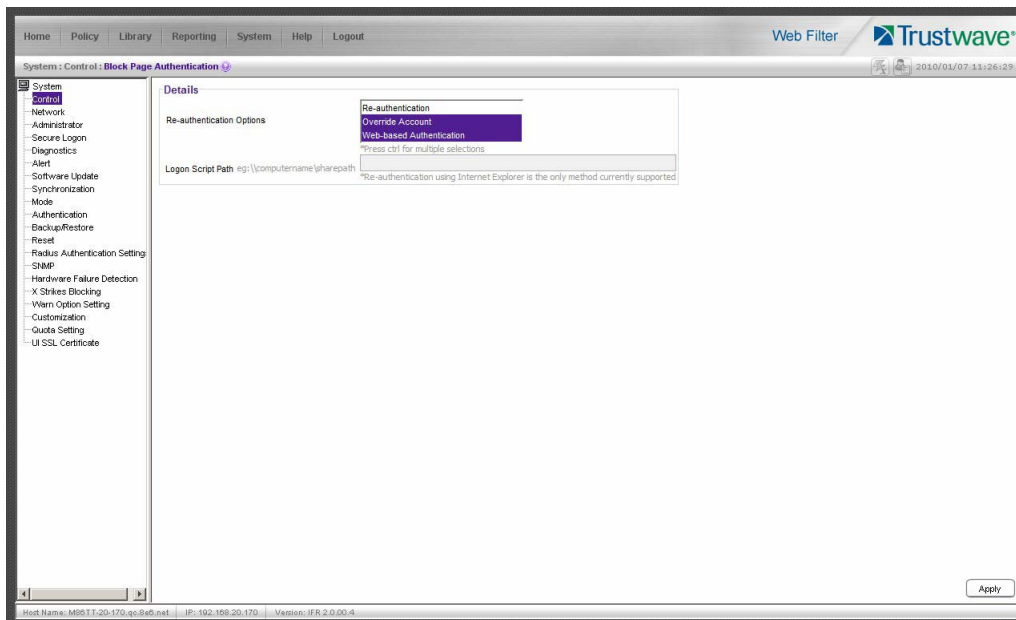
3. Click the "X" in the upper right corner of the window to close it.



Tip: Click **Delete CSR** to remove the certificate from the server.

2.3.6 Specify block page settings

Click **Control** and select **Block Page Authentication** from the menu to display the **Block Page Authentication** window:



2.3.6.1 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.
- **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.
- **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.



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



Notes:

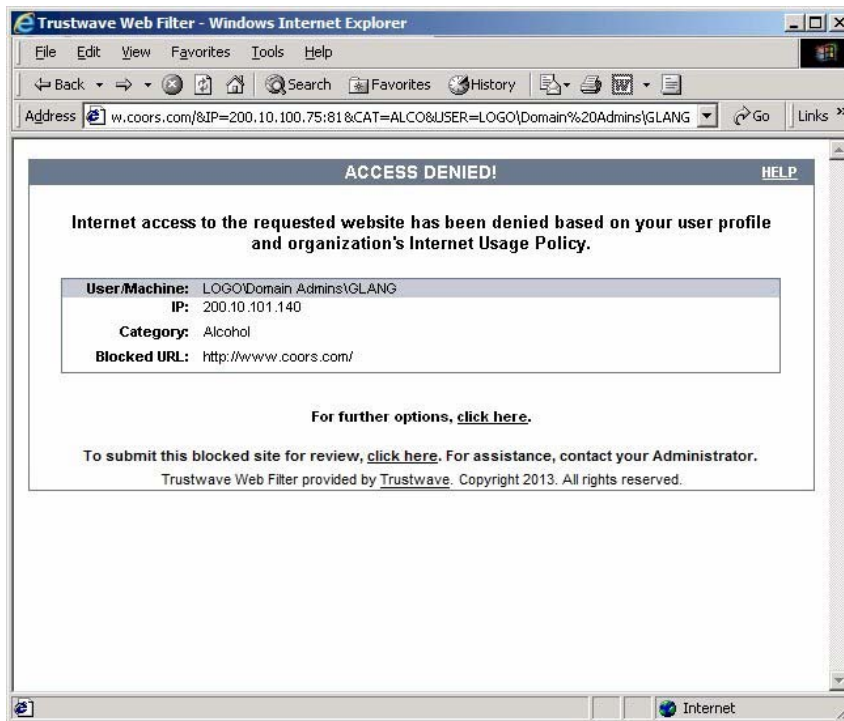
- See the Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for information about the Override Account feature.
- The Re-authentication option only supports Internet Explorer browsers. End users who are using other browser types (Firefox, Safari, Chrome, etc.) will not be able to re-authenticate themselves.

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 Web Filter 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.

2.3.6.1.1 Block page

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



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 Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for information on creating a customized block page using your own design.
- If using the Mobile Security Client (MSC), block pages served from the mobile server do not include the options link.

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:

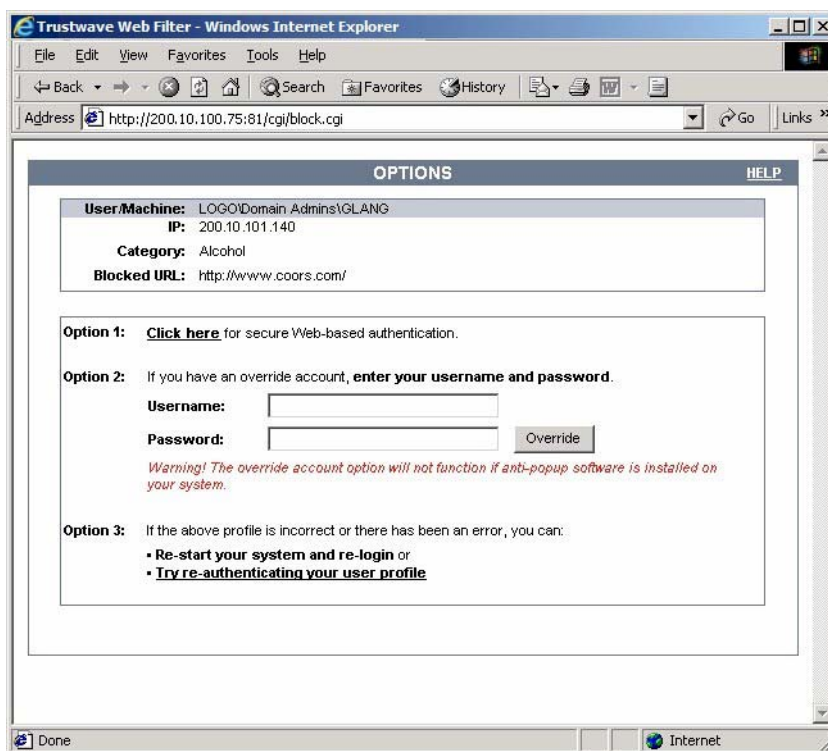
- **HELP** - Clicking this link takes the user to Trustwave's Technical Support page that explains why access to the site or service may have been denied.
- **Trustwave** - Clicking this link takes the user to Trustwave's Web site.

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 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.

2.3.6.1.2 Options page

The Options page displays when the user clicks the following link in the block page: **For further options, [click here](#).**



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

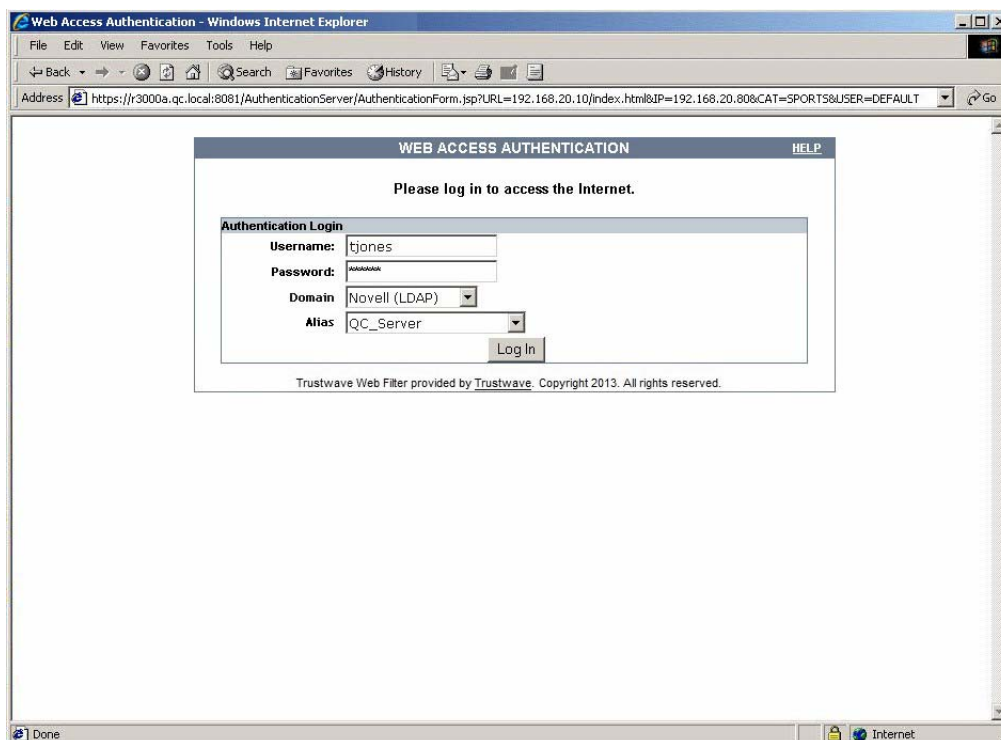
The frame beneath the User/Machine frame includes additional options, based on settings made in the Block Page Authentication window. These options are described in the following sections.

2.3.6.1.3 Options page, Web-based Authentication

This option 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:



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

2.3.6.1.4 Options page, Override Account

This option 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.



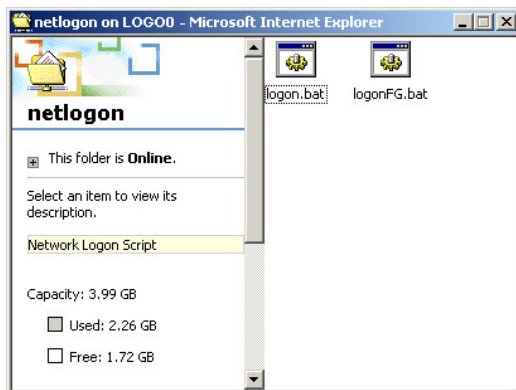
Notes:

- 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 Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for information about the Override Account feature.

2.3.6.1.5 Options Page, Re-Authentication

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 Web-based Authentication, 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:



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

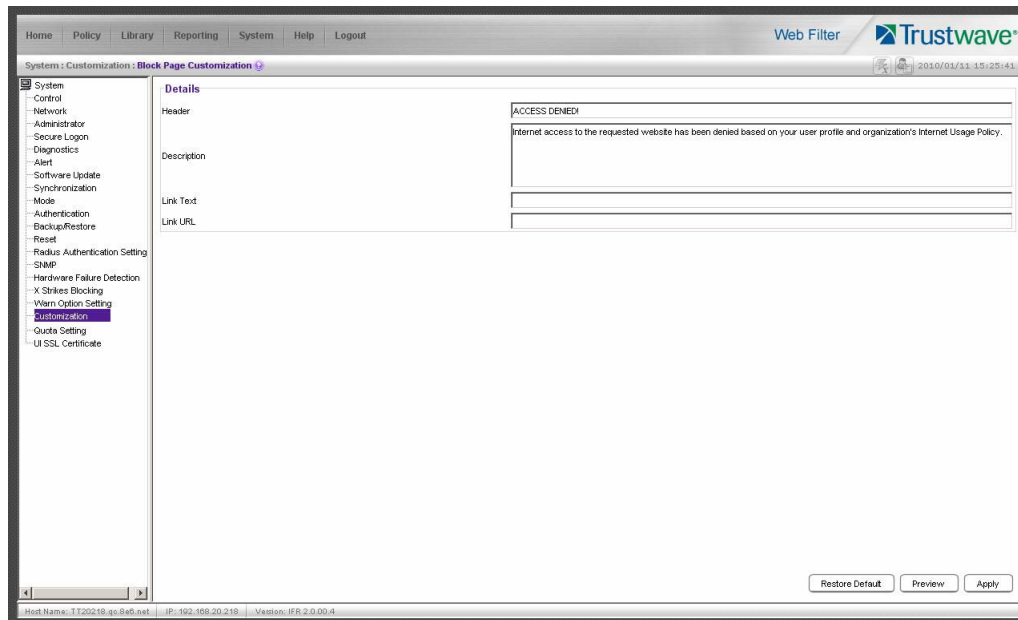


Note: If the end user is using a non-IE browser type (i.e. Firefox, Safari, or Chrome) he/she will see a message specifying that IE is the only browser type supported for re-authentication.

2.3.6.2 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 menu to display the 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 Trustwave'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.

2.3.6.2.1 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 Trustwave Web Filter 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.trustwave.com/support/r3000/accessdenied.asp>” 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.

2.3.6.3 Authentication Form Customization

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



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.

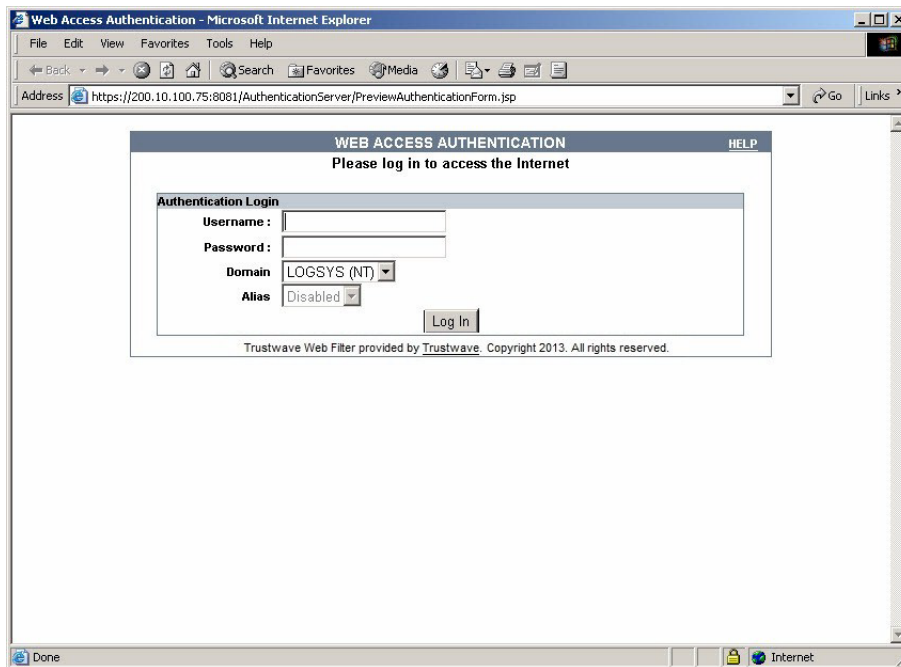
2. Click **Apply**.



Tip: Click **Restore Default** and then **Apply** to revert to the default text in this window.

2.3.6.3.1 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:



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

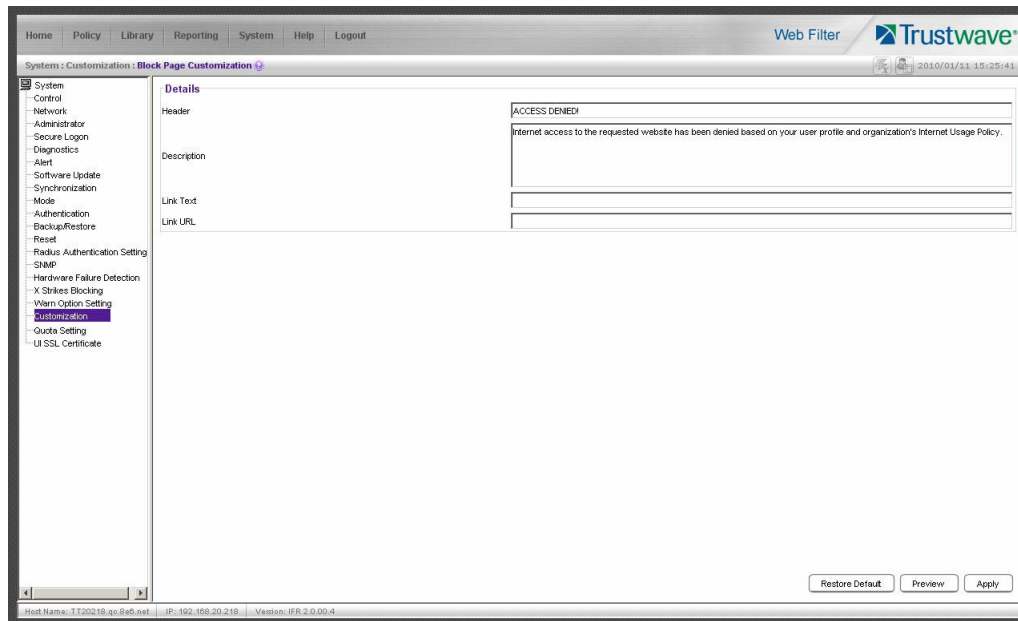
2. Click the "X" in the upper right corner of the window to close the sample Authentication Request Form.



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.

2.3.6.4 Block Page Customization

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



Note: See Appendix B: Create a Custom Block Page from the Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator 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.

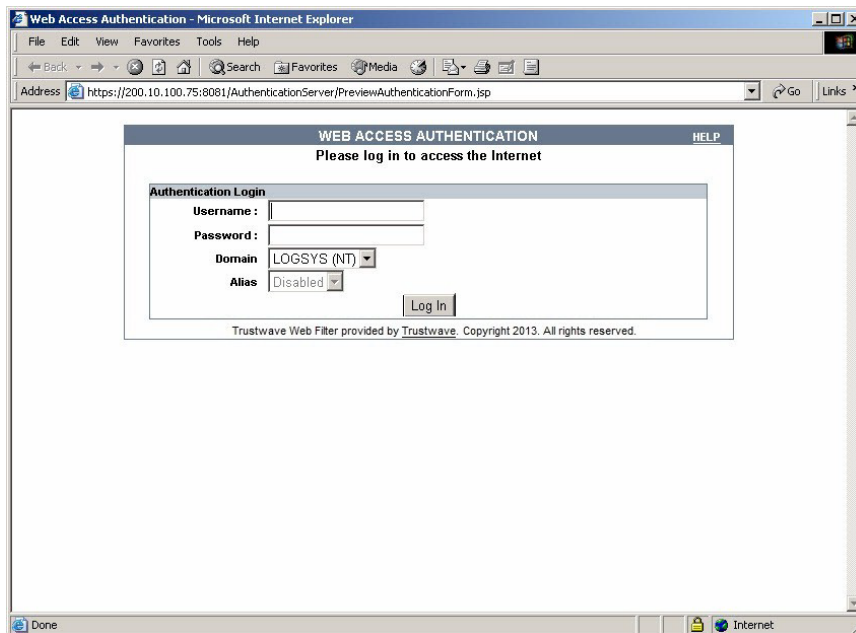
2. Click **Apply**.



Tip: Click **Restore Default** and then **Apply** to revert to the default text in this window.

2.3.6.4.1 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:



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 Trustwave's Technical Support page that explains why access to the site or service may have been denied.
- **Trustwave** - Clicking this link takes the user to Trustwave'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 sub-section.
- **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.

2.4 Set up Group Administrator Accounts

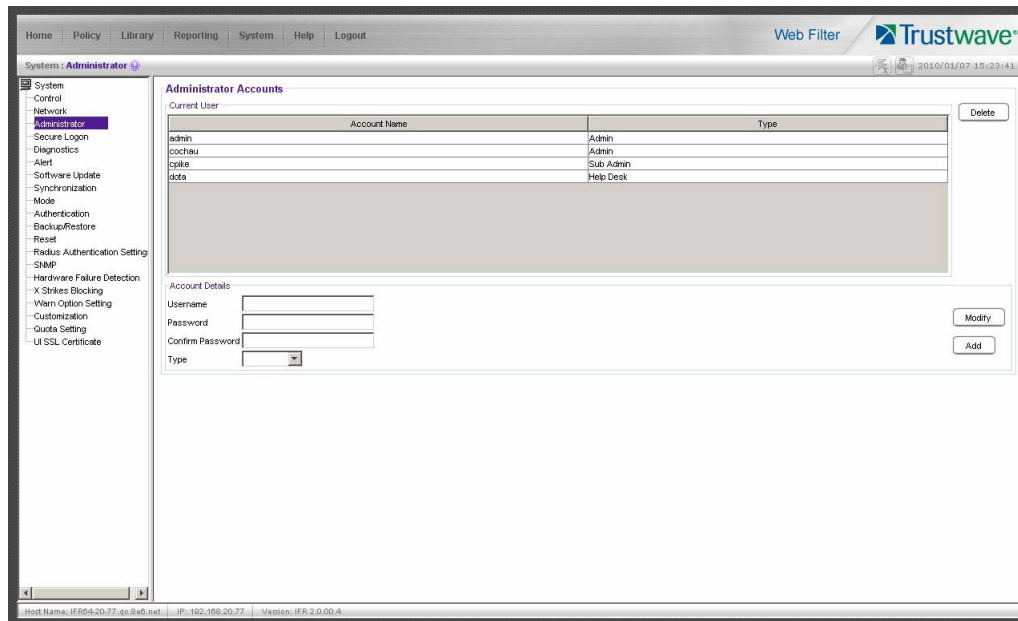
The global administrator creates group administrator (Sub Admin) accounts so that these group administrators can be assigned to manage specific LDAP entities (nodes) set up in the Policy tree. Sub Admin group administrator accounts are set up in the Administrator window from the System section of the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



Note: IP group administrator accounts are set up in the IP branch of the Policy tree when new IP groups are created. See Chapter 2: Policy screen from the Global Administrator Section of the Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for information on creating IP groups.

2.4.1 Add Sub Admins to manage nodes

Click Administrator to display the Administrator window:



2.4.1.1 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.

2.4.1.2 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.

2.4.1.3 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.

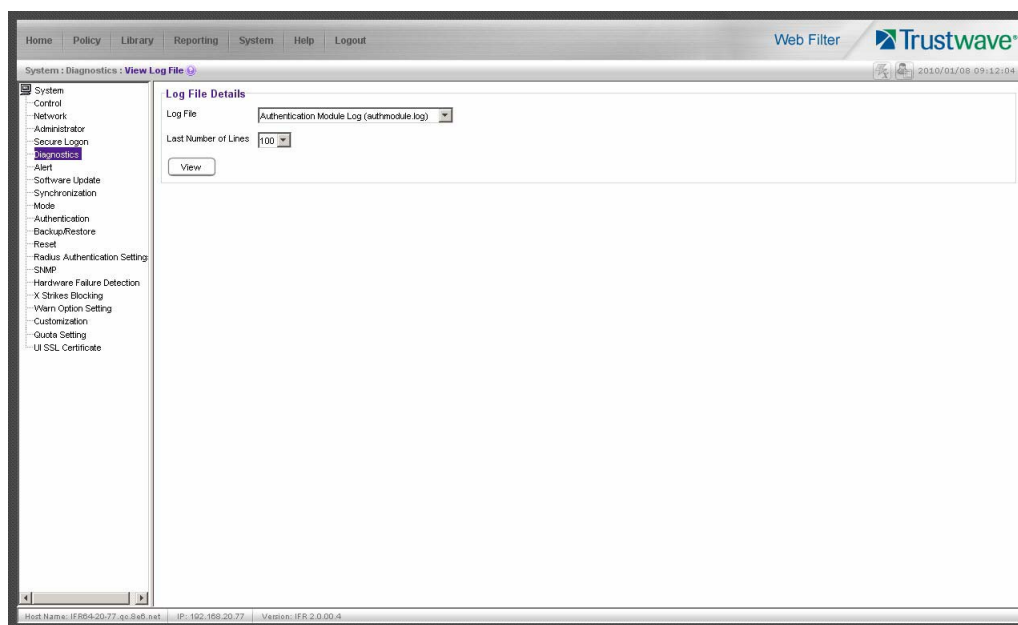


Note: If a group administrator assigned to an LDAP node is deleted, that group administrator must be removed from assignment to that node and another group administrator set up for assignment to manage that node. See Chapter 4: Manage Nodes for information on assigning and re-assigning a node for management.

2.5 View Log Results

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

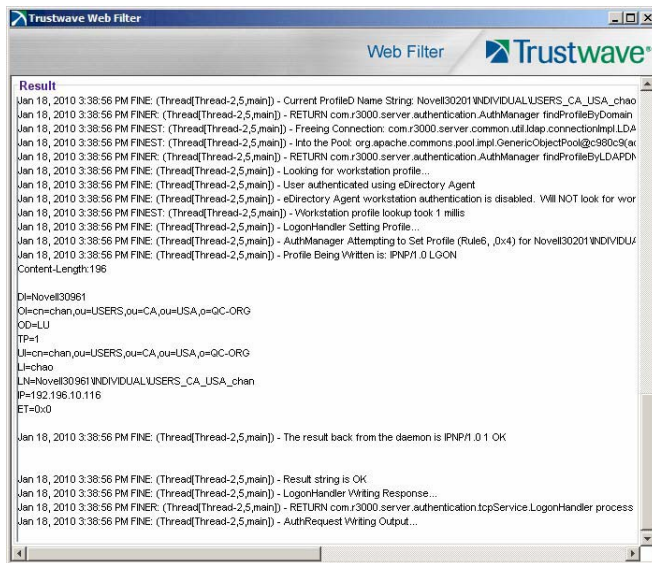
1. Click Diagnostics and select View Log File from the menu to display the View Log File window:



Note: In this Guide, only authentication-related options will be addressed. For information about all other options, see the View Log File window in the Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator 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 window:



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

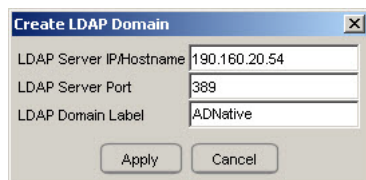
3 LDAP Authentication Setup

3.1 Create an LDAP Domain

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

3.1.1 Add the LDAP domain

1. Click LDAP in the navigation panel to open the menu, and select Add Domain to open the Create LDAP Domain dialog box:



Field	Value
LDAP Server IP/Hostname	190.160.20.54
LDAP Server Port	389
LDAP Domain Label	ADNative

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.

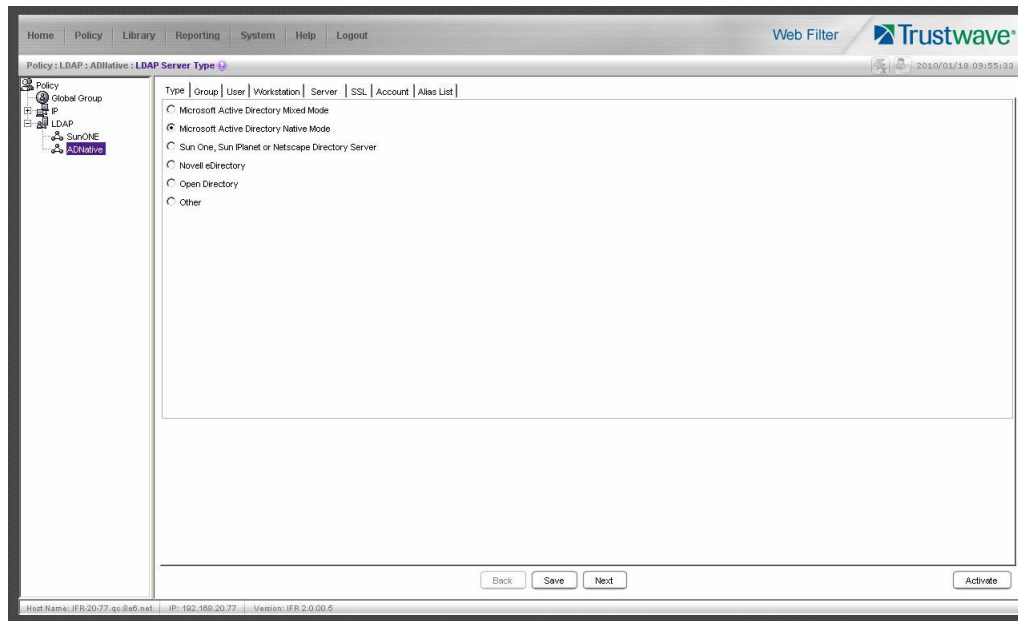
5. Click **Apply** to add the domain to the tree. This action takes you directly to the LDAP domain window (see View, modify, enter LDAP domain details).

3.1.2 Refresh the LDAP branch

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

3.1.3 View, modify, enter LDAP domain details

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



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.



Caution: The instructions in this 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.

3.1.3.1 Type

Based on the entries made when creating the LDAP domain, the Web Filter 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.



Caution: 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.

3.1.3.2 Group

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

Figure 7: 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, the following action(s) is/are available for specifying a particular group profile assignment, if necessary:
 - If using Active Directory, the “Use Primary Group” action 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” action displays on this tab. You may wish to check this box to indicate that profiles based on dynamic groups should be assigned to users.
 - If using Active Directory Native mode, Sun One, Novell eDirectory, or Open Directory, the “Use Nested Group” action displays on this tab. This feature saves you time when configuring policies. After the group policy is configured, all sub-groups within that group will use the same policy and do not need to be configured, unless a special policy is required for a sub-group and that policy is given a higher priority than the group policy.



Note: If the options for “Use Dynamic Group” and “Use Nested Group” are both available, Trustwave recommends using nested groups over dynamic groups for optimum performance of the Web Filter.

3. If any modifications were made on this tab, click **Save**.
4. **Next** to go to the User tab.

3.1.3.3 User

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

Figure 8: Domain Details window, User tab

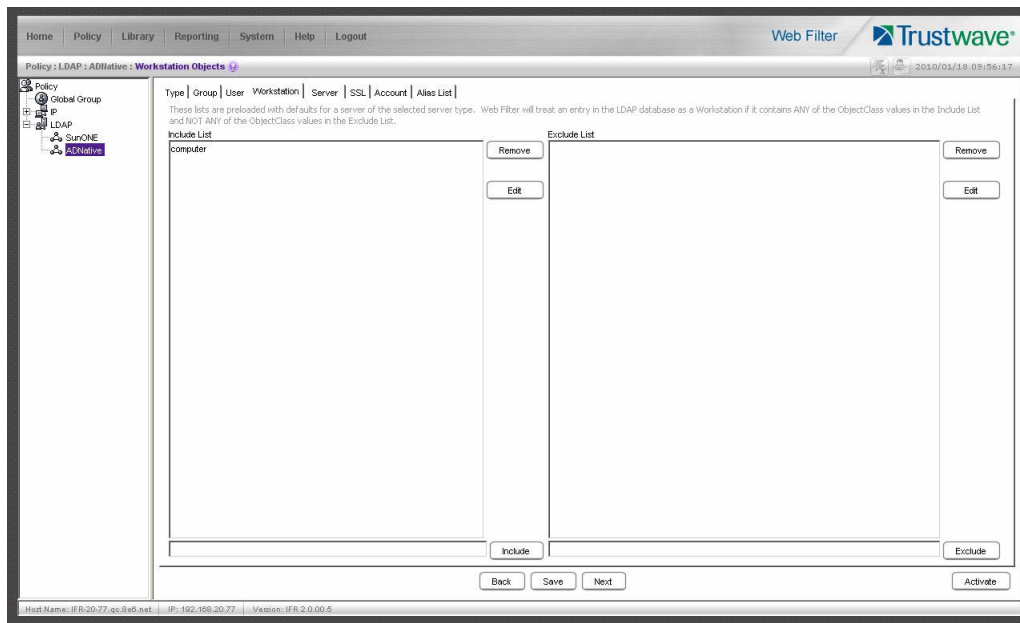
By default, the Include List and Exclude List are populated with appropriate user objects, based on the server type.

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

3.1.3.4 Workstation

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

Figure 9: Domain Details window, Workstation tab



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

- 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.

3.1.3.5 Server

The LDAP domain address information populates the Server tab.

Figure 10: Domain Details window, Server 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.
 - A fully qualified domain name entry is required on a mobile Web Filter using an LDAP server to authenticate mobile end users.
 - 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.

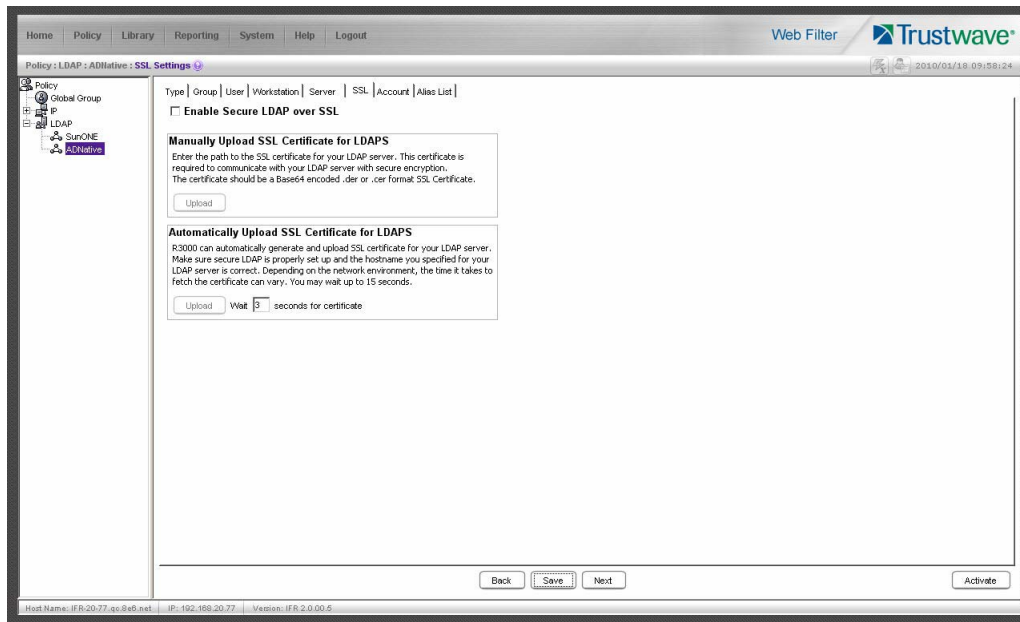
If this field is not populated, enter the LDAP query base exactly as set up on the LDAP server. For example, if the entry on the LDAP server is DC=QA,DC=local, you must enter DC=QA,DC=local —**not** dc=QA,dc=local **or** DC=QA,DC=Local.

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

3.1.3.6 SSL

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

Figure 11: Domain Details window, SSL tab

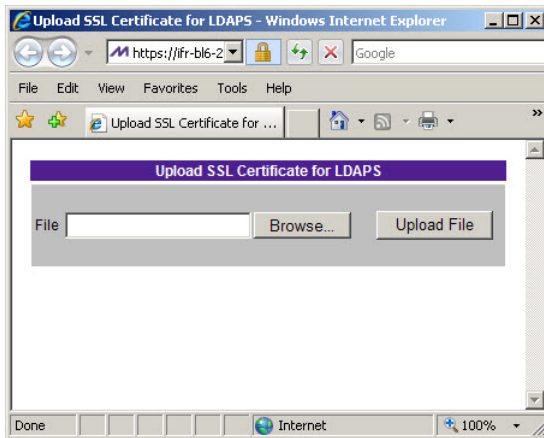


Note: See Appendix B: Obtain, Export an SSL Certificate for information on how to obtain a Sun One server's SSL certificate, or how to export an Active Directory or Novell server's SSL certificate to your desktop and then upload it to the Web Filter.

1. If applicable, click in the "Enable Secure LDAP over SSL" action. 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 window:



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



Caution: 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 Account tab.

3.1.3.7 Account

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

Figure 12: 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” action 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:

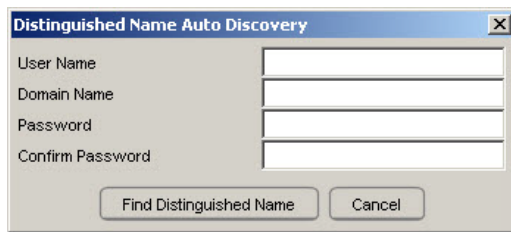
`cn=Administrator,cn=Users,dc=qc2domain,dc=local`

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 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. Togo . company . 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 box closes and the fields on this tab become populated with appropriate data.



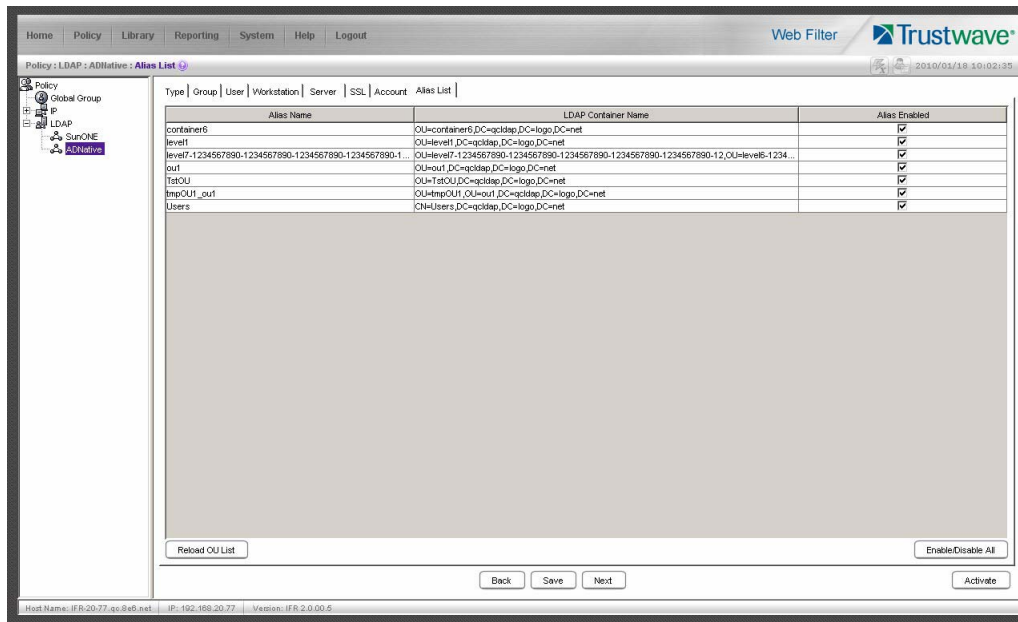
Note: Once the Distinguished Name and password are successfully saved on this tab, the Distinguished Name Auto Discovery frame will no longer display at the bottom of this tab.

2. Click **Save** to save your entries.
3. Click **Next** to go to the Alias List tab.

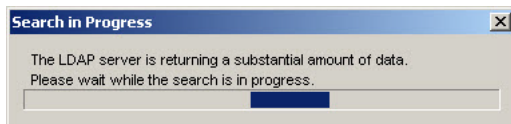
3.1.3.8 Alias List

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.

Figure 13: 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:



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 action. To deselect an item, click the action 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. 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.

3.1.4 Delete a domain

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

3.2 Set up LDAP Domain Nodes

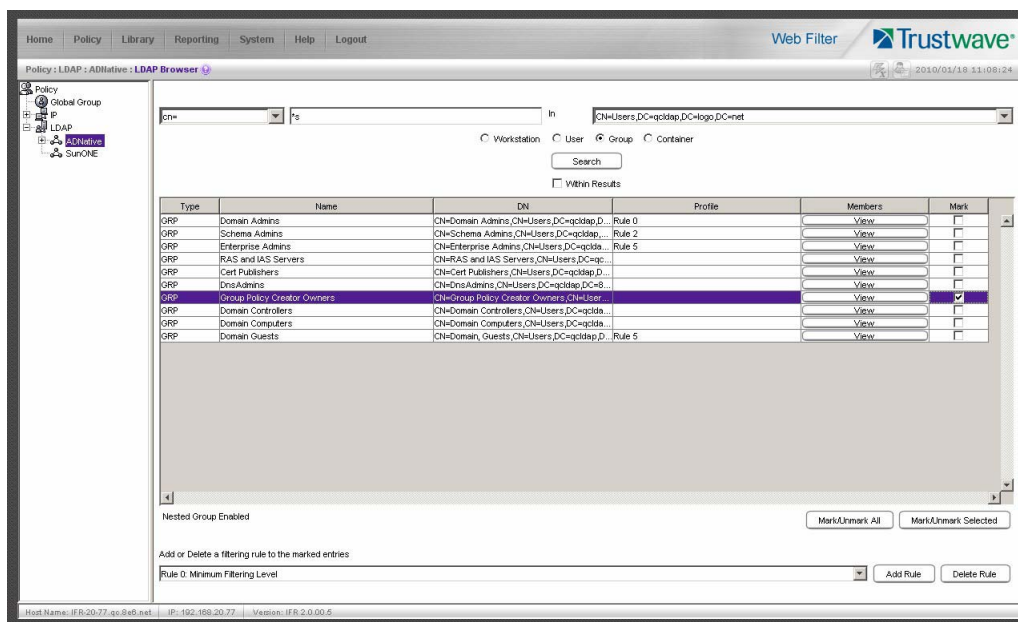
In the navigation panel, the LDAP domain branch of the tree menu includes options for setting up entities (nodes) in the domain so that filtering profiles can later be created. The following options are used in this setup process: Manage Profile Objects, Set Group Priority, Manually Add Workstation,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

3.2.1 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 menu to display the LDAP Browser window.

Figure 14: 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. If the "Use Nested Group" option was available in the Group tab of Domain Details, "Nested Group Enabled" or "Nested Group Disabled" displays towards the bottom left of this window, depending on whether or not this feature was enabled or disabled in the Group tab.
- See Appendix C: LDAP Server Customizations if using an OpenLDAP server.

3.2.1.1 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 action.

3.2.1.2 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" action, 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.

3.2.1.3 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 action 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.

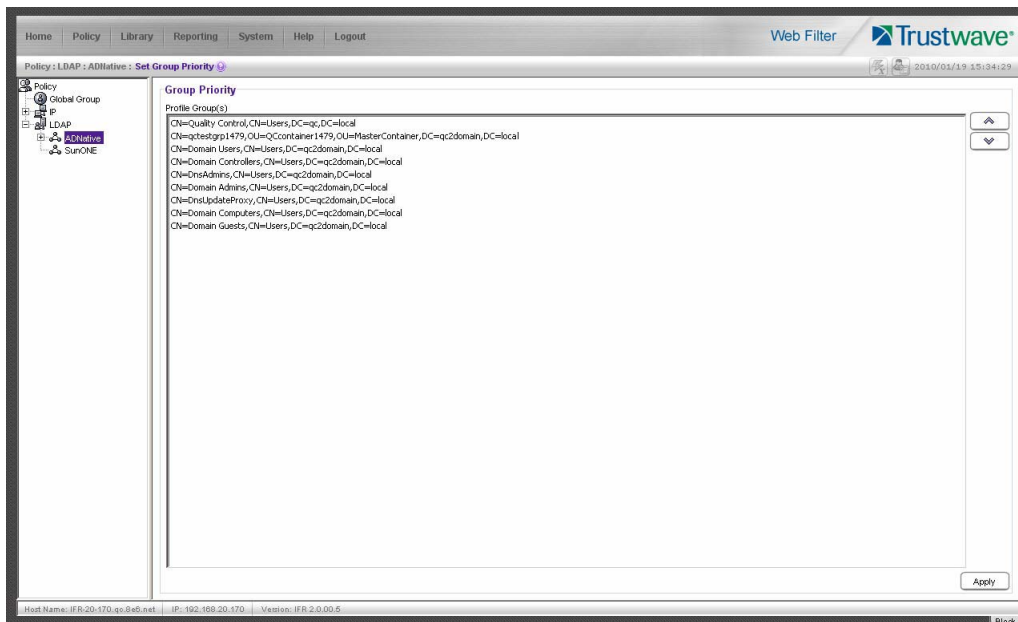
3.2.1.4 Delete a rule

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 action for the entity.
2. Click **Delete Rule** to remove the entity's profile from the tree.

3.2.2 Specify a group's filtering profile priority

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

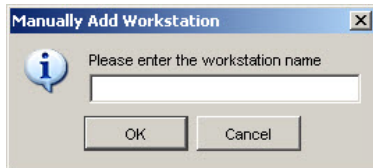
- Groups automatically populate the Profile Group(s) list box, if these groups have one or more identical users and were added to the tree list via the LDAP Browser window.
- An entry for the Group Priority list is added to the end of the list when the group profile for that group is added to the Web Filter, 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.

3.2.3 Manually add a workstation name to the tree

1. Select the LDAP domain, and choose Manually Add Workstation from the menu to open the Manually Add Workstation dialog 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.

3.2.4 Manually add a user's name to the tree

1. Select the LDAP domain, and choose Manually Add Member from the menu to open the Manually Add Member dialog 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=nwr-d-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.

3.2.5 Manually add a group's name to the tree

1. Select the LDAP domain, and choose Manually Add Group from the menu to open the Manually Add Group dialog 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.

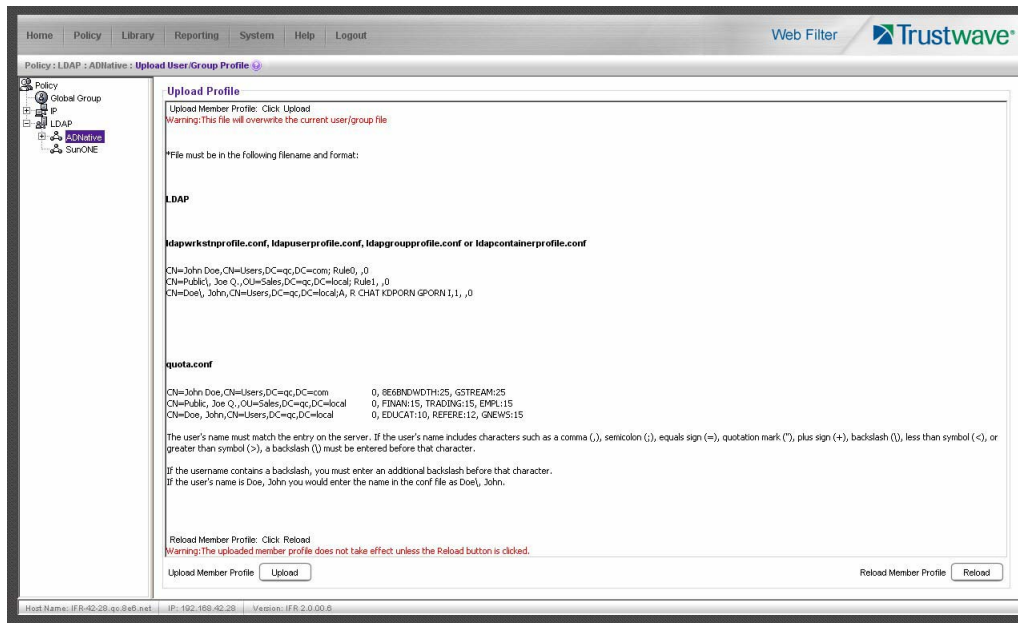
2. Enter the group's name in the text box, using the entire Distinguished Name format.
3. Click **OK** to add the group name to the domain's section of the tree.



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.

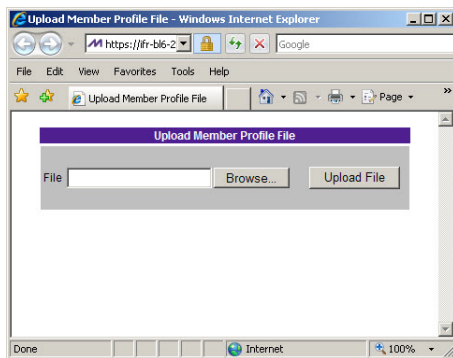
3.2.6 Upload a file of filtering profiles to the tree

1. Select the LDAP domain, and choose Upload Profile from the menu to open the 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 both the refresh message page and the Upload Member Profile File window:



Note: Leave the refresh page open until the file containing the profile has been uploaded.

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



Caution: 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.

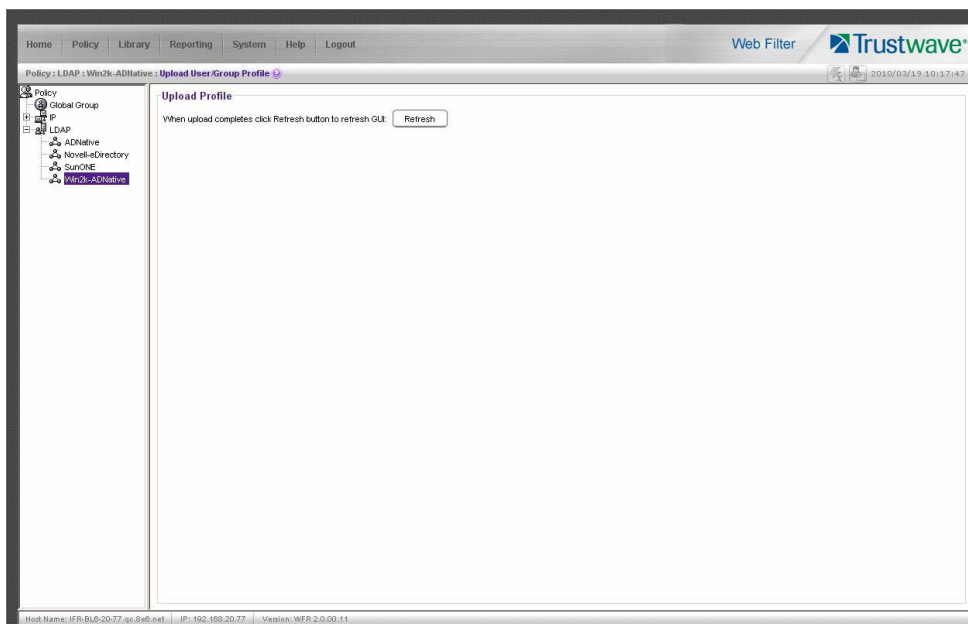


Note: See Appendix D: Profile Format and Rules for examples of valid filtering profile formats to use when creating a list of profiles to be uploaded to the server.



Caution: 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 window informs you to click Reload in order for these changes to be effective.
6. Click the "X" in the upper right corner of the Upload Member Profile File window to close it.
7. Click **Refresh** in the refresh page to refresh the LDAP branch of the tree:



8. After refreshing the page, return to the Upload User/Group Profile window and click **Reload**.

4 Manage Nodes

Once LDAP domains are set up in the Policy 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.

4.1 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.

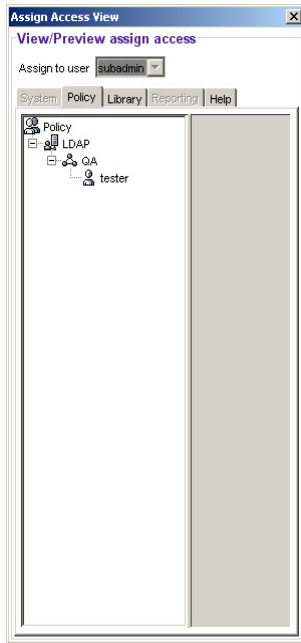
1. Click Assign to at any level of the LDAP Policy tree (domain, group, workstation, member, or container) to open the Assign Access window. In the Assign Access to selected tree nodes frame, the name of the entity (Node Name) displays, along with that node's Assignable status. If the node has already 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:

The screenshot shows a window titled "Assign Access" with a sub-header "Assign access to selected tree nodes". It contains a table with the following data:

Node Name	Assignable	Assigned User
tester	<input checked="" type="checkbox"/>	

Below the table, there is a checkbox for "Unassigned Access" which is unchecked, and a dropdown menu labeled "Assign to user". At the bottom of the window are two buttons: "Preview Assign" and "Apply".

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

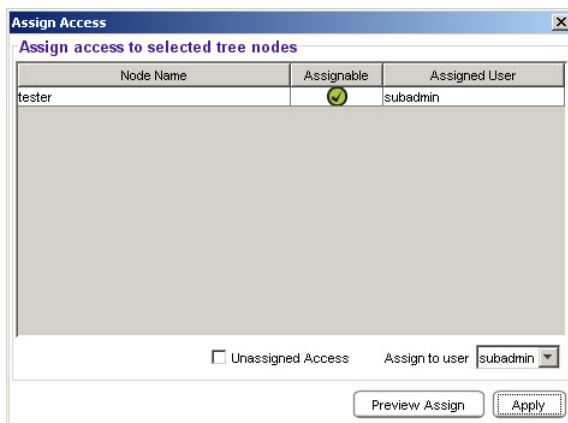


4. Click the Policy, Library, and Help tabs to view the menu topics, sub-topics, and tree nodes currently available to that Sub Admin.
5. Click the "X" in the upper right corner of that window to close it.



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:



7. Click the "X" in the upper right corner of the Assign Access window to close it.



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

4.2 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.

The chart below illustrates the options available for filtering profile creation and maintenance for the entity type:

	Domain	Container	Group	Individual	Workstation
Details	X	X	Member		
Manage Profile Objects	X				
Set Group Priority	X				
Manually Add Workstation / Member /Group	X				
Upload Profile	X				
Profile		X	X	X	X
Exception URL	X	X	X	X	X
Time Profile	X	X	X	X	X
Approved Content	X	X	X	X	X
Web-based Authentication Timeout	X	X	X	X	
Delete	X				
Remove		X	X	X	X
Assign to	X	X	X	X	X



Tips:

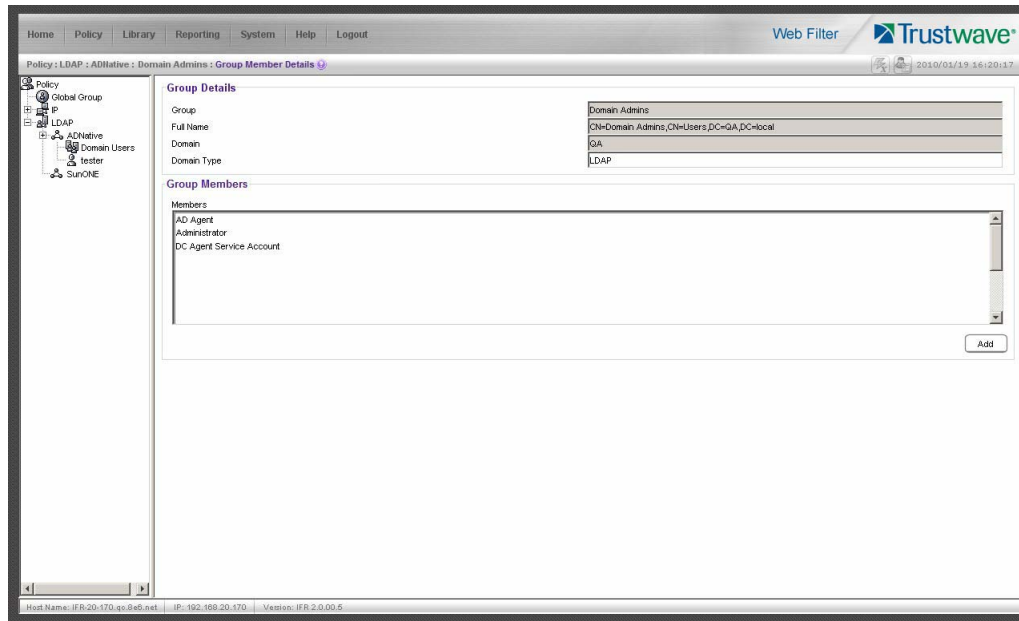
See Assign Sub Admin to an LDAP Node for information on changing the assignment of an LDAP node to another Sub Admin.

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

4.2.1 Add a group member to the tree list

From the domain, select the group and choose Group Member Details from the menu to display the Group/Member Details window.

Figure 15: 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 Group Members frame.

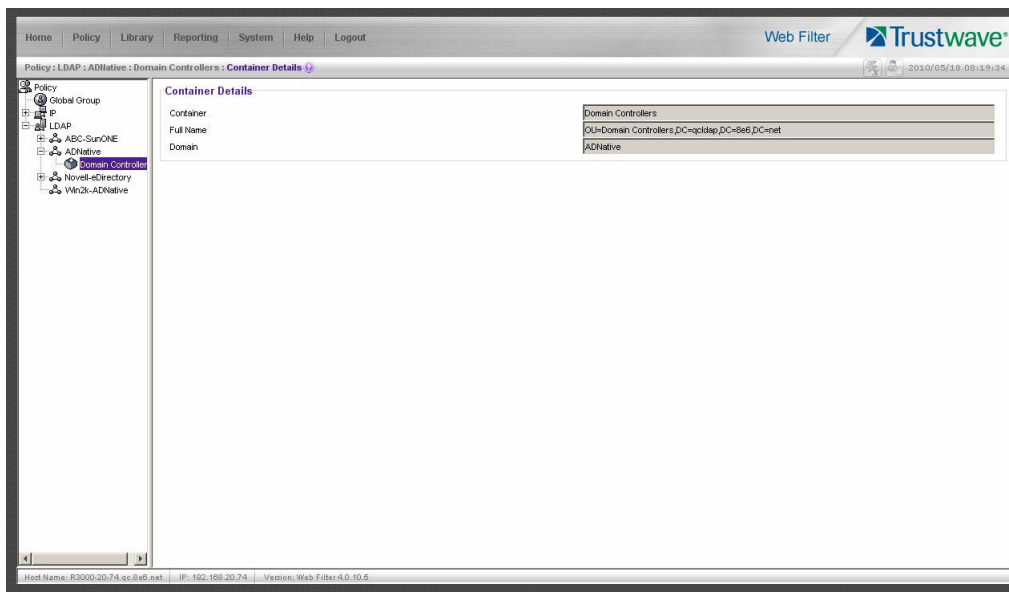
To add a member to the tree list so that a profile can be created for that member:

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

4.2.2 View Container Details

From the Policy tree, select the domain and choose Container Details from the menu to display the Container Details window.

Figure 16: Container Details window



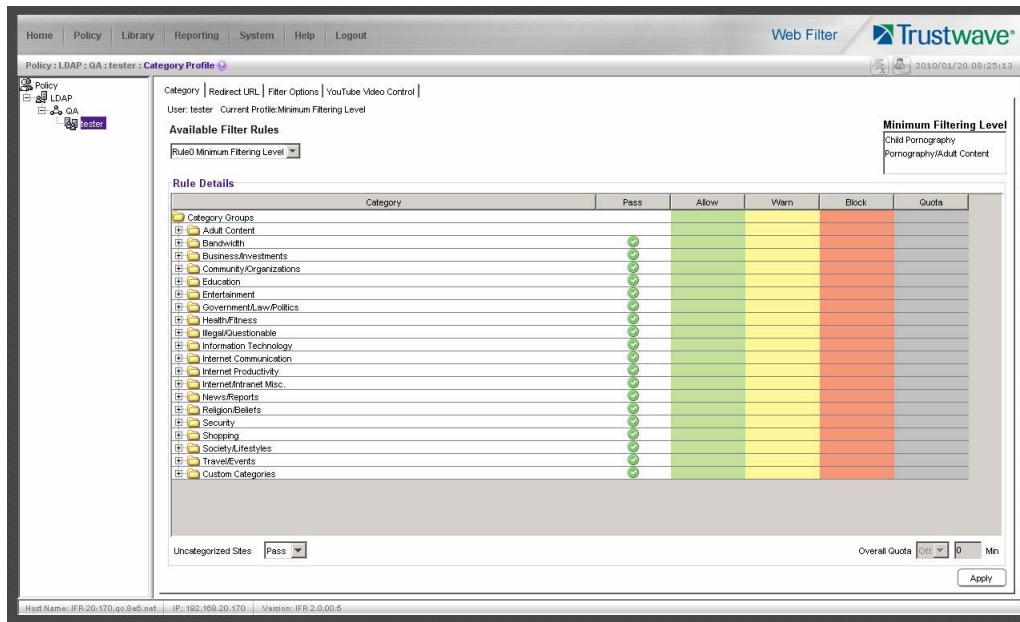
This view only window provides the following information about the container:

- Container - Name assigned to the container on the LDAP server
- Full Name - Distinguished Name for the container
- Domain - Name of the domain in which the container belongs

4.2.3 Add or maintain a node's profile

From the domain, select the node and choose Profile from the menu to display the default Category tab of the Profile window.

Figure 17: 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, Filter Options, and YouTube Video Control tabs comprise the profile string for the entity.

4.2.3.1 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 Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for more information about these windows.

By default, "Rule0 Minimum Filtering Level" displays in the **Available Filter Rules** 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 Trustwave CIPA Compliance", and "Rule5 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 Rules** 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 Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.

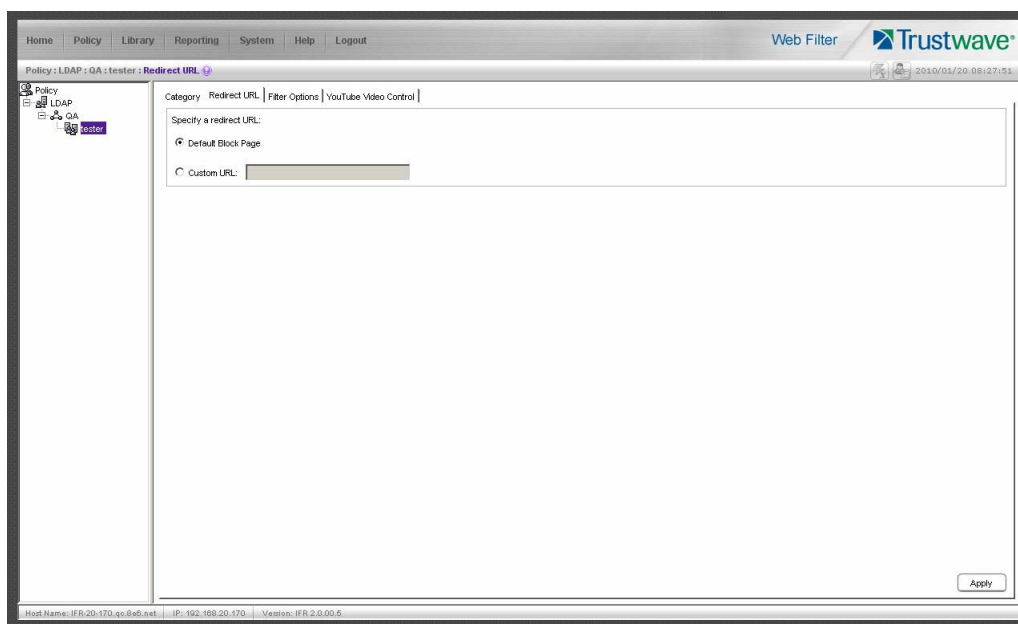
- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned "Off". If turned "On", enter the number of minutes in the **Min** field to indicate when the end user's access to passed library groups/categories with quotas 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.

4.2.3.2 Redirect URL

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

Figure 18: 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".

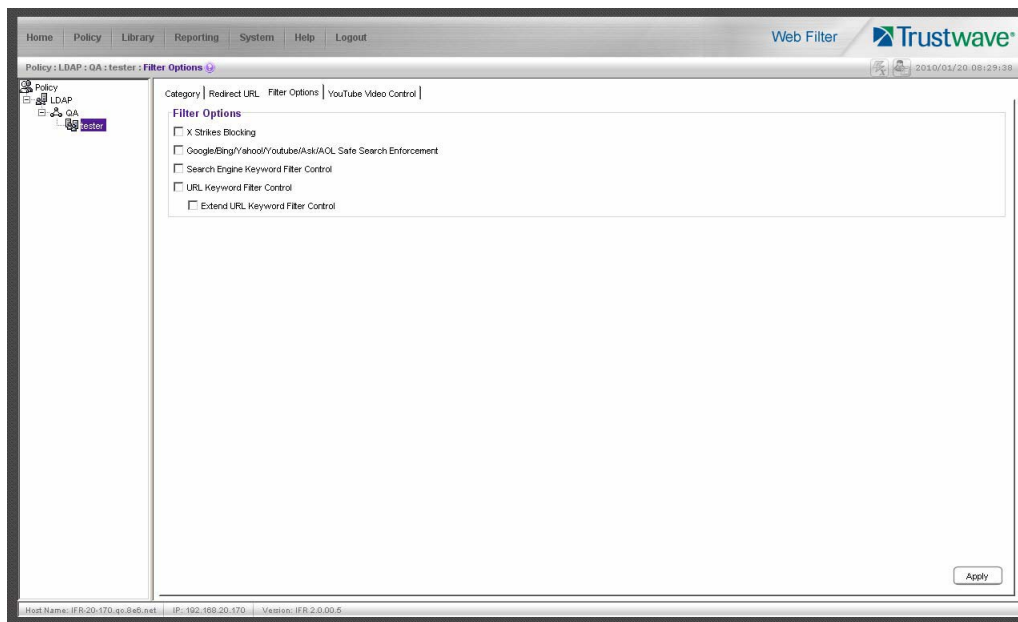
If "Custom URL" is selected, enter the redirect URL in the corresponding text box. Users will be redirected to the designated page at this URL instead of the block page.

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

4.2.3.3 Filter Options

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

Figure 19: 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 check box(es) corresponding to the option(s) to be applied to the filtering profile: "X Strikes Blocking", "Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".



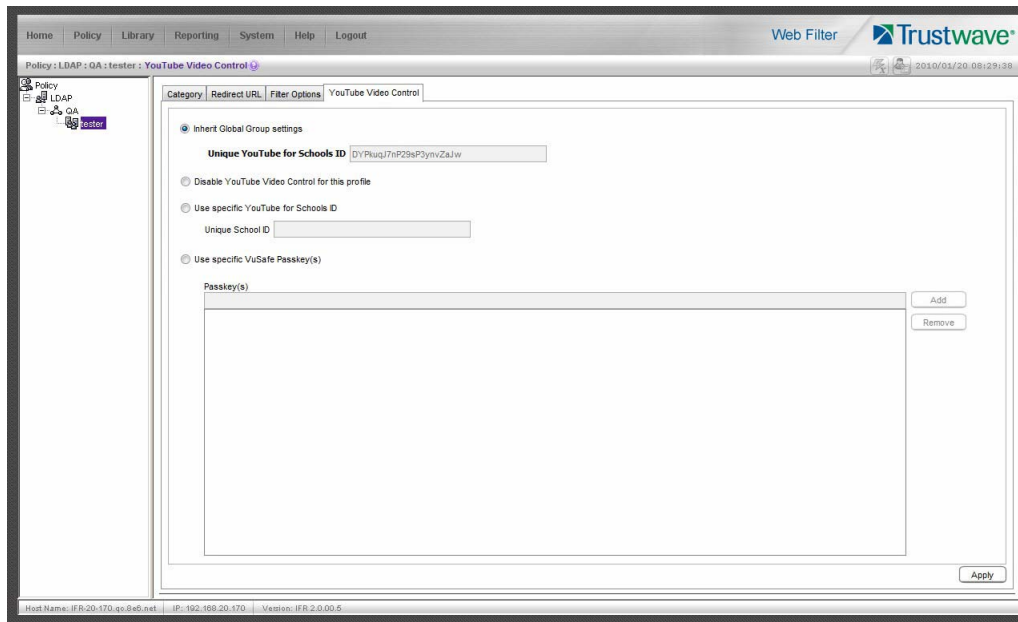
Note: See the Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for information about Filter Options.

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

4.2.3.4 YouTube Video Control

Click the YouTube Video Control tab to display the YouTube Video Control page of the Profile window.

Figure 20: Group Profile window, YouTube Video Control tab, LDAP group



YouTube Video Control is used for specifying YouTube video settings to be applied to the entity's filtering profile.

By default, the profile will "Inherit Global Group settings", which is one of the following options: "Unique YouTube for Schools ID", "VuSafe is currently enabled", or "YouTube Video Control is currently disabled".

4.2.3.4.1 Configure YouTube Video Control settings

1. The profile can be configured to use any one of the following options, independent of Global Group settings:
 - "Inherit Global Group settings" - Click the corresponding radio button to select this option.
 - "Disable YouTube Video Control for this profile" - Click the corresponding radio button to select this option.
 - "Use specific YouTube for Schools ID" - Click the corresponding radio button to select this option, and then enter the **Unique School ID**.



Note: If the Global Group already has this option set, a separate YouTube for Schools ID can be used instead of the Global Group YouTube for Schools ID.

- "Use specific VuSafe Passkey(s)" - Click the corresponding radio button to select this option, and then enter the **Passkey(s)** to be used, clicking **Add** to include each passkey in the list box.



Tip: To remove a passkey from the list box, select it in the list box, and then click **Remove**.

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

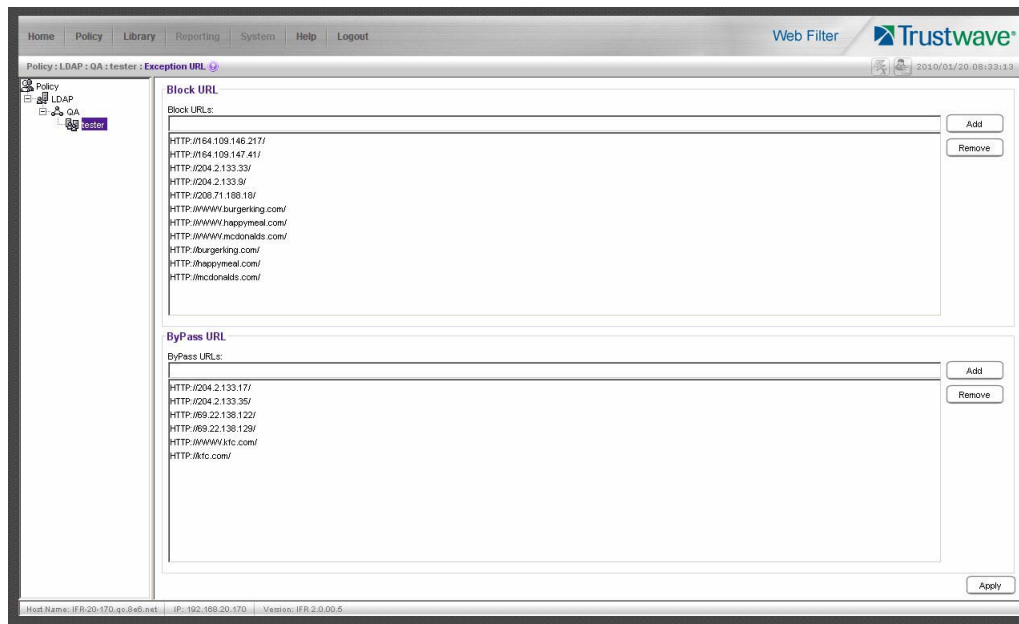


Note: If using YouTube for Schools, be sure to **unblock** YouTube in the user's profile. If using VuSafe, be sure to **block** YouTube in the user's profile.

4.2.4 Add an Exception URL to the profile

From the domain, select the node and choose Exception URL from the menu to display the Exception URL window.

Figure 21: 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 Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator Guide for information on configuring and using the minimum filtering level.

4.2.4.1 Valid 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_wfnj111MU



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

- case-specific entries - these entries are used by the Approved Content feature that blocks or allows end user accessibility to specific YouTube video URLs
- wildcard entry format that uses an asterisk (*) followed by a period (.) and then the URL, such as:
*.coors.com

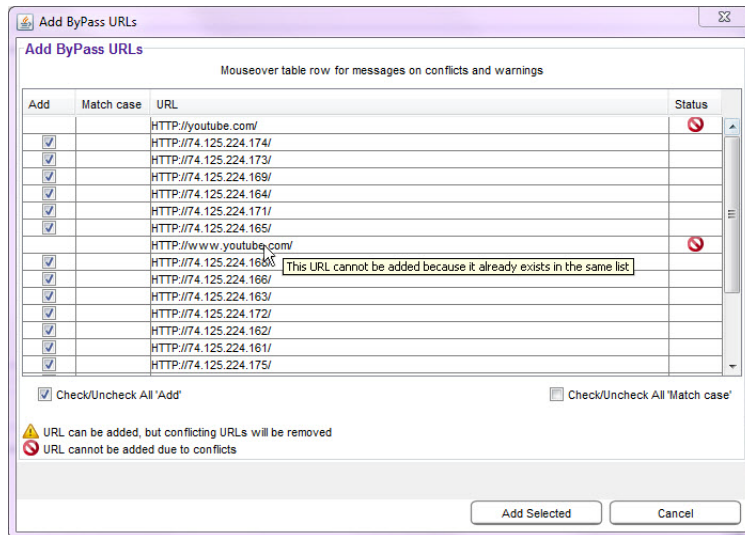


Tip: The minimum number of levels that can be entered for a wildcard entry is three (e.g. *.yahoo.com) and the maximum number of levels is six (e.g. *.mail.attachments.message.yahoo.com).

4.2.4.2 Add URLs to Block URL or ByPass URL frame

To block or bypass specified URLs, in the Block URL or the ByPass URL frame:

1. Type the URL to be blocked in the **Block URLs** field, or the URL to be bypassed in the **ByPass URLs** field.
2. Click **Add** to open the Add Block URLs / Add Bypass URLs window to view all corresponding URLs found by the query:



This window includes the pre-populated "Add" check box preceding each URL in the table. Uncheck any check box corresponding to a URL you do not want to include in your list.



Tips:

Click the "Check/Uncheck All 'Add'" check box at the bottom of this window to toggle between selecting or de-selecting all Add column check boxes in this window.

See the subsequent Status column messages and icons sub-section for information regarding conflicting URLs found by the query.

If a multi-level URL query was executed (as in <http://yahoo.com/mail>), the Match case column contains an empty check box for each entry in the table. Check the check box corresponding to a URL entry you want to designate as being case-specific. The URL entry made by the end user must exactly match this entry in order for the URL to be blocked or bypassed, as set up in this window.



Tips:

Click the "Check/Uncheck All 'Match case'" check box at the bottom of this window to toggle between selecting or de-selecting all Match case column check boxes in this window.

Click Cancel to close this window without making any selections.

3. Click **Add Selected** to close the window and to add your selection(s) in the appropriate URL list box.

4.2.4.2.1 Status column messages and icons

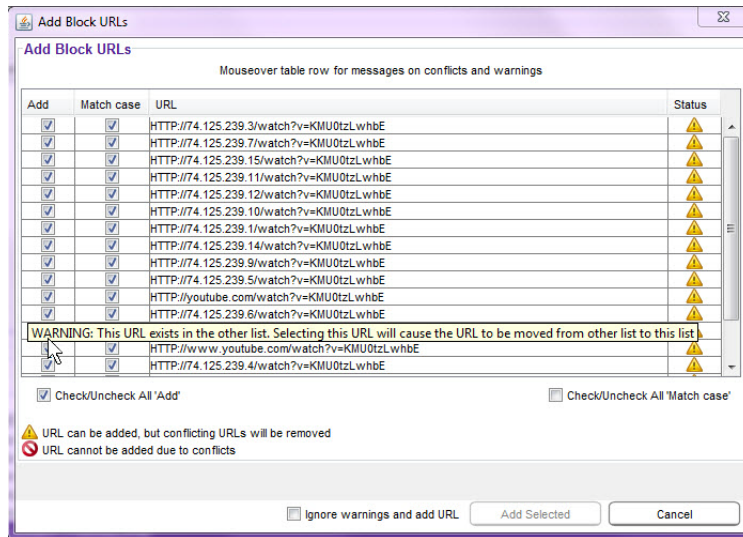
If conflicting URL entries are found by the query, the following message displays at the top of the query results window: "Mouseover table row for messages on conflicts and warnings".

In the Status column of a URL with a conflict, one of two icons displays: either the yellow warning triangle containing an exclamation point, or the red circle with a line through it. Mousing over the affected URL displays a tooltip message indicating the URL already exists in the list, and the type of action that can be performed, if any.

URL conflict types are identified by the legend at the bottom of the window:

- "URL can be added, but conflicting URLs will be removed" - Preceded by the yellow warning triangle icon containing an exclamation point, this type of conflict indicates the URL entry found by the query is already included in the other frame of the Exception URL window (ByPass URL or Block URL).

When a URL is found in both bypass and block lists, the “Ignore warnings and add URL” check box displays to the left of the Add Selected button at the bottom of the window:



Clicking this check box activates the Add Selected button. Clicking **Add Selected** closes the window and moves the selected URLs to the opposite frame in the Exception URL window.

- “URL cannot be added due to conflicts” - Preceded by the red circle icon with a line through it, this type of conflict indicates the URL is already included in the Exception URL list.

If a URL found by the query results is already included in the current list, it will not include a check box in the Add column since it cannot be added again.

4.2.4.3 Remove URLs from Block URL or ByPass URL frame

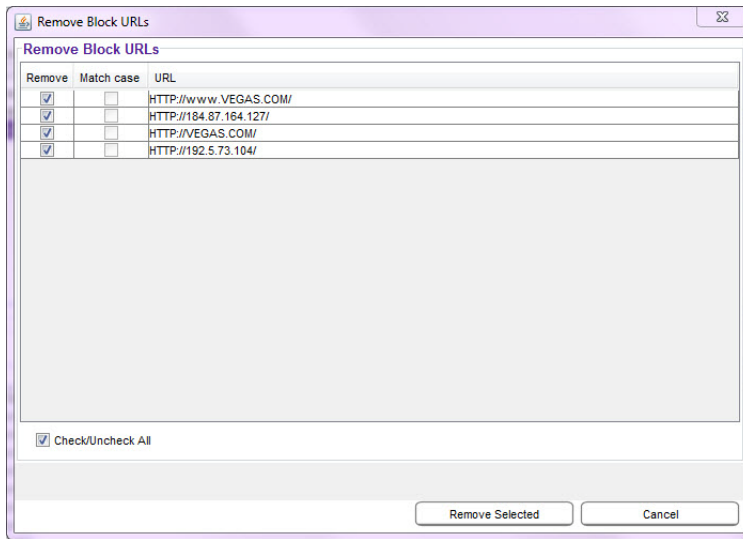
To remove URLs from the Block URL or the ByPass URL frame:

1. Select a URL to be removed from the Block URL / ByPass URL list box; your selection populates the Block URLs field / ByPass URLs field.



Tip: Choose a non-IP address URL to maximize results to be returned by the URL query.

2. Click **Remove** to open the Remove Block URLs / Remove ByPass URLs window to view all corresponding URLs found by the query:



This window includes the pre-populated "Remove" check box preceding each URL in the table. Uncheck any check box corresponding to a URL you do not want to remove from your list.



Tip: Clicking the "Check/Uncheck All" check box at the bottom of this window toggles between selecting or de-selecting all check boxes in this window..

3. Click **Remove Selected** to close the window and to remove your selection(s) from the appropriate URL list box.

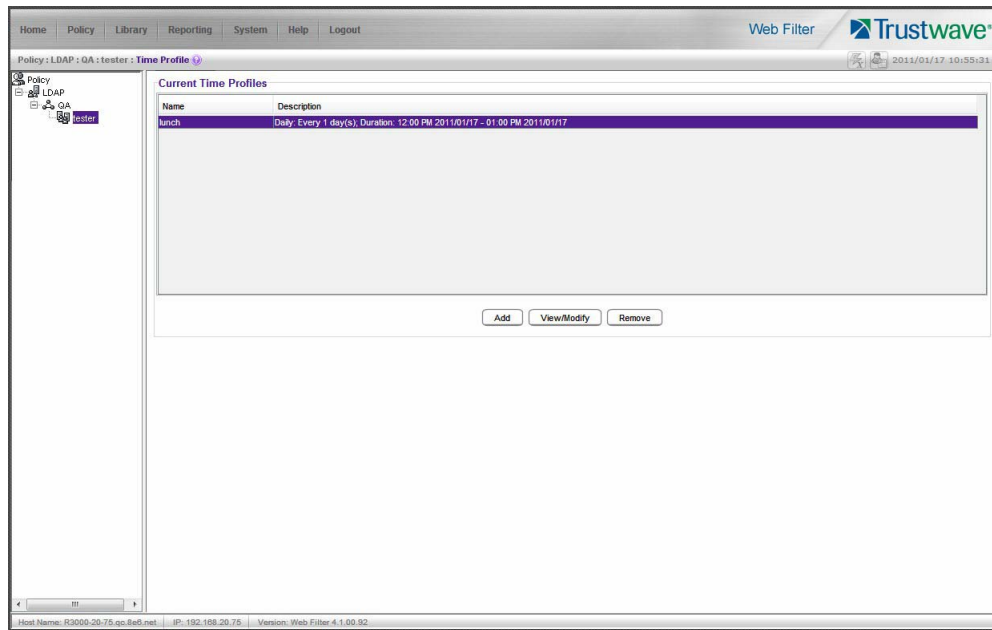
4.2.4.4 Apply settings

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

4.2.5 Create a Time Profile for the node

From the domain, select the node and choose Time Profile from the menu to display the Time Profile window.

Figure 22: Time Profile window, LDAP group



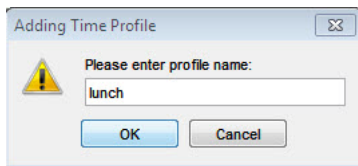
This window is used for setting up or modifying a filtering profile to be activated at a specified time.

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.

4.2.5.1 Add a Time Profile

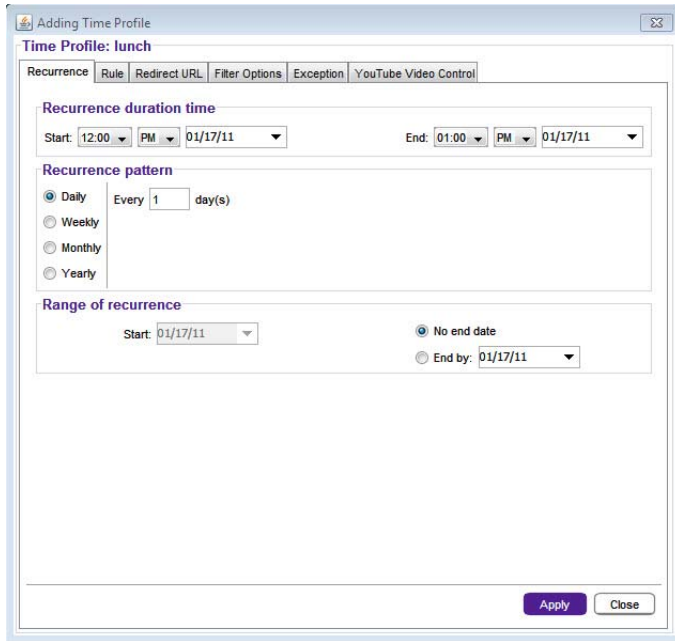
To create a time profile:

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



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

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



- In the Recurrence duration time frame, specify **Start** and **End** time range criteria:
 - 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.
 - Indicate whether this time slot is "AM" or "PM".
 - 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 box:



In this 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.

- In the Recurrence pattern frame, choose the frequency this time profile will use:

- **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:
 - a. week of the month: "First" - "Fourth", or "Last"
 - b. 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:
 - a. week of the month: "First" - "Fourth", or "Last"
 - b. day of the month: "Sunday" - "Saturday", "Day", "Weekday", "Weekend"
 - c. month: "January" - "December".

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

If "2" is entered and the "First" "Monday" of "February" are selected, this profile will be used every two years on the first Monday in February. For example, if the current month and year are January 2011, the first Monday in February this year would be the 7th. The next time this profile would be used will be in February 2013.

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 URL, Filter Options, Exception, YouTube Video Control) and specify criteria to complete the time profile. (See Category Profile, Redirect URL, Filter Options, Exception URL, and YouTube Video Control in this sub-section for information on entries to make in these 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 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.

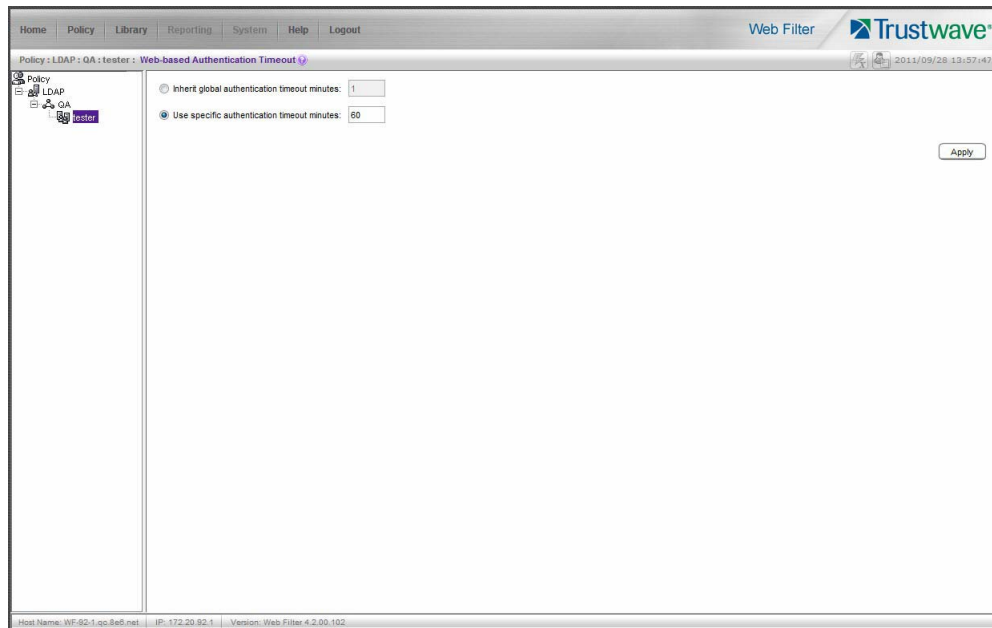


Caution: If there is an error in a time profile, the Description for that time profile displays in red text. Select that time profile and click **View/Modify** to make any necessary corrections.

4.2.6 Set Tier 2, Tier 3 timeout minutes

From the domain, select the node and choose Web-based Authentication Timeout from the menu to display the Web-based Authentication Timeout window.

Figure 23: Web-based Authentication Timeout window, LDAP group



Note: This window is only active if “Tier 2” or “Tier 3” and its time-based fallback option is enabled in the Enable/Disable Authentication window.

This window is used for determining the number of minutes the end user’s Web-based authentication filtering profile will be active.

If Tier 3 and its time-based fallback option is enabled in **System | Authentication | Enable/Disable Authentication** window, the end user will only use the set number of timeout minutes for Internet usage if the Java applet does not launch in his/her browser.

To set the duration of Internet usage for this profile:

1. Choose one of the following options by clicking its corresponding radio button:
 - **Inherit global authentication timeout minutes** - By default this option is selected, and time-out minutes set in Enable/Disable Authentication for the selected tier type display greyed-out in the field to the right. For Tier 2, the default number is “30” timeout minutes, and for Tier 3, that number is “1”.
Applying this option to the entity’s profile will immediately activate the number of timeout minutes set for the tier type in Enable/Disable Authentication. The entity will inherit any modified settings if the tier type or number of minutes is modified in that window.
 - **Use specific authentication timeout minutes** - Selecting this option lets you configure the number of timeout minutes for the end user to access the Internet via his/her authentication profile.
2. After making modifications in this window, click **Apply**.

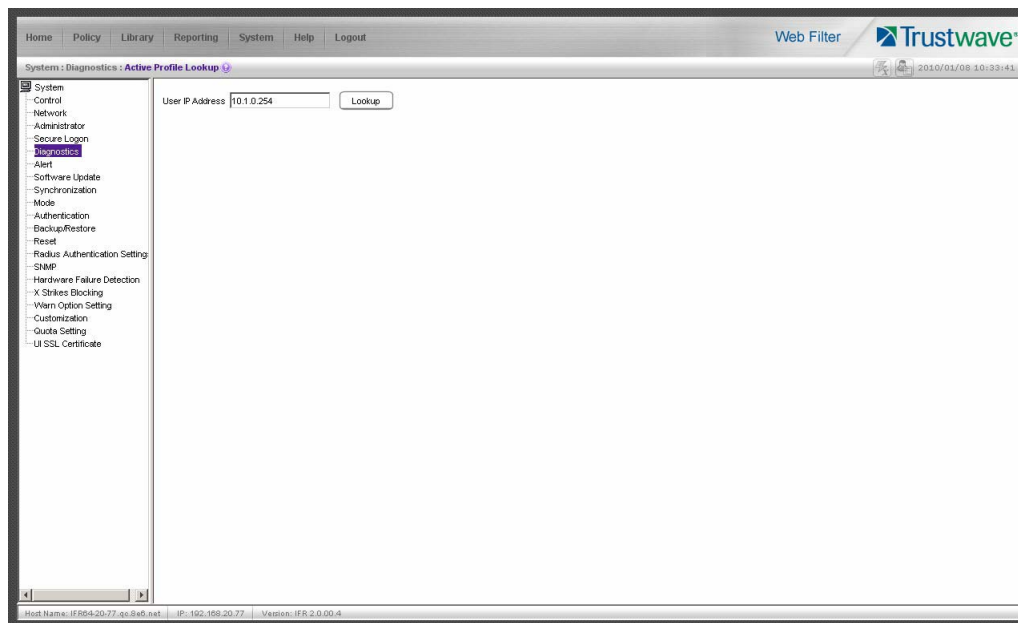
4.2.7 Remove a node's profile from the tree

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

4.3 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.

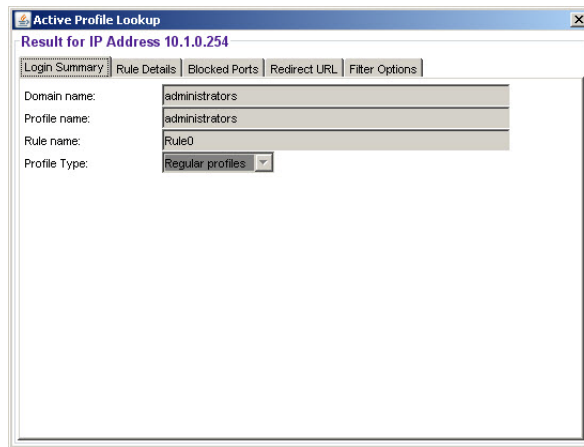
1. In the System section of the user interface, select **Diagnostics | Active Profile Lookup** to display the Active Profile Lookup window



Note: Only filtering profile lookups for LDAP nodes will be addressed in this sub-section. Please refer to the Trustwave Web Filter Administrator Guide or the Web Filter portion of the Trustwave WFR Administrator 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 Policy section of the Web Filter, and each node must have a filtering profile.

2. In the **User IP Address** field, enter the IP address of the end user.
3. Click **Lookup** to verify whether or not an LDAP profile is active for that IP address.

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



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 spending 100 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!/Youtube/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 box to close it.

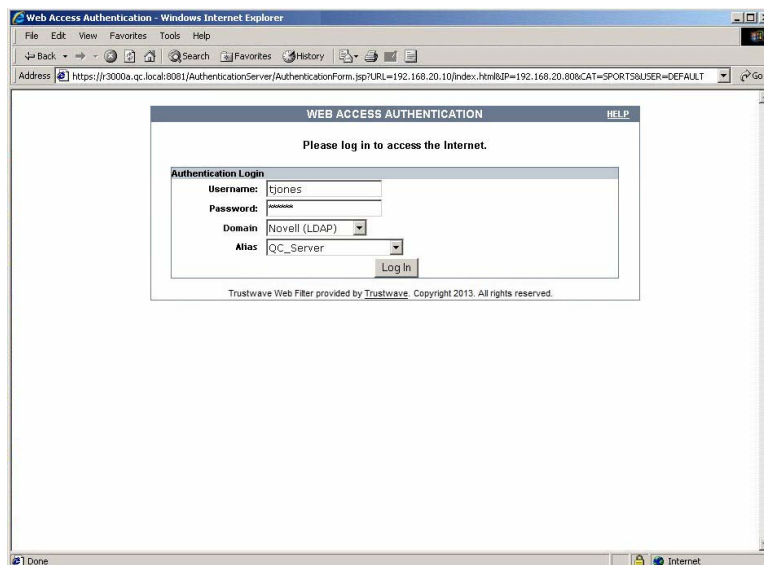
5 Authentication Deployment

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

5.1 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.

Figure 24: 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).



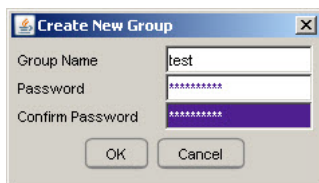
Note: On WFR units, the Usage Graphs window can be used for viewing and analyzing the number of end users who have been authenticated, and their usage of the Internet. See Usage Graphs from the Reporting screen section of the Web Filter section of the Trustwave WFR Administrator Guide for more information about this reporting tool.

5.1.1 Test Web-based authentication settings

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

5.1.1.1 Create an IP Group, "test"

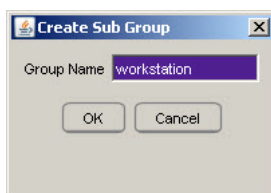
1. Click the IP branch of the tree.
2. Select Add Group from the menu to open the Create New Group dialog box:



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.

5.1.1.2 Create a Sub-Group, "workstation"

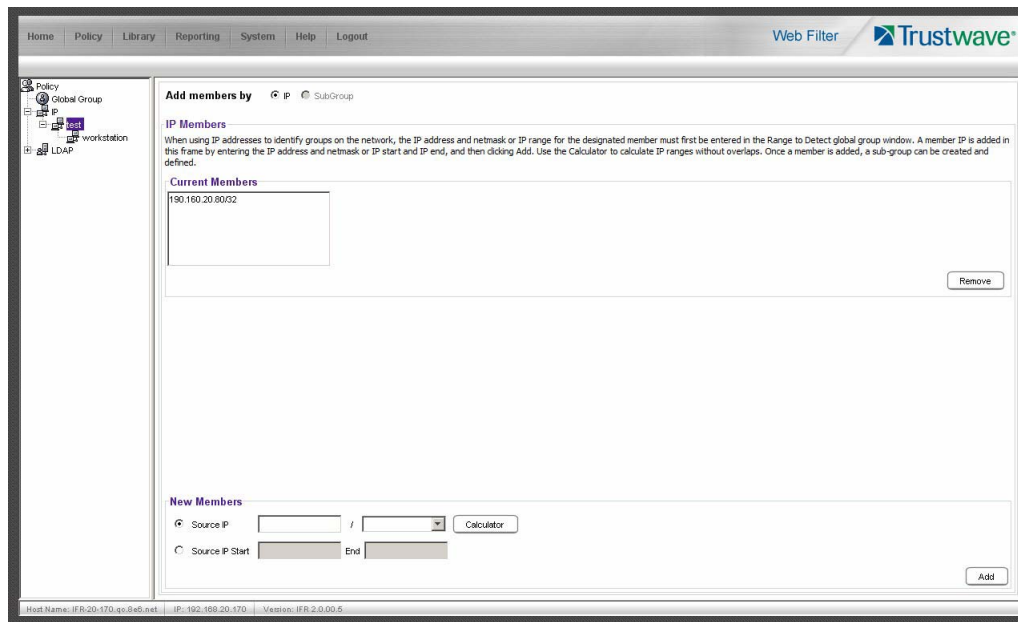
1. Select the IP Group from the tree.
2. Click Add Sub Group in the menu to open the Create Sub Group dialog box:



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

5.1.1.3 Set up "test" with a 32-bit net mask

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

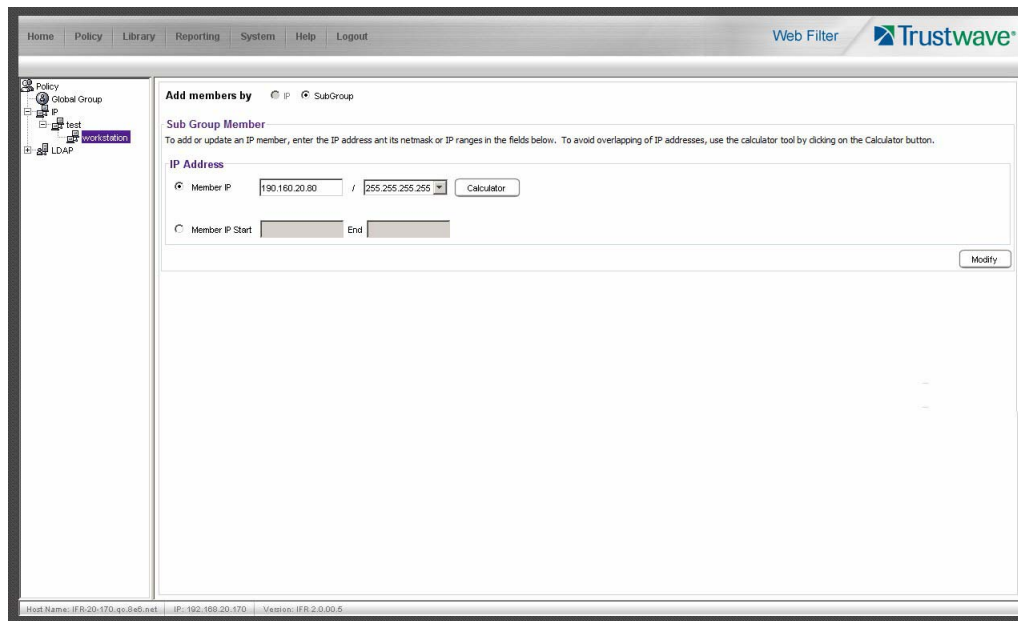


3. Click the radio button corresponding to "Source IP".
4. Enter the **Source IP** address of the workstation, and select *255.255.255.255* as the subnet mask.
5. Click **Add** to include the IP address in the Current Members list box.

5.1.1.4 Give "workstation" a 32-bit net mask

1. Select the IP Sub-Group "workstation" from the tree.

2. Click Members in the menu to display the 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**.

5.1.1.5 Block everything for the Sub-Group

1. Select the IP Sub-Group "workstation" from the tree.

- Click Sub Group Profile in the menu to display the Sub Group Profile window:

The screenshot shows the Trustwave Web Filter interface. The top navigation bar includes Home, Policy, Library, Reporting, System, Help, and Logout. The main content area is titled 'Web Filter' and 'Trustwave'. The left sidebar shows a tree view with 'Global Group', 'test', and 'workstation' under 'LDAP'. The main area displays the 'Sub Group Profile' window for the 'workstation' group. The 'Available Filter Rules' dropdown is set to 'Custom Profile'. The 'Rule Details' table shows a list of categories with columns for Pass, Allow, Warn, Block, and Quota. The 'Block' column is highlighted in red, indicating that all categories are set to be blocked. The 'Minimum Filtering Level' is set to 'Child Pornography/Pornography/Adult Content'. The 'Uncategorized Sites' dropdown is set to 'Block'. The 'Overall Quota' is set to '0' with a 'Min' button. The 'Apply' button is at the bottom right.

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content				●	
Bandwidth				●	
Business/Investments				●	
Community/Organizations				●	
Education				●	
Entertainment				●	
Government/Law/Publics				●	
Health/Fitness				●	
Illegal/Questionable				●	
Information Technology				●	
Internet Communication				●	
Internet Productivity				●	
Internet/Intranet Misc.				●	
News/Reports				●	
Religion/Beliefs				●	
Security				●	
Shopping				●	
Society/Lifestyles				●	
Travel/Events				●	
Custom Categories				●	

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

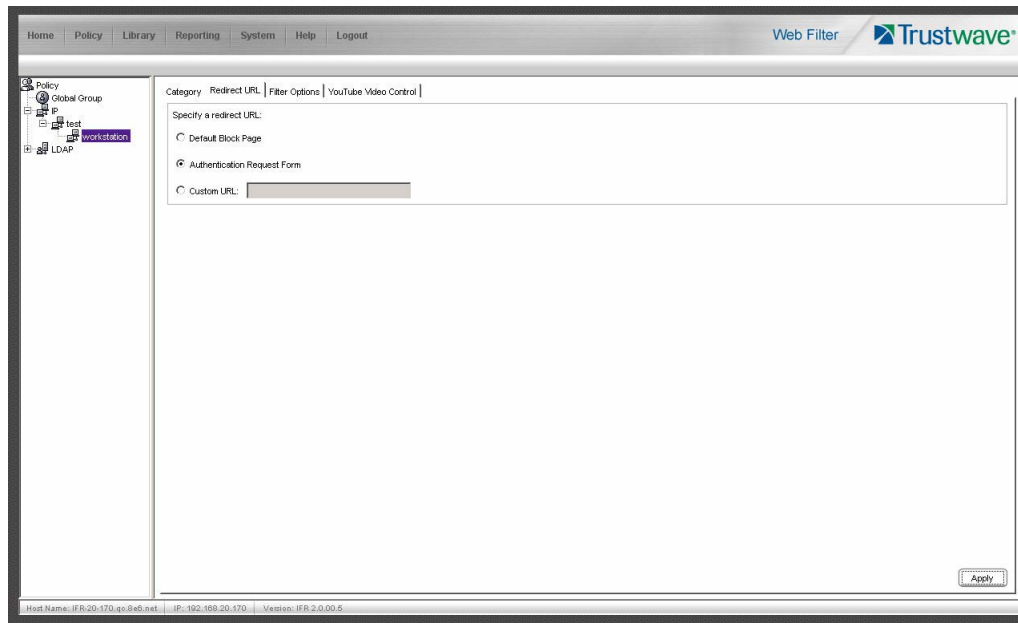


Tip: Blocks of category groups can be moved by clicking the first category group, and then pressing the Shift key on your keyboard while clicking the last category group, and then clicking in the Block column.

- For **Uncategorized Sites**, select "Block".
- Click **Apply**.

5.1.1.6 Use Authentication Request Page for redirect URL

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



2. Select "Authentication Request Form".

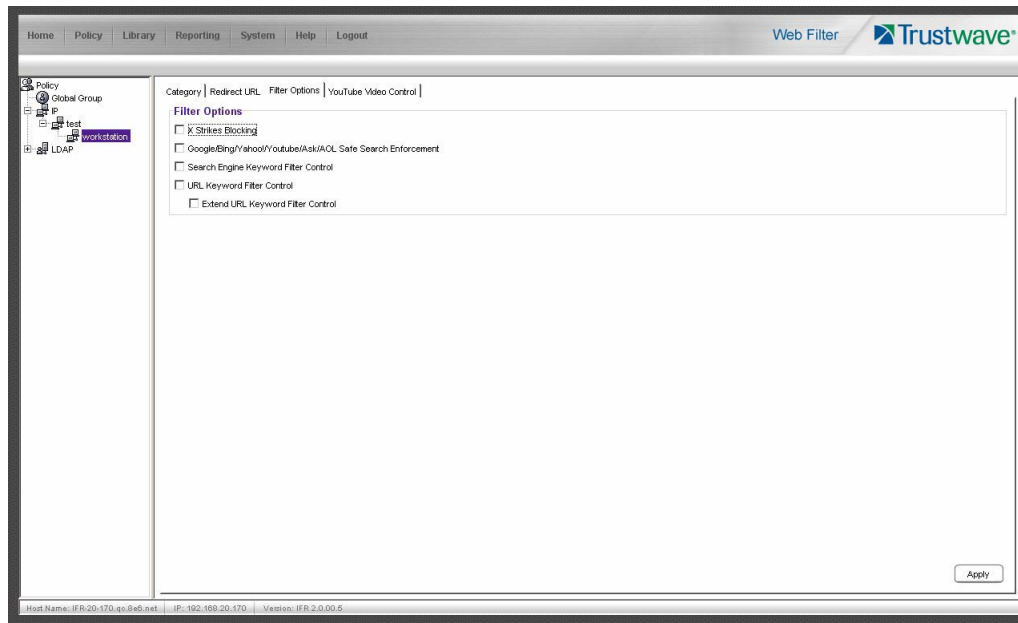


Note: The host name of the Web Filter will be used in the redirect URL of the Authentication Request Form, not the IP address. Be sure a forward/reverse DNS entry for the Web Filter is made on the DNS server.

3. Click **Apply**.

5.1.1.7 Disable filter options

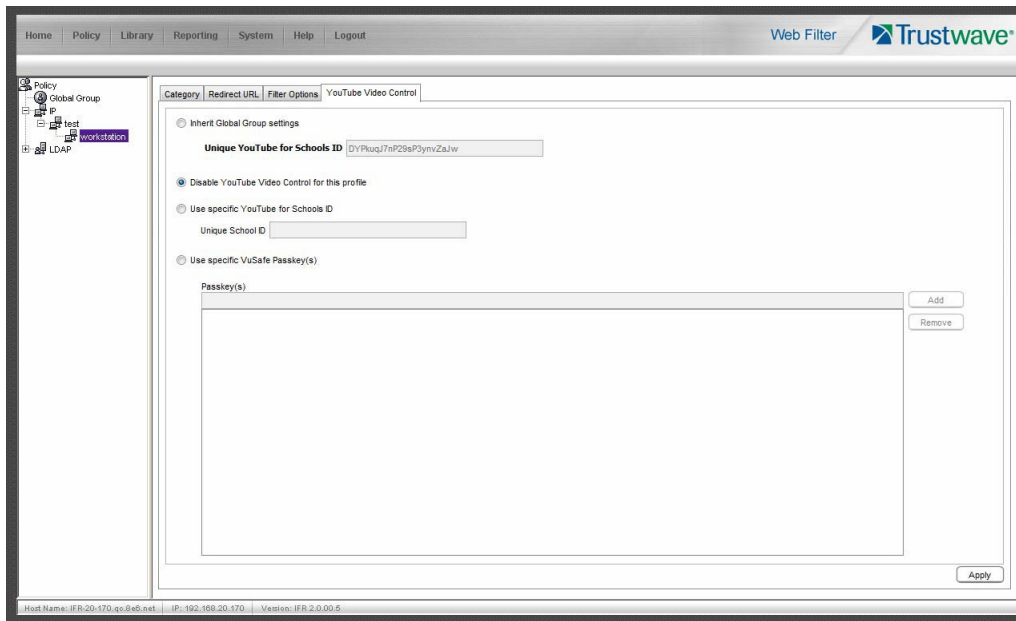
1. Click the Filter Options tab to display the Filter options page:



2. Uncheck all the check boxes: "X Strikes Blocking", "Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".
3. Click **Apply**.

5.1.1.8 Disable YouTube Video Control

1. Click the YouTube Video Control tab to display the YouTube Video Control page:



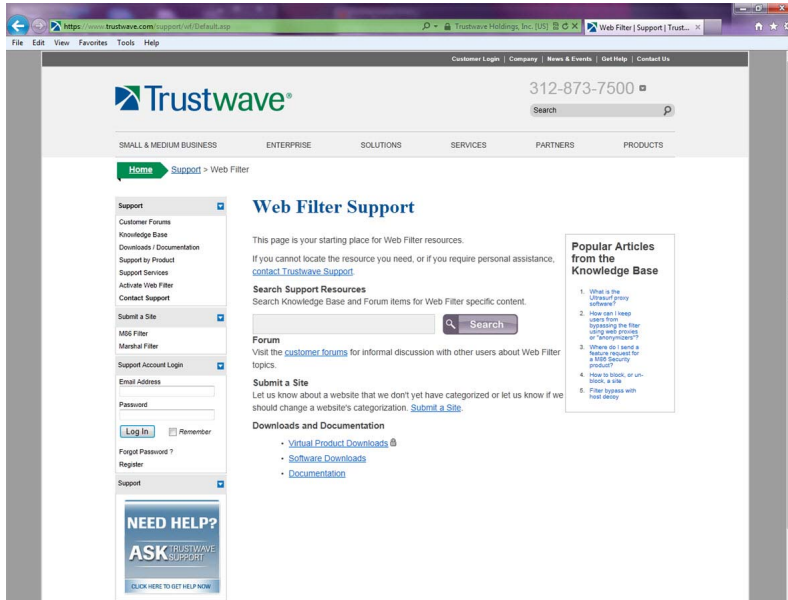
2. Click "Disable YouTube Video Control for this profile".
3. Click **Apply**.

5.1.1.9 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 Web Filter:

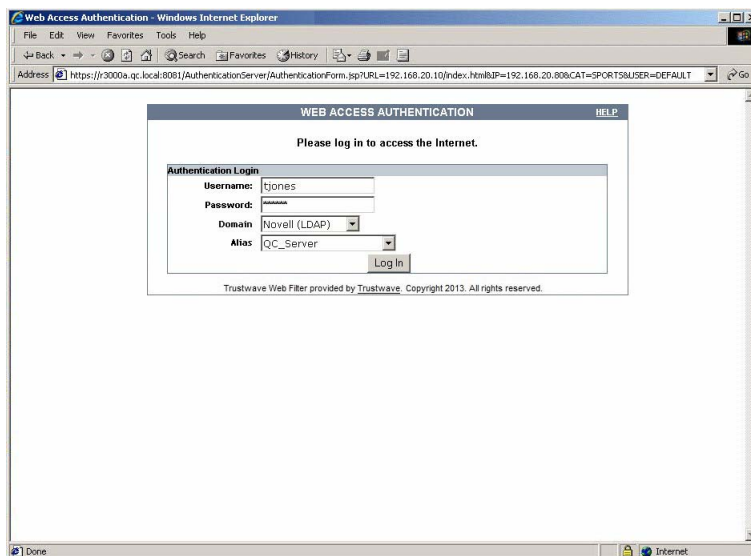


2. Enter a URL in the **Address** field of the browser window.



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

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



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.

5.1.2 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.

5.2 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.

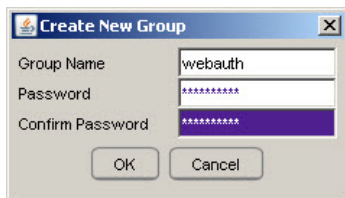
- If Tier 1 net use based authentication will be used: Go to the Activate net use based authentication sub-section for instructions on testing the login script and modifying the Global Group Profile for authenticating users.

5.2.1 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 Web Filter.

5.2.1.1 Create a new IP Group, “webauth”

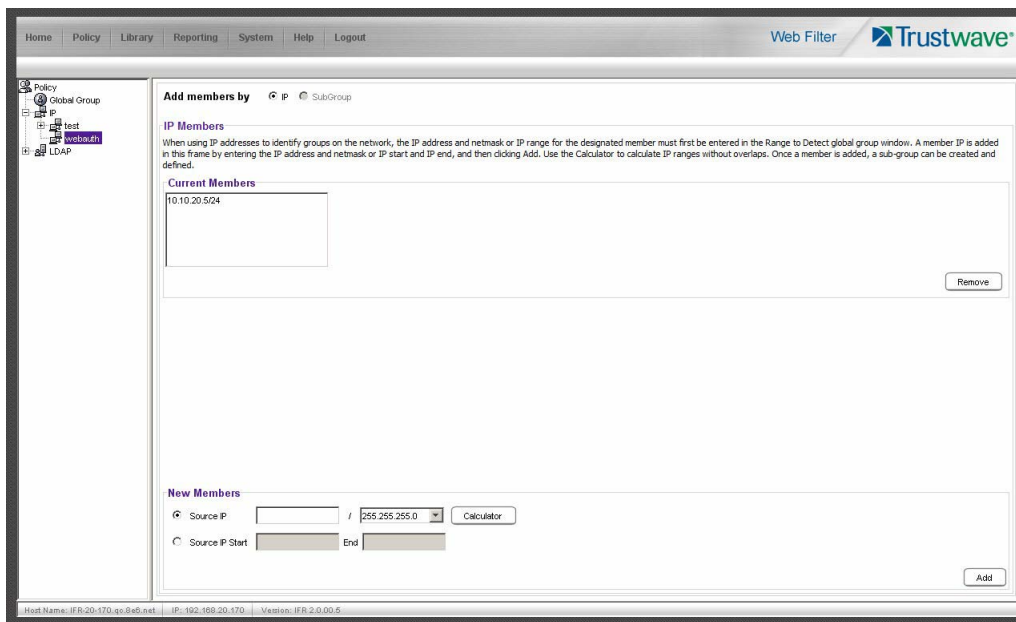
1. Click the IP branch of the tree.
2. Select Add Group from the menu to open the Create New Group dialog box:



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.

5.2.1.2 Set “webauth” to cover users in range

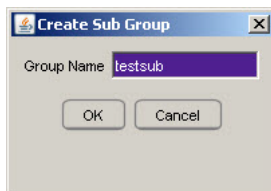
1. Select the IP group “webauth” from the tree.
2. Click Members in the menu to display the Members window:



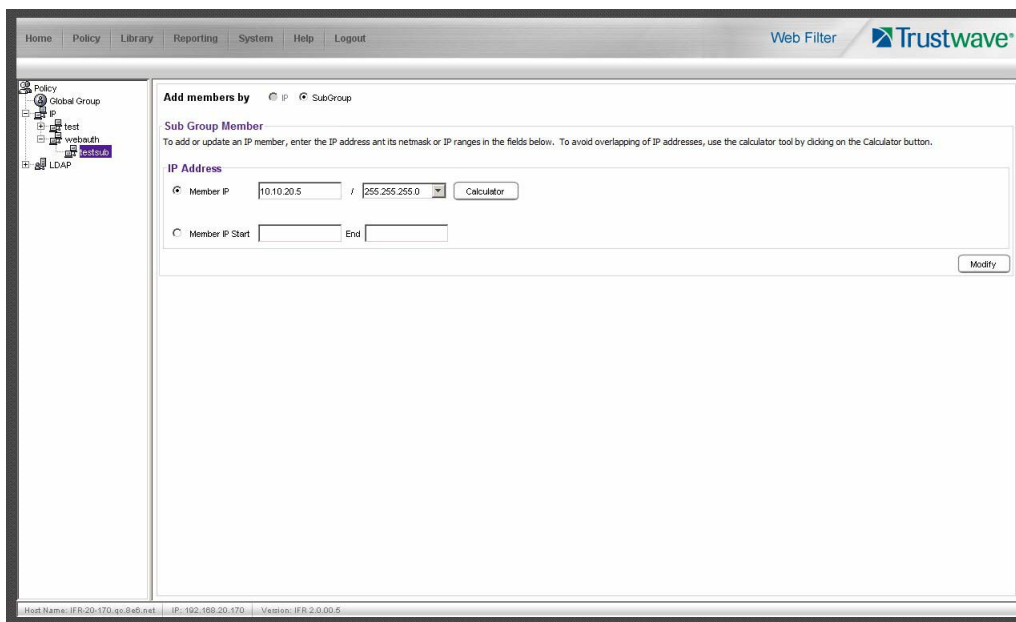
3. Click the radio button corresponding to "Source IP".
4. Enter the **Source IP** address of the workstation and specify the subnet mask for the range of user IP addresses of users to be authenticated.
5. Click **Add** to include the IP address range in the Current Members list box.

5.2.1.3 Create an IP Sub-Group

1. Select the IP Group "webauth" from the tree.
2. Click Add Sub Group in the menu to open the Create Sub Group dialog 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 menu to display the 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**.

5.2.1.4 Block everything for the Sub-Group

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

The screenshot shows the Trustwave Web Filter interface. On the left, a tree view shows the hierarchy: Policy > Global Group > IP > test > webauth > subgroups. The main window is titled 'Category | Redirect URL | Filter Options | YouTube Video Control'. Below the title bar, it says 'Group: testsub Current Profile: Custom Profile'. There are two tabs: 'Available Filter Rules' and 'Minimum Filtering Level'. The 'Available Filter Rules' tab is active, showing a dropdown menu set to 'Custom Profile'. Below this is a table with the following columns: Category, Pass, Allow, Warn, Block, and Quota. The 'Block' column is highlighted in red. The 'Minimum Filtering Level' tab is also visible, showing 'Child Pornography' and 'Pornography/Adult Content'. At the bottom of the window, there is a section for 'Uncategorized Sites' with a dropdown set to 'Block' and an 'Overall Quota' set to '0' with a 'Min' button. An 'Apply' button is at the bottom right.

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 Productivity					
Internet/Intranet Misc.					
News/Reports					
Religion/Beliefs					
Security					
Shopping					
Society/Lifestyles					
Travel/Events					
Custom Categories					

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

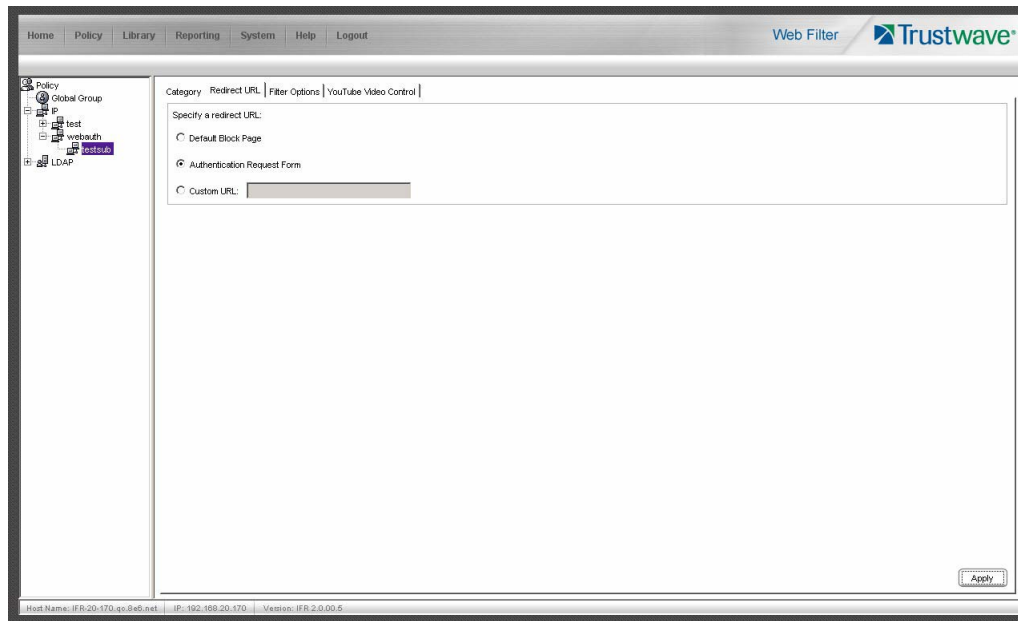


Tip: Blocks of category groups can be moved by clicking the first category group, and then pressing the Shift key on your keyboard while clicking the last category group, and then clicking in the Block column.

4. For **Uncategorized Sites**, select "Block".
5. Click **Apply**.

5.2.1.5 Use Authentication Request Page for redirect URL

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



2. Select "Authentication Request Form".



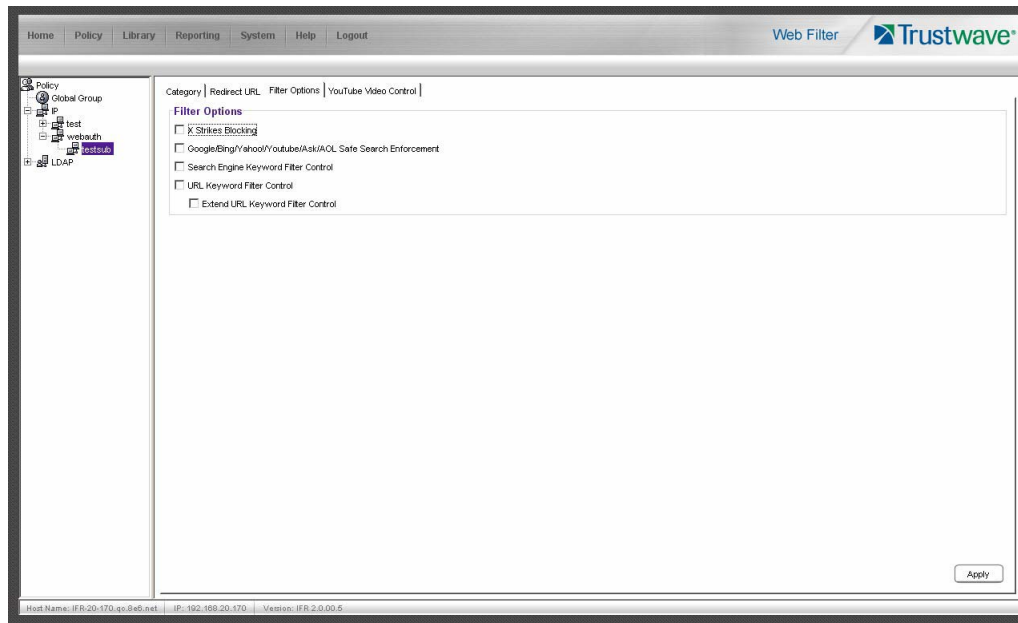
Note: Since the Authentication Request Form radio button selection uses the host name of the server—not the IP address—be sure there is a DNS resolution for the host name.

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.

5.2.1.6 Disable filter options

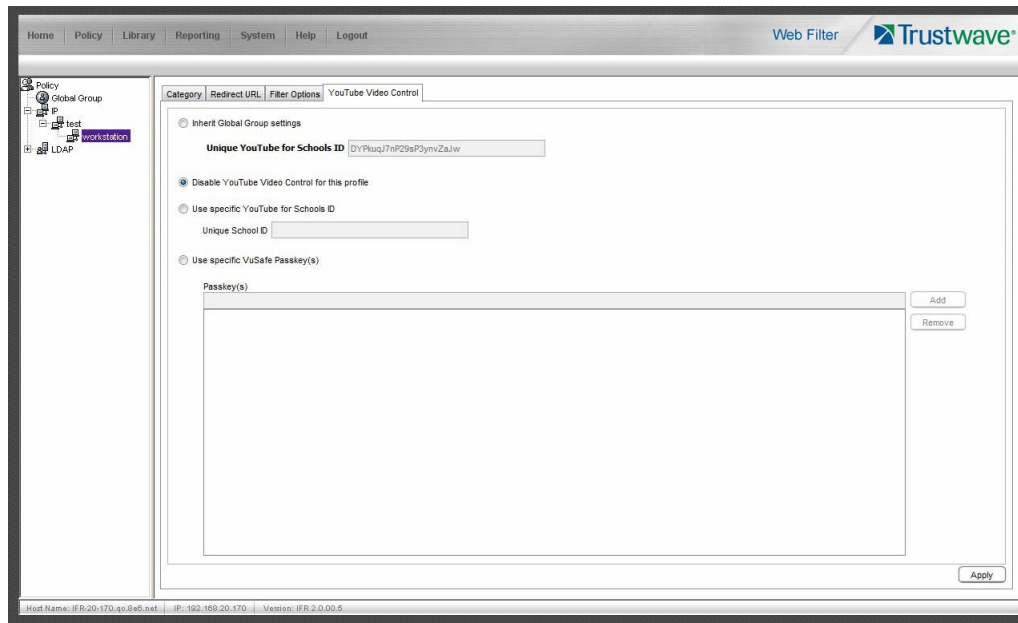
1. Click the Filter Options tab to display the Filter options page:



2. Uncheck all the check boxes: "X Strikes Blocking", "Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement", "Search Engine Keyword Filter Control", "URL Keyword Filter Control", and "Extend URL Keyword Filter Control".
3. Click **Apply**.

5.2.1.7 Disable YouTube Video Control

1. Click the YouTube Video Control tab to display the YouTube Video Control page:

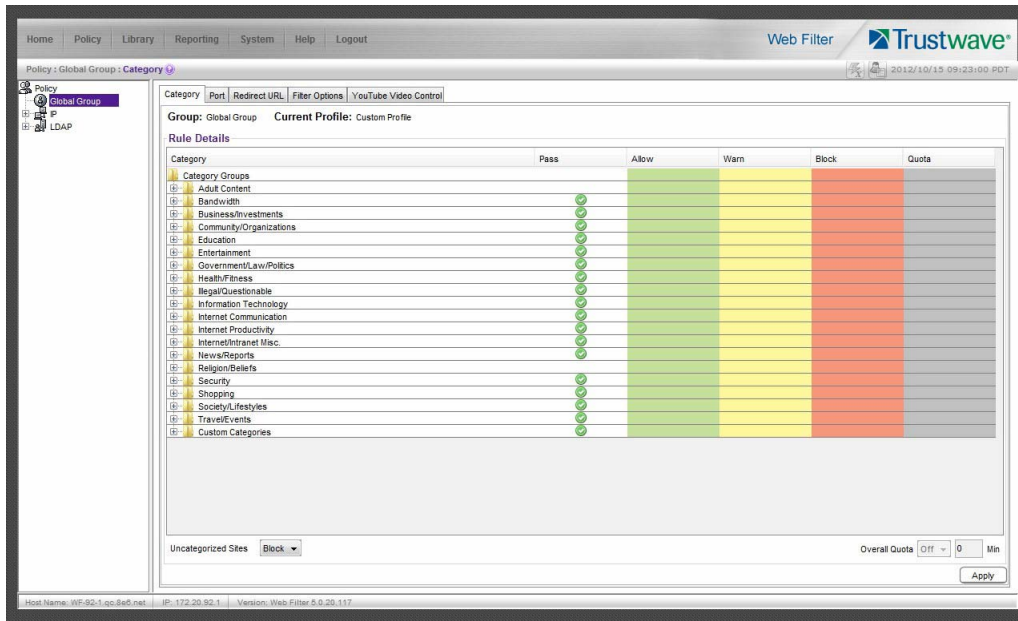


2. Click "Disable YouTube Video Control for this profile".
3. Click **Apply**.

5.2.1.8 Set Global Group to filter unknown traffic

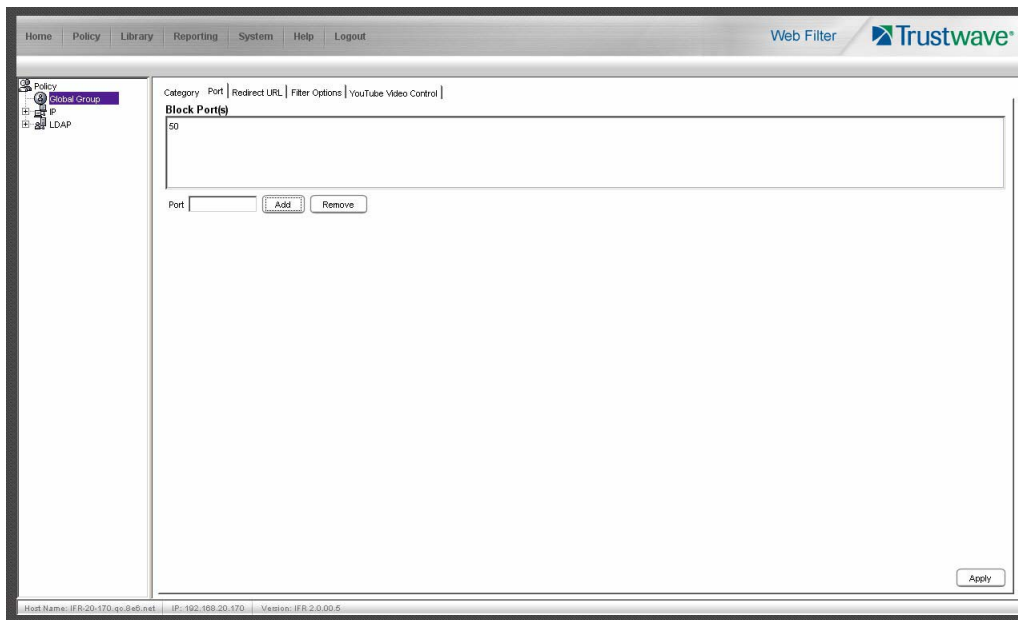
1. Click Global Group in the tree to open the menu.

2. Select Global Group Profile to display the Category tab of the Profile window:



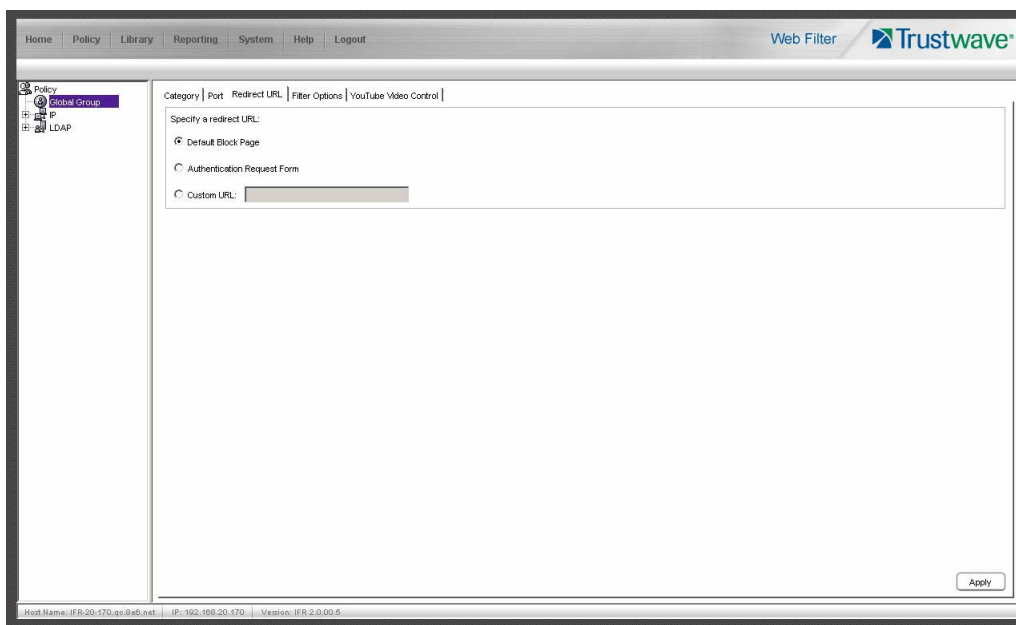
- a. In the Category Profile page, select categories to block, pass, white list, or assign a warn setting, and indicate whether uncategorized sites should pass, trigger a warn message for the end user, or be blocked.
- b. Click **Apply**.

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

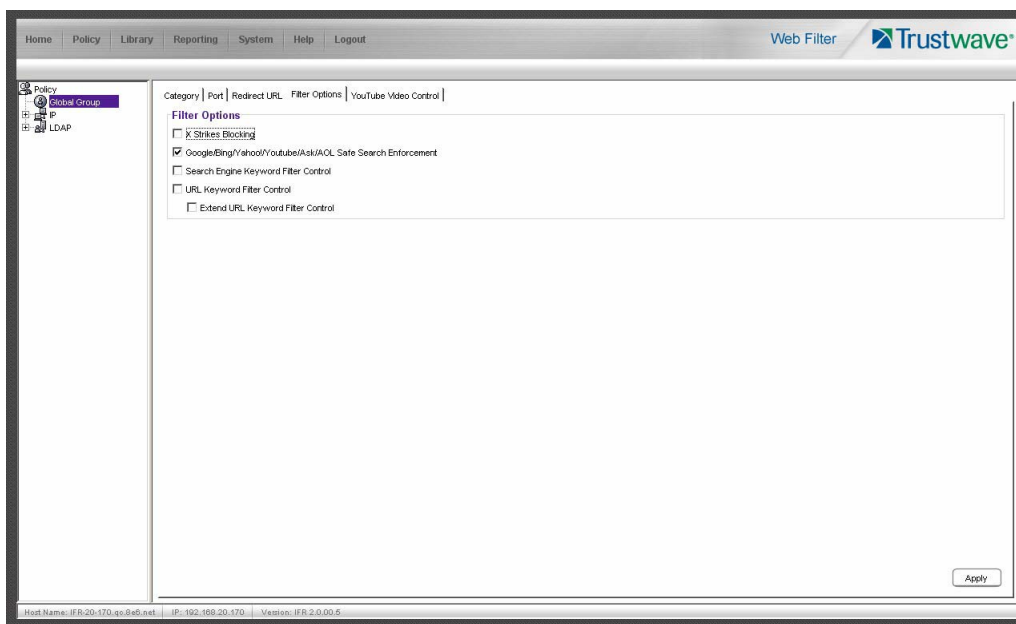


- a. In the Port page, enter the **Port** number to be blocked.

- b. Click **Add** to include the port number in the Block Port(s) list box. After entering all port numbers to be blocked, click **Apply**.
4. Click the Default Redirect URL tab to display the Redirect URL page:



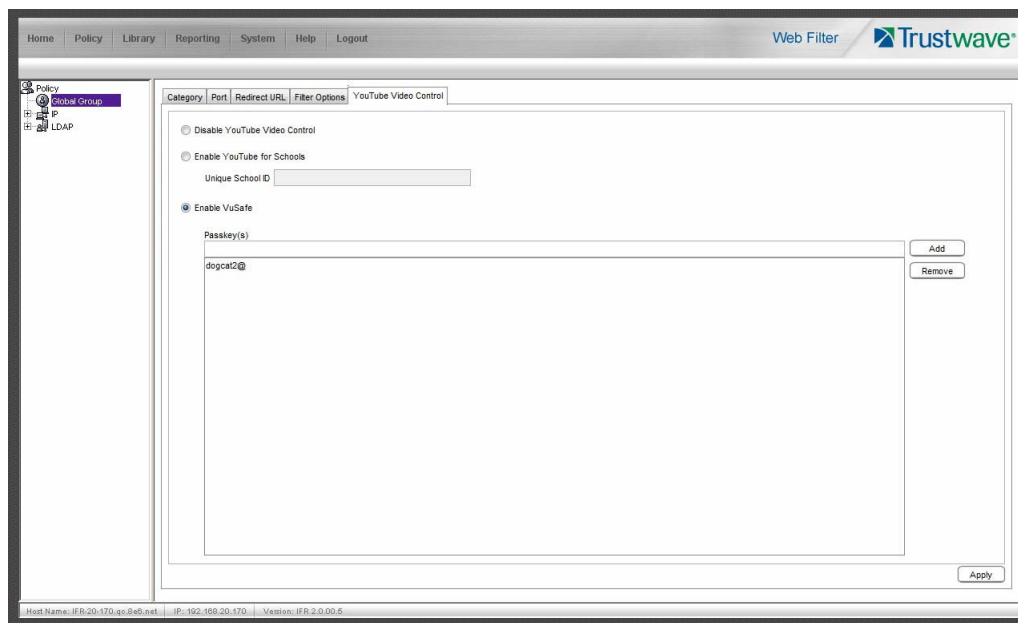
- a. Select "Default Block Page".
 - b. Click **Apply**.
5. Click the Filter Options tab to display the Filter Options page:



- a. Select filter options to be enabled.

b. Click **Apply**.

6. Click the YouTube Video Control tab to display the YouTube Video Control page:



a. Specify the YouTube Video Control option to use, or disable this option.

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.

5.2.2 Activate Web-based authentication for the Global Group

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

5.2.2.1 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.

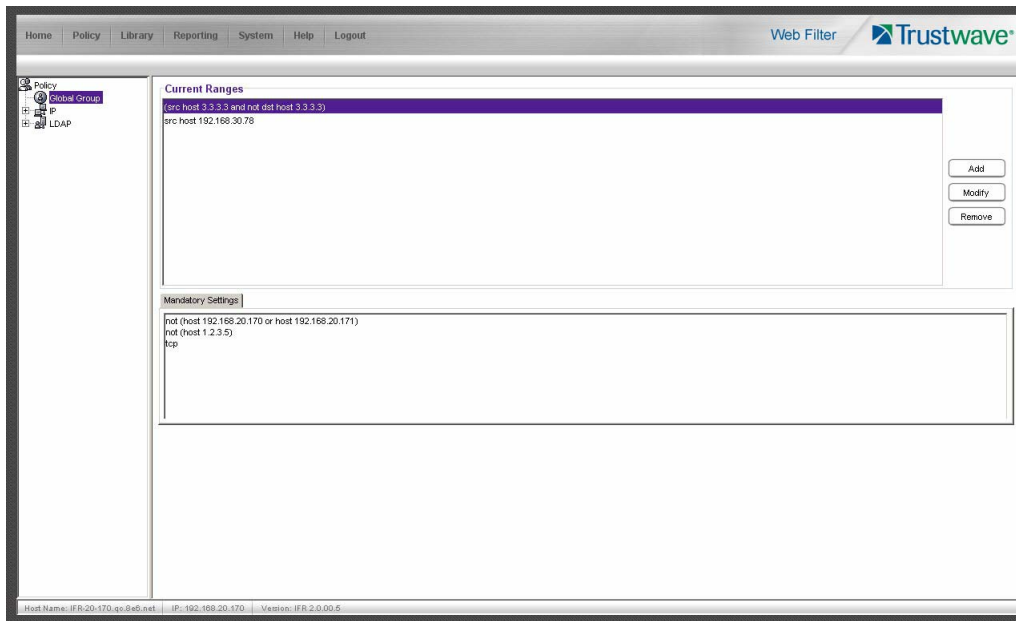
5.2.2.2 Block Web access, logging via Range to Detect



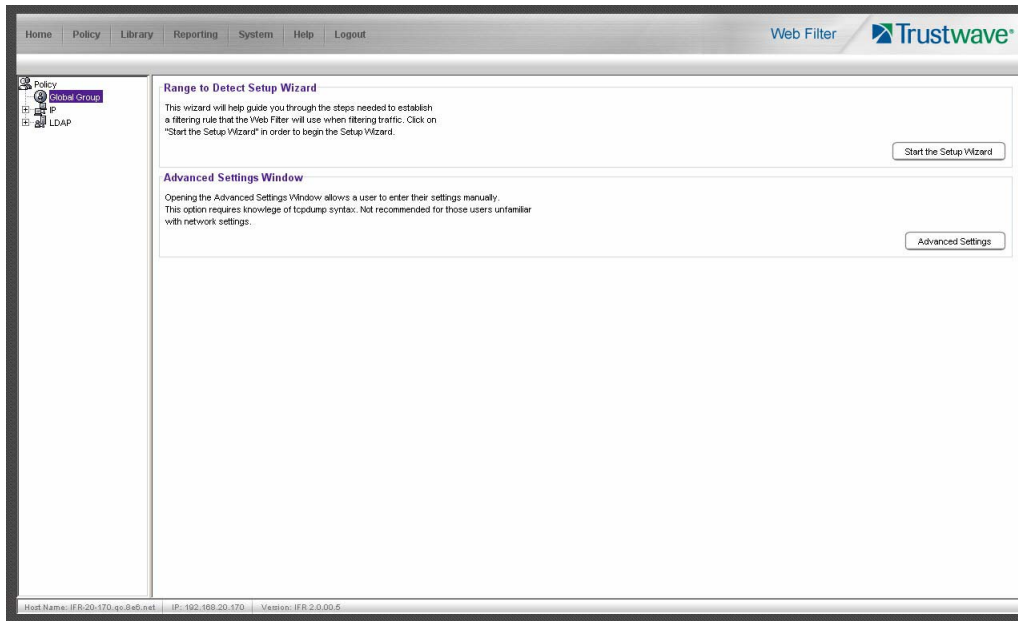
Note: Segments of network traffic should not be defined if using the firewall mode.

5.2.2.2.1 Range to Detect Settings

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



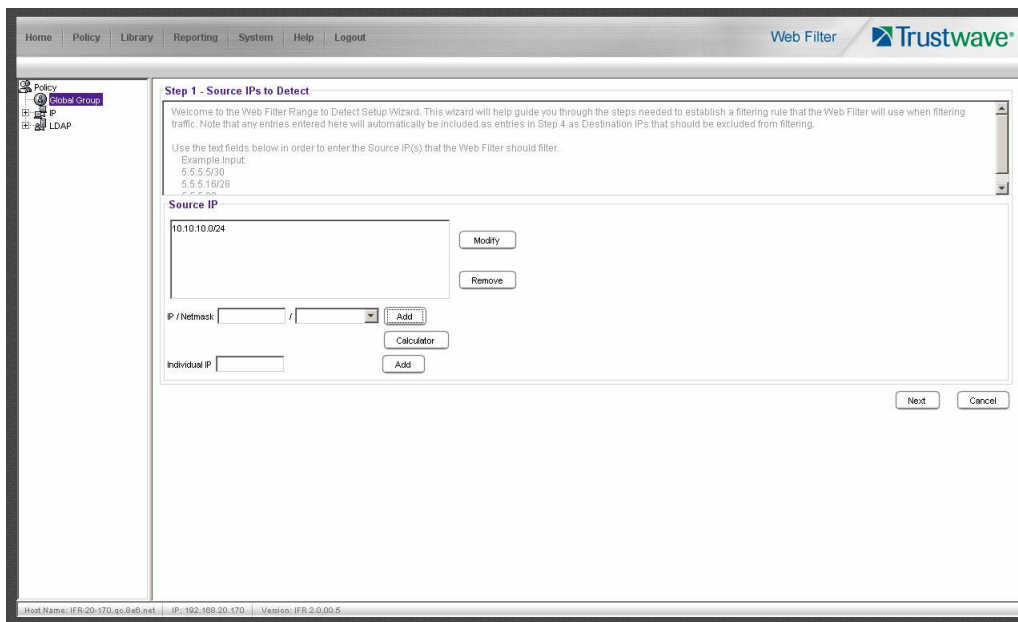
3. In the Current Ranges frame, click **Add** to go to the next Settings page:



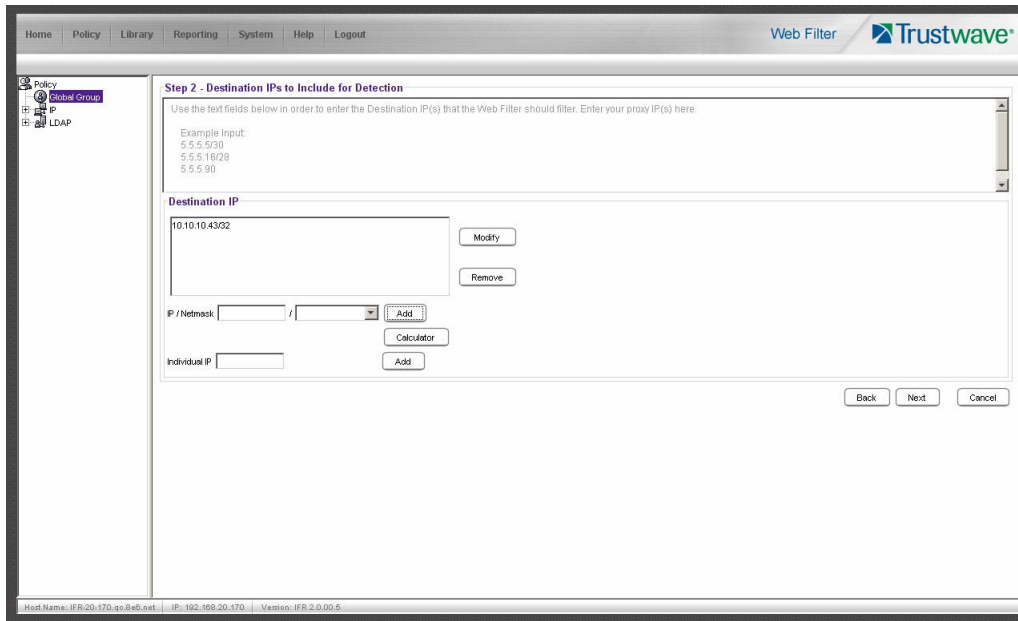
4. Click **Start the Setup Wizard** to display Step 1 of the Range to Detect Setup Wizard:

5.2.2.2 Range to Detect Setup Wizard

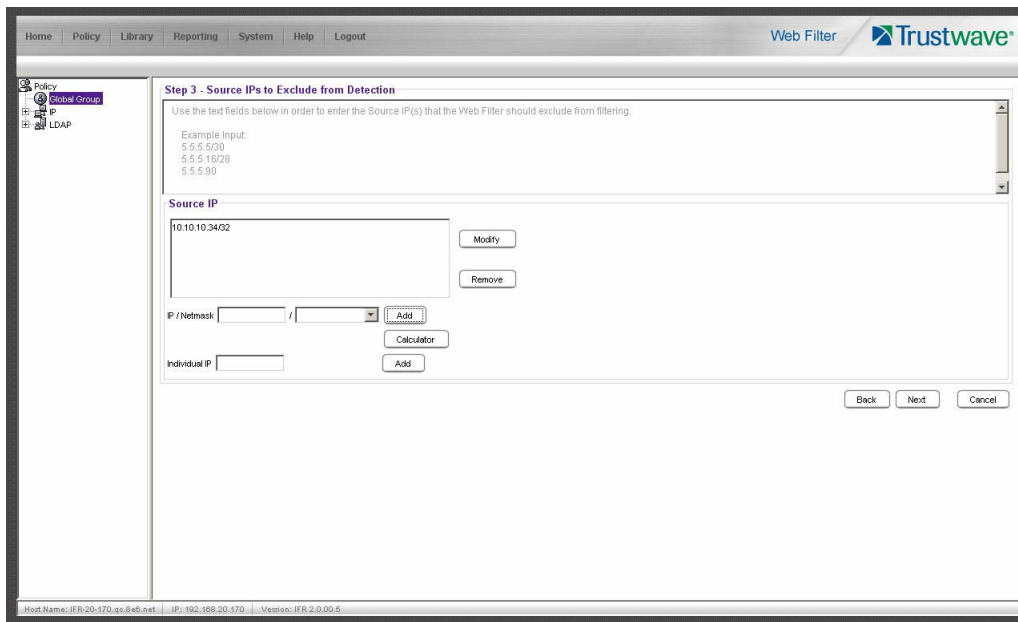
1. In the first step of the wizard, enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address of the source IP address(es) to be filtered.



2. Click **Next** to go to Step 2 of the Wizard:

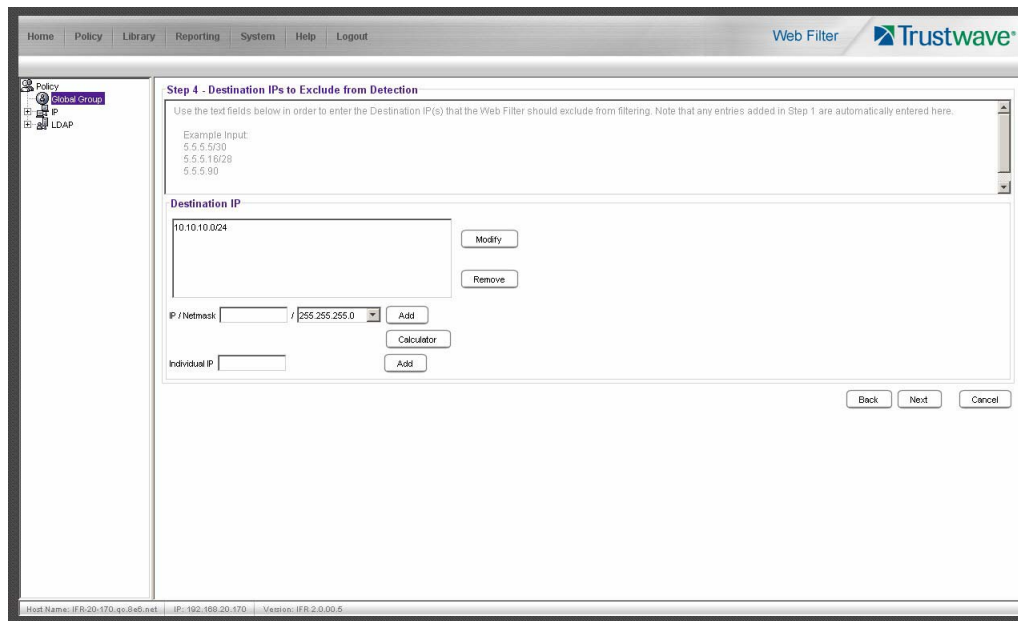


3. An entry for this step of the Wizard is optional. If there are destination IP address(es) to be filtered, enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address.
4. Click **Next** to go to Step 3 of the Wizard:

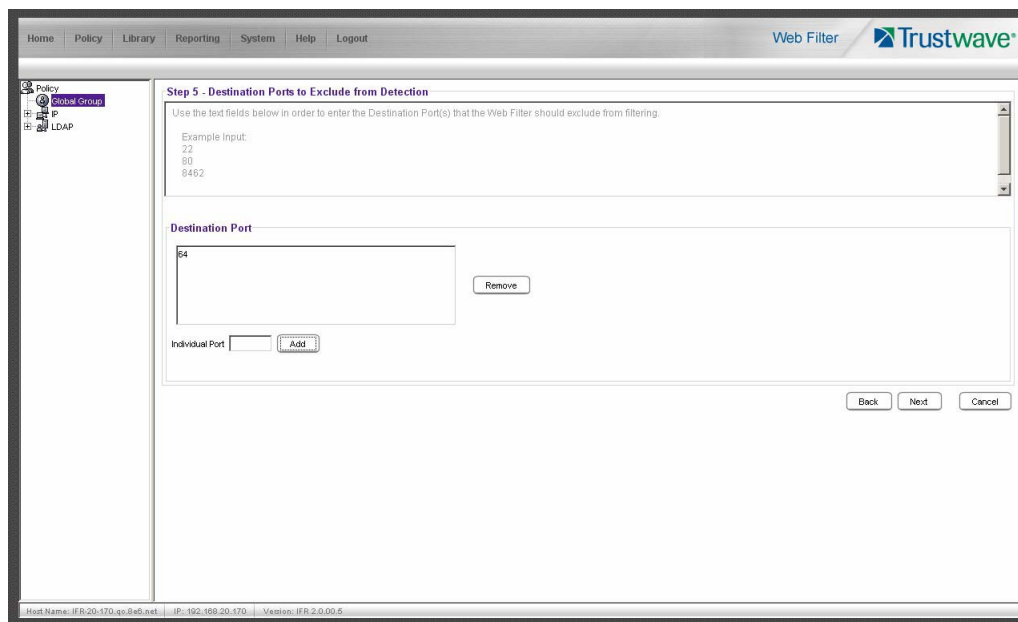


5. An entry for this step of the Wizard is optional. If there are source IP address(es) to be ignored, enter the **IP** address and specify the **Netmask**, or enter the **Individual IP** address.

- Click **Next** to go to Step 4 of the Wizard:



- 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.
- Click **Next** to go to Step 5 of the Wizard:



- 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:

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.

Skip to Section 5.2.2.4 to complete this process.

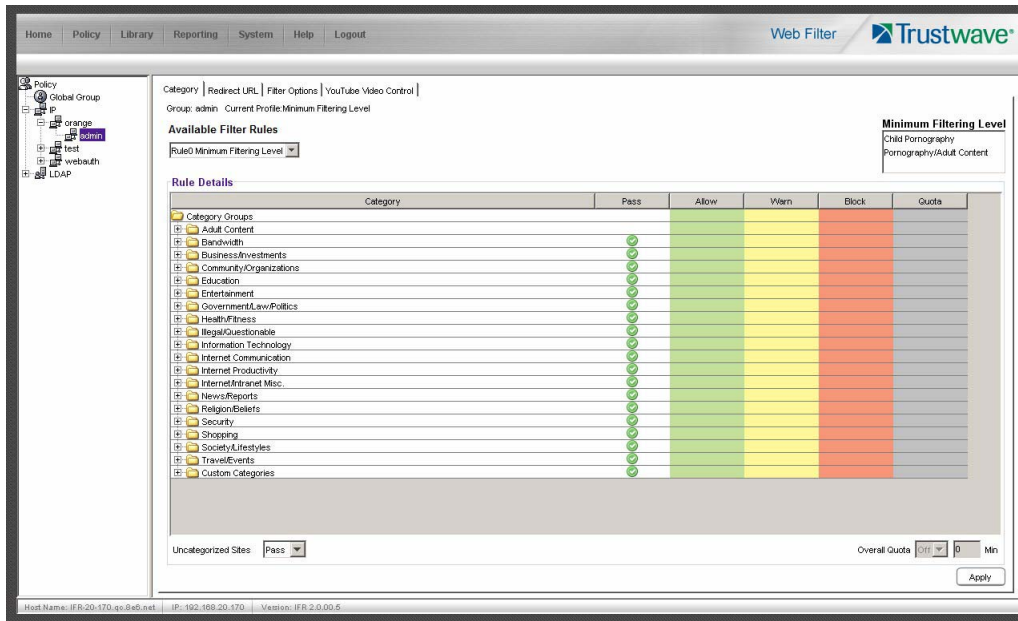
5.2.2.3 Block Web access via IP Sub-Group profile



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

1. Select the IP Sub-Group from the tree.

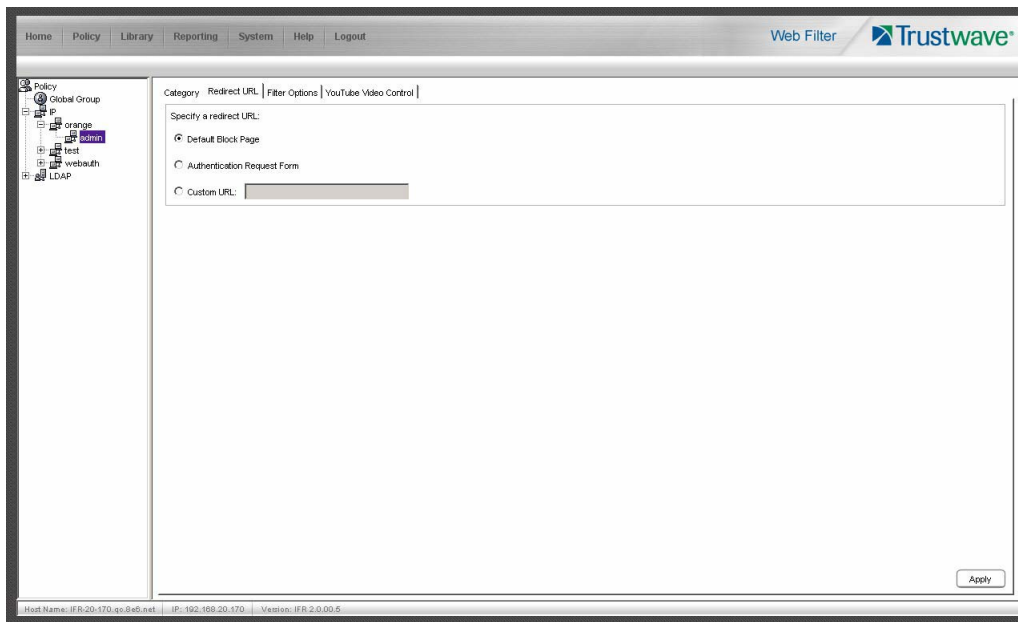
2. Click Sub Group Profile in the menu to display the Sub Group Profile window:



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.

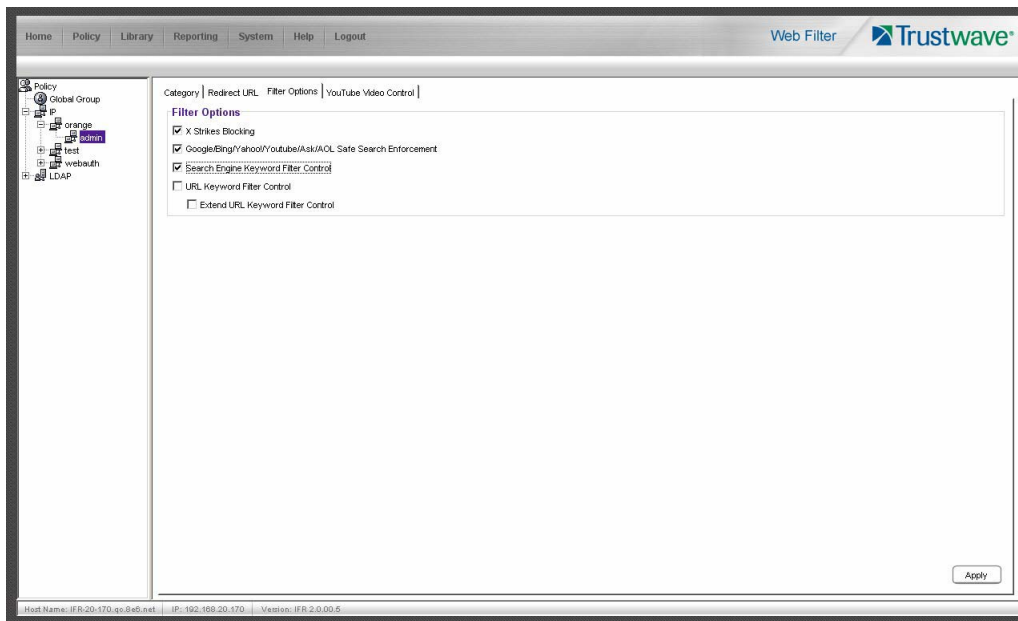
4. Click **Apply**.

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



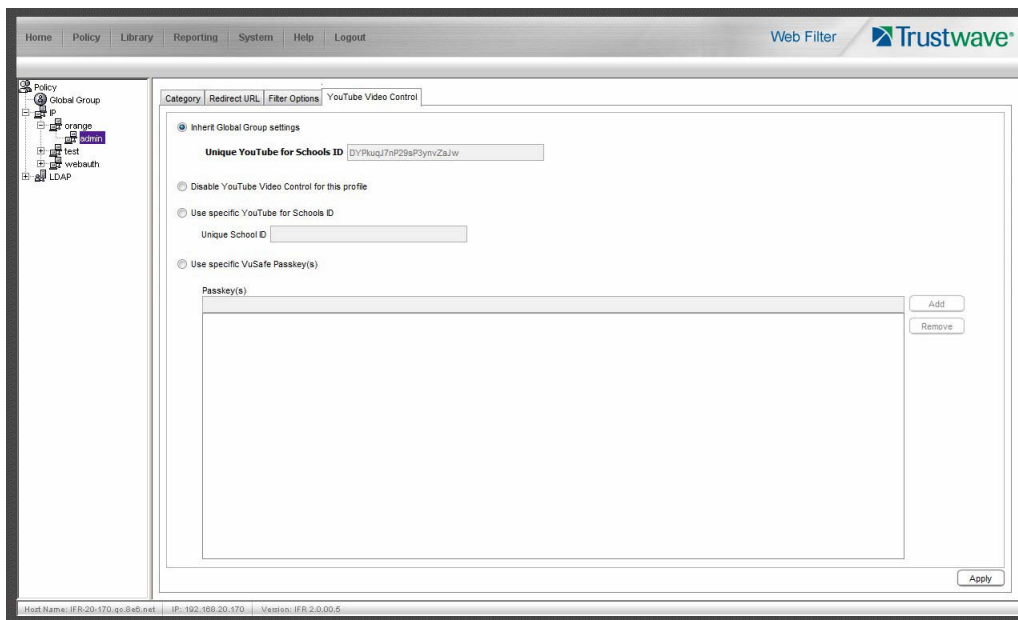
6. Select "Default Block Page", and then click **Apply**.

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



8. Select filter options to be enabled.

9. Click the YouTube Video Control tab to display the YouTube Video Control page:

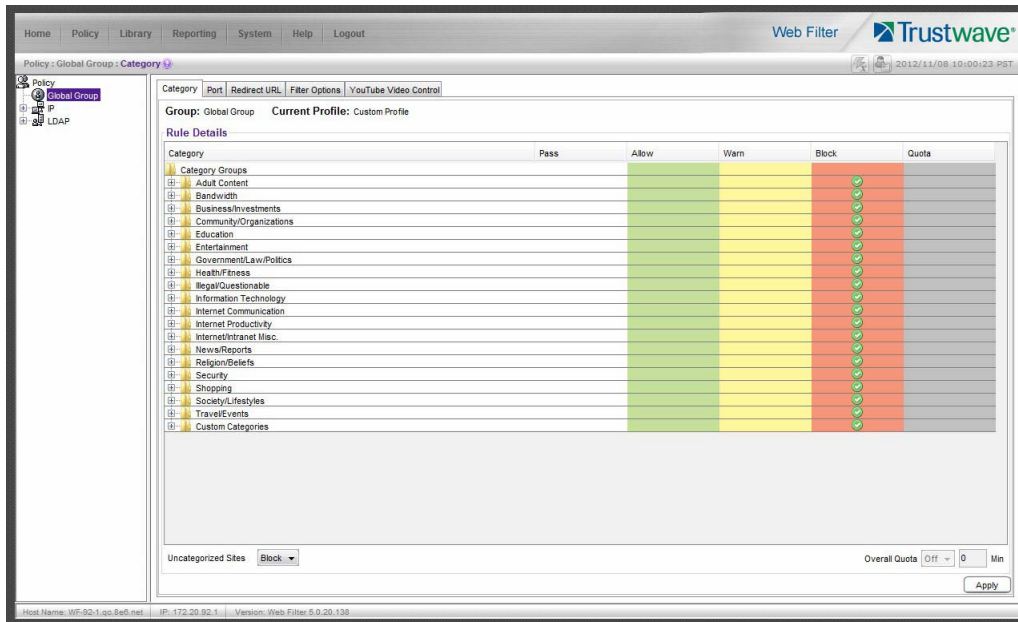


10. Select the YouTube Video Control option to use and click **Apply**.

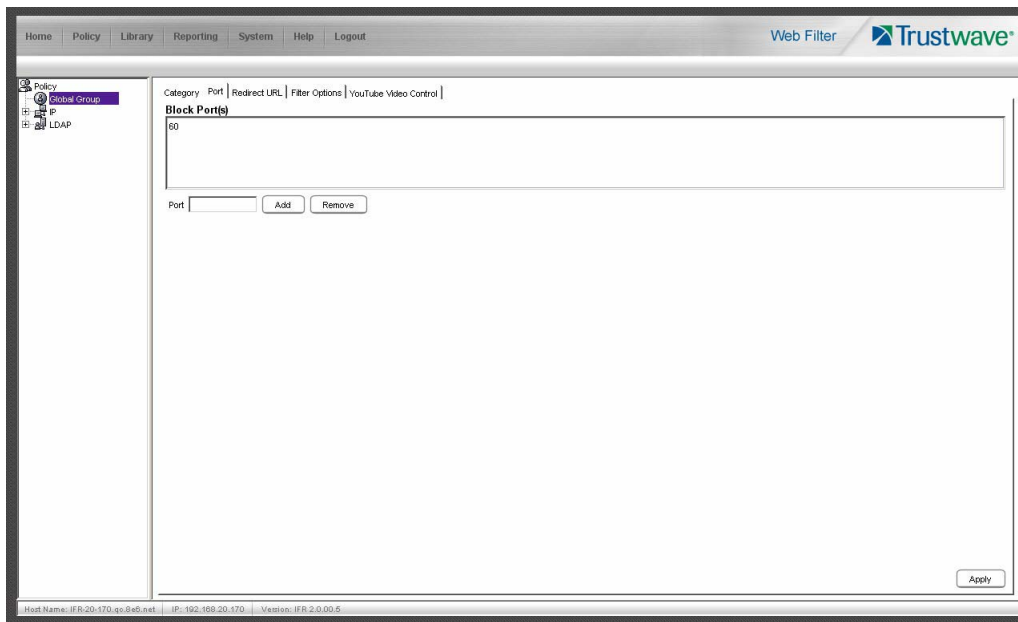
As a result of these entries, the machine will not be served the Authentication Request Form, and will use the default block page instead.

5.2.2.4 Modify the Global Group Profile

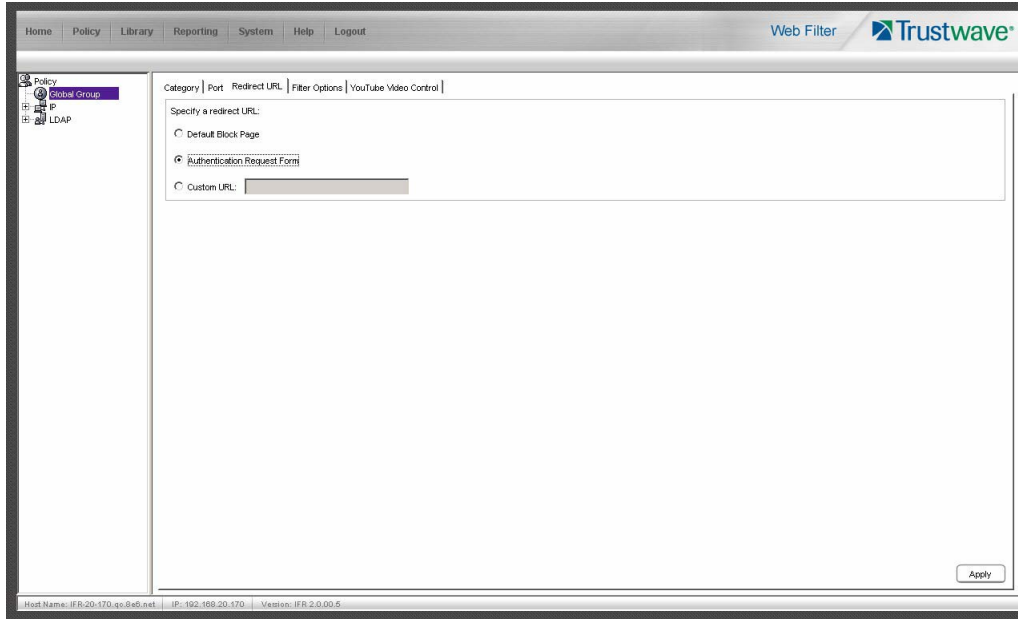
1. Click Global Group in the tree to open the menu.
2. Select Global Group Profile to display the Category tab of the Profile window:



- 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:



- 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 Redirect URL tab to display the Redirect URL page:



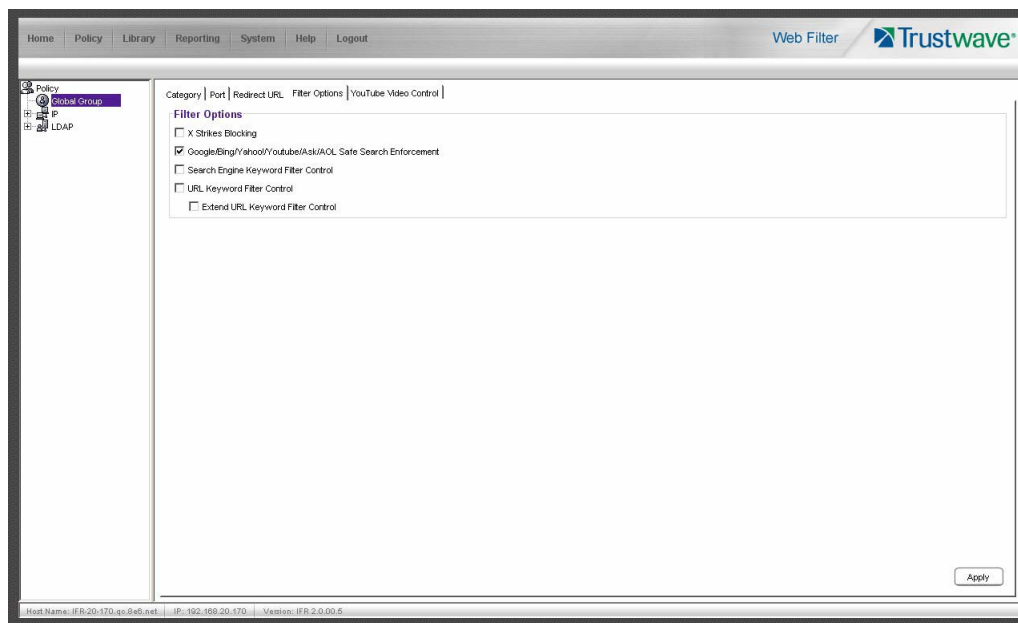
- a. Select "Authentication Request Form".



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.

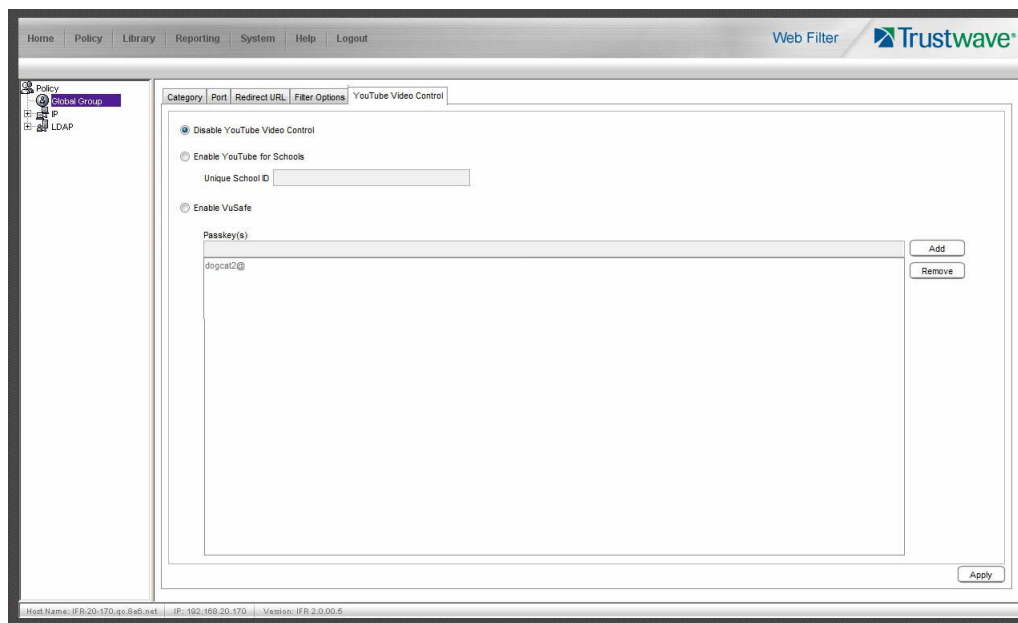
- b. Click **Apply**.

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



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

6. Click the YouTube Video Control tab to display the YouTube Video Control page:



- a. Specify the YouTube Video Control option to use.
- 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.

5.2.3 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.

5.2.3.1 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 Web Filter. Users will be blocked according to the profiles set up on the domain.

5.2.3.2 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 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**.

Glossary

ADS

Active Directory Services is a Windows 2000/2003/ 2008 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 Web Filter.

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.

bridge mode

A Web Filter set up in the bridge mode will filter all requests as with Invisible mode. Bridge mode also filters HTTPS content for Google and YouTube, using a built-in proxy to decrypt the HTTPS traffic for these sites only.

common name (cn)

An attribute type entered for a username and group when using LDAP.

container

An LDAP server object that can be comprised of containers, organizational units, or domains. Container objects can also "contain" other objects, such as user objects, group objects, and computer objects.

directory

This information source on a server contains attribute-based data relevant to a DN entry.

directory service

Uses a directory on a server to automate administrative tasks for storing and managing objects on a network (such as users, passwords, and network resources users can access). ADS, DNS, and NDS (Novell Directory Services) are types of directory services.

Distinguished Name (DN)

A string of "cn" and "dc" attribute types comprised of the username and group name, domain name, and DNS suffix. For example: "cn=admin_user, cn=admin, dc=yahoo, dc=com". The "ou" attribute type also could be a part of the DN. For example: "cn=Joe Smith, ou=users, ou=sales, dc=acme, dc=com".

DNS

Domain Name Service is a distributed Internet directory service. DNS is used mostly for making translations between domain names and IP addresses.

domain

An entity on a network comprised of servers, workstations, and peripherals.

domain component (dc)

An attribute type entered for a domain name and DNS suffix when using LDAP.

domain controller

An authentication server that answers logon requests from workstations in a Windows 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

A Web Filter 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 Web Filter, except for managing master IP groups, LDAP domains, and each member's associated filtering profile. The global administrator configures the Web Filter, 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

A Web Filter 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 Web Filter. 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 Web Filter 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 conjunction 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

A Web Filter 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 Web Filter 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 "trustwave.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.

Appendices

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.

A.1 Authentication Tier Selections

Web Filter authentication is designed to support the following server types for the specified tier(s):

A.1.1 Tier 1: Net use based authentication



Note: Login scripts must be used for net use based authentication.

Using NetBIOS:

- Windows 2003 / 2008 Server in mixed/legacy mode

Using LDAP:

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

A.1.2 Tier 2, Tier 3: Web-based authentication

1. Using an LDAP domain:

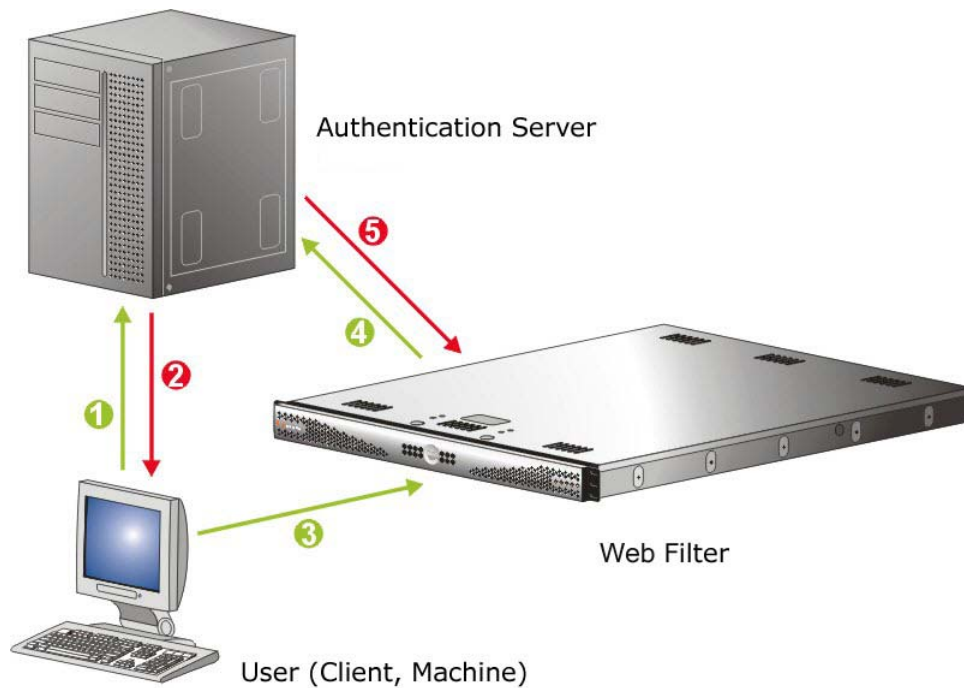
- Windows Active Directory 2002 and 2003
- Novell eDirectory
- Sun One directory server
- Open Directory server

A.2 Tier 1: Single Sign-On Authentication

A.2.1 Net use based authentication process

The following diagram and steps describe the operations of the net use based user authentication process.

Figure 25: 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 Web Filter 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 Web Filter 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 Web Filter matches the user's login name or group name with a stored list of profile settings in the Web Filter. 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 Web Filter senses this change and returns the IP address to the configured global filtering level.



Caution: Authentication will fail if a Network Address Translation (NAT) device is set up between the authentication server and end user clients.

A.2.1.1 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.

A.2.2 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 set-ups.

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.

A.2.3 Name resolution methods

The name resolution process occurs when the Web Filter 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 Web Filter hosts file.

A.2.4 Configuring the authentication server

When configuring authentication, you must first go to the authentication server and make all necessary entries before configuring the Web Filter.

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

A.2.4.1 Login scripts

Login (or logon) scripts are used by the Web Filter for reauthenticating users on the network.

The following syntax must be entered in the appropriate directory on the authentication server console:

A.2.4.2 Enter net use syntax in the login script

The virtual IP address is used by the Web Filter 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 Web Filter.

- For testing, user information can be specified on the command line as follows:
NET USE \\virtualip\R3000\$ /user:DOMAINNAME\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 2003 / 2008 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 Web Filter 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.

A.2.5 LDAP server setup rules



Caution: The instructions in this 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 Web Filter 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 Web Filter 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.com-pany.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.

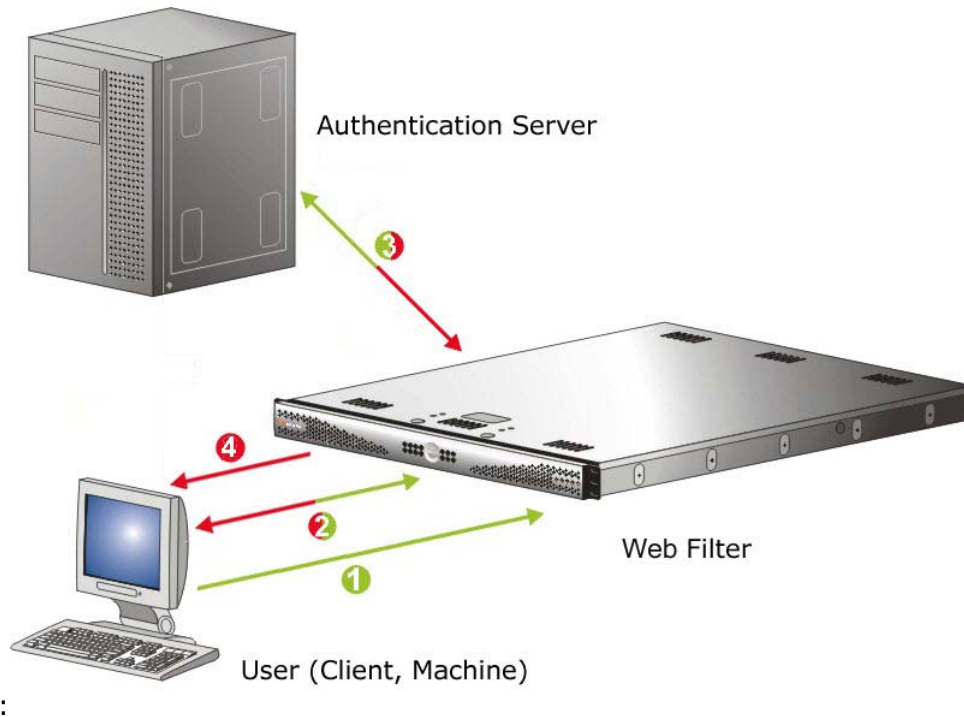


Note: All filtering profiles are stored on the Web Filter.

A.3 Tier 2: Time-based, Web Authentication

The following diagram and steps describe the operations of the time-based authentication process.

Figure 26: Web-based authentication module diagram



1. The user makes a Web request by entering a URL in his/her browser window.
2. The Web Filter 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 Web Filter 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.

A.3.1 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 Web Filter to maintain a connection with the client machine, so the Web Filter 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 Web Filter via NET USE in order for the profile to be removed in either environment.

A.3.1.1 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, Trustwave'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

```

A.3.1.2 Tier 1 and Tier 2 Script

In an environment in which both Tier 1 and Tier 2 are used, this version of Trustwave's script should be inserted into the network's login script. Trustwave'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.

A.4 Tier 3: Session-based, Web Authentication

Figure 26 and the 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 Web Filter 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 Web Filter verifies the user's information with the authentication server (Domain Controller, Active Directory, LDAP, etc.).
4. A Java applet 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 window remains open.



Note: If the Java applet fails to launch, as on Android and iOS-based devices, enabling the time-based fallback option lets the user access the Internet for the duration of time specified.

A.5 Authenticator

The Authenticator ensures the end user is identified on his/her workstation, via an executable file that launches during the login process. To use this option in a Windows environment, the Authenticator client can be installed on the user's workstation or launched from a network share during login. In a Macintosh environment, the application should be installed on the client machine, where it will be automatically launched when the user logs in.

Tips:



- When installing this application on multiple Macintosh workstations simultaneously, the Apple Remote Desktop product can be used to deploy the Authenticator in bulk.
- See <http://www.trustwave.com/software/8e6/hlp/auth/auth.html> for online help.

A.5.1 Workstation requirements



Note: If using the Authenticator in a Citrix Virtual Desktop Infrastructure (VDI) environment, see <http://www.trustwave.com/software/8e6/hlp/auth/auth-citrix.html> for setup information.

A.5.1.1 Windows environment

The Authenticator client works with the following Windows operating systems:

- Windows XP Pro SP1 and 2
- Windows XP with Novell client v4.91
- Windows Vista (all editions except Home and Starter)
- Windows 7 (all editions except Home and Starter)



Notes:

- Windows XP and Vista and 7 Home/Starter Editions can be used if the Novell eDirectory client and Authenticator are installed in a Novell network environment.
- Terminal Services must be enabled on Windows for Fast User Switching support.
- Remote Desktop Connections are not supported.

A.5.1.2 Macintosh environment

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

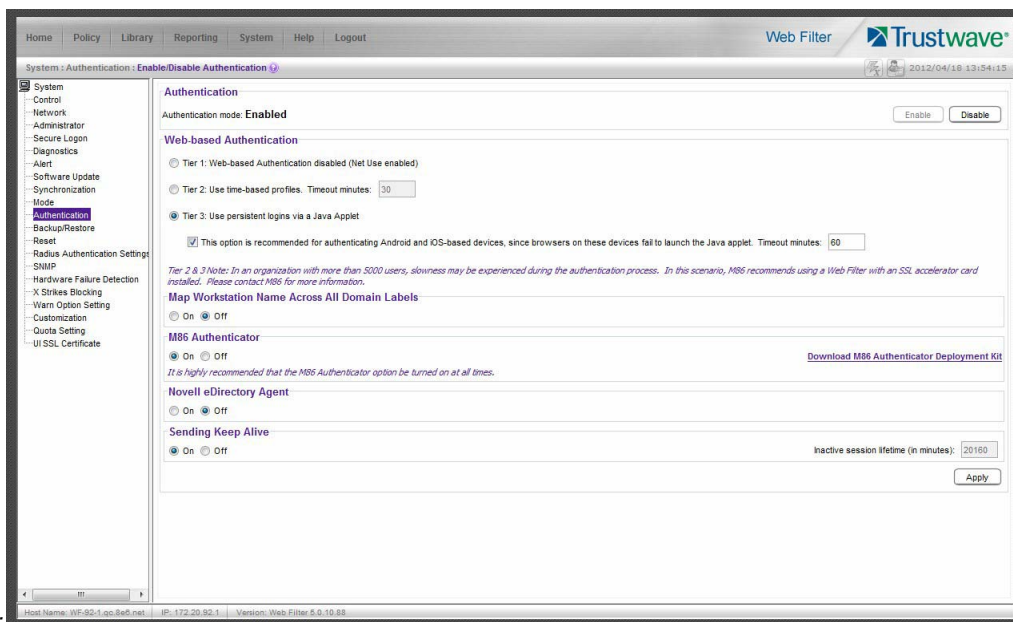
- Macintosh OS X 10.5 or 10.6
- Intel processor

A.5.2 Enable, download Authenticator

Downloading, installing and configuring the Authenticator Deployment Kit on a Windows machine results in the creation of a platform-specific package that can be installed on a network share accessible by an Active Directory domain controller, a Novell eDirectory server, or on a Windows or Macintosh workstation joined to a domain via Active Directory or OpenDirectory.

When installed on a workstation, the Authenticator automatically authenticates the end user when the user logs into the workstation. If installing the deployment kit in a Macintosh environment, an Open Directory server should be used. The end user will be automatically authenticated when logging into the workstation.

1. To enable the Authenticator, in the Web Filter user interface, navigate to **System | Authentication | Enable/Disable Authentication**.



2. In the Authenticator frame, click "On".
3. To download the Authenticator, click **Download Authenticator Deployment Kit** to launch the Authenticator Web page where you select the Authenticator file you wish to download.

A.5.3 Authenticator Deployment Kit

The Authenticator Deployment Kit, used for configuring the Authenticator for deployment via the Package Editor, is comprised of the following resources:

- Unconfigured packages containing the Authenticator software
- A tool for setting or modifying Authenticator packages (the "package editor," CfgTool.exe)
- A script for uninstalling the Authenticator from a Macintosh workstation (Uninstall-Authenticator.sh)
- Link to an online help file providing an overview of this product

A.5.4 Work flow in environments

The administrator downloads and then installs the Authenticator Deployment Kit on his/her machine. Then he/she uses the Package Editor application to configure packages for a Windows or Macintosh environment.

A.5.4.1 Windows environment

1. Once the Authenticator client package for Windows is configured, the administrator installs that package on target workstations, or deploys it via a network logon script.
2. Using a Windows machine, an end user logs on the Active Directory domain, or logs on the eDirectory tree via a Novell client.
3. The Authenticator is launched in one of the following methods, based on the installation mode setup:
 - a. Netlogon Mode - If the Authenticator is deployed via a network logon script, the script invokes Authenticat.exe from a network share.
 - b. User Mode - If installed in User Mode, Authenticator is launched from the user's local \Program Files tree via a startup registry key.
 - c. Service Mode - If installed in Service Mode, Authenticator starts with Windows, and detects the user login dynamically.



Note: The Service Mode is not supported in Novell Client for Windows.

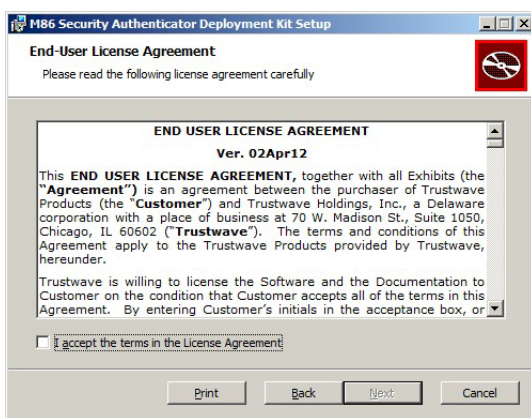
4. Authenticator determines the authentication environment, then retrieves the username and related identifying information using either Windows or Novell APIs, and sends this information (via LOGON event) to the Web Filter.
5. The Web Filter looks up the group memberships for the user (via Windows AD, PDC, or eDirectory through LDAP), and determines the profile assignment.
6. The Web Filter sets the profile for the end user with username (including the group name, if it is available) and IP.
7. The Authenticator client periodically sends a "heartbeat" packet to the Web Filter to sustain the connection and profile as long as the user is logged in and connected to the network.
8. The end user logs off, and the Authenticator client sends a LOGOFF event to the Web Filter. The Web Filter removes the user's profile.

A.5.4.2 Macintosh environment

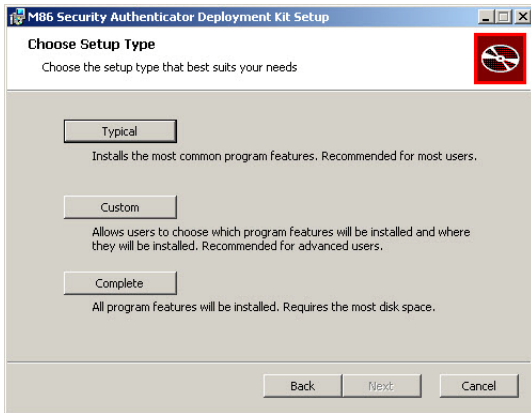
1. Once the Macintosh package is configured, the administrator installs the package on target workstations.
2. An end user logs on the domain, and OS X launches Authenticator.
3. Authenticator identifies the end user by using OS X Directory Services, retrieving the username and related identity information, which it sends to the Web Filter (via a LOGON event).
4. The Web Filter looks up the user's group memberships and determines the profile assignment.
5. The Web Filter sets the profile for the end user with username (including the group name, if it is available) and IP.
6. Authenticator client continually sends a "heartbeat" to the Web Filter until the end user logs off or disconnects.
7. If the user logs off, Authenticator sends a LOGOFF event to the Web Filter. The Web Filter removes the user's profile.

A.5.5 Download and install the Deployment Kit

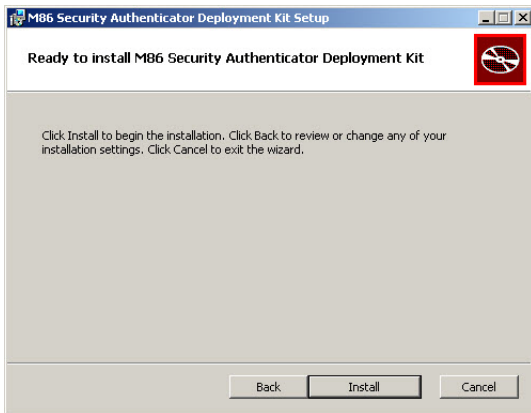
1. In the Web Filter user interface, go to **System | Authentication | Enable/Disable Authentication** window.
2. In the Authenticator frame, click **Download Authenticator Deployment Kit** to launch the Trustwave Web page where you can select the Authenticator Deployment Kit file to download to your machine.
3. Once the deployment kit .msi file is downloaded to your machine, click that file to launch the Authenticator Deployment Kit Setup Wizard, with the End User License Agreement displayed:



4. After reading the EULA, click the check box corresponding to "I accept the terms in the License Agreement", and then click **Next** to go to the Choose Setup Type step:



5. Select the setup option for installing the Authenticator ("Typical", "Custom", "Complete"), and then click **Next** to proceed with the option you selected for installing the application. If you chose the Custom option, you will need to specify where or how the main executable and support files will be installed on your machine, and/or where or how Windows and Macintosh packages for the Authenticator will be installed for distribution to user workstations.
6. When your machine is ready to install the Deployment Kit, the page that confirms the installation process is ready to begin displays:



7. Click **Install** to begin the installation process. The following page displays when the installation process is complete:



8. Click **Finish** to close the wizard dialog box.

A.5.6 Access the Deployment Tool window

Once the Authenticator Deployment Kit is installed on your machine, the Authenticator Deployment Tool window and Authenticator Package Configuration window are used for configuring packages for Windows or Macintosh.

The Authenticator Deployment Tool window is accessible via **Start | All Programs | M86 Authenticator Deployment Kit | Package Editor**.

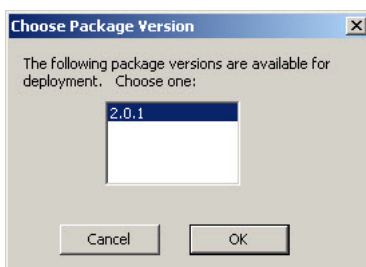
The Authenticator Deployment Tool's package editor log window displays the operations performed when creating and configuring packages.



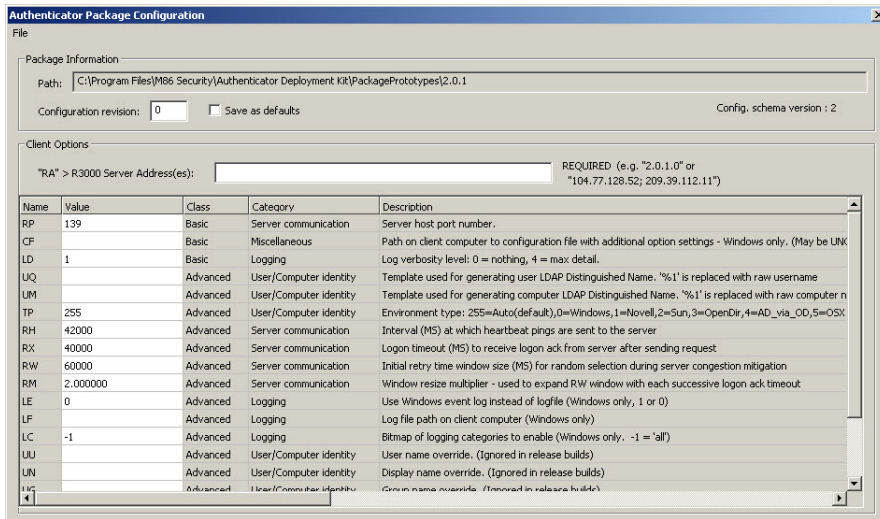
Note: Before exiting the Authenticator Deployment Tool and Package Configuration windows, be sure to save all entries you intend to save for packages you've configured. To exit the Authenticator Deployment Tool window, with the Package Configuration window closed, go to **File | Exit**.

A.5.7 Configure a New Package set

1. In the Authenticator Deployment Tool window, go to **File | New Package...** to open the Choose Product Version dialog box:



2. Select the Authenticator software version from the available choices, and then click **OK** to close the Choose Product Version dialog box and to open the Package Configuration window:



3. The Package Configuration window is comprised of the Package Information and Client Options frames.



Note: To exit the Package Configuration window at any time before saving your edits, select **File | Cancel** from the menu.

A.5.7.1 Specify Package criteria

The Package Information frame includes the following information: Path on the system where the current package is located, Configuration revision number, Configuration schema version number, and package version numbers.

The following fields are editable:

- **Configuration revision:** This number is automatically incremented by "1" each time changes made to the package configuration are saved. When deploying the Authenticator to end user workstations, the installer uses this revision number to determine whether a newer configuration is already installed on the workstation.



Tip: To ensure updates to end user workstations are properly applied, if you are making configuration-only changes, it is better to edit the previous package rather than create a new one.

- **Save as defaults:** By checking this box, your configuration will be saved in a central defaults file for use in the next "Save" command.



Tip: By enabling this feature, if creating a new package you can apply these saved default settings to the new package by choosing **File | Apply Defaults** from the menu.

A.5.7.2 Specify Client Options

The Client Options frame includes fields used for specifying configuration settings.

1. In the field "**RA** | **R3000 Server Address(es)**" enter the virtual IP address(es) of the Web Filter server(s), separating more than one IP address by a semi-colon (;). Typically this entry is just a single IP address for each server, but the full syntax is:

```
{server_spec};{server_spec};...
```

```
server_spec= {hostname or IP addr} [: port]
```

2. Review the Basic class parameter fields and make any necessary modifications in the corresponding **Value** fields:

Name	Value	Category	Description
RP	139	Server communication	Server host port number: This value is used for any server_spec which does not contain an explicit port number. If this value is changed from the default value, the new port number must be entered via a command line change in the Web Filter. (Contact Technical Support for assistance in making this change in the Web Filter.)
CF		Miscellaneous	Path on client computer to configuration file with additional option settings; Windows only. (May be UNC)
LD	1	Logging	Log verbosity level: 0 = nothing, 4 = max detail.

3. For advanced users, if necessary, make modifications in the corresponding **Value** field for any of these Advanced class parameters:

Name	Value	Category	Description
UQ		User/Computer identity	Template used for generating user LDAP Distinguished Name. '%1' is replaced with raw username.
UM		User/Computer identity	Template used for generating computer LDAP Distinguished Name. '%1' is replaced with raw computer name.
UT	255	User/Computer identity	Environment type: 255=Auto(default), 0=Windows, 1=Novell, 2=Sun, 3=OpenDir, 4=AD_via_OD, 5=OSX
RH	42000	Server communication	Interval (MS) at which heartbeat pings are sent to the server.
RX	40000	Server communication	Logon timeout (MS) to receive logon ack from server after sending request.
RW	60000	Server communication	Initial retry time window size (MS) for random selection during server congestion mitigation.
RM	2.0	Server communication	Window resize multiplier: Used for expanding RW window with each successive logon ack timeout.
LE	0	Logging	Use Windows event log instead of logfile. (Windows only, 1 or 0)
LF		Logging	Log file path on client computer. (Windows only; operates from the command line)
LC	-1	Logging	Bitmap of logging categories to enable. (Windows only. -1 = 'all')

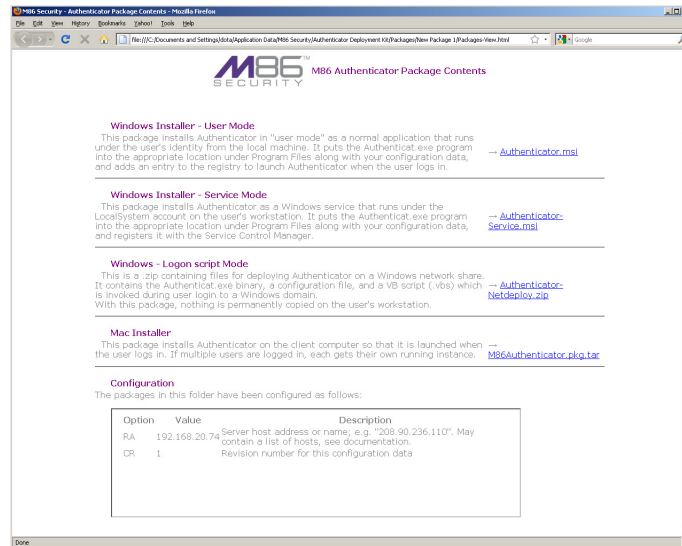
A.5.7.3 Save configuration settings, download files

In the Package Configuration window, the following options are available from the File menu for saving the package configuration:

- **Save** - Saves the current package
 - **Save as...** - Launches the Save Package window in which you specify the **Package Name**, click **OK** and then **Yes** in a dialog box to close both the box and window
 - **Save and Quit** - Saves your edits and closes the Package Configuration window

When the package is saved the Configuration revision number in the Package Configuration window is automatically incremented to the next sequential number, and the Authenticator Package Contents local Web page launches, providing a summary of package contents with links to various components generated in the package.

Figure 27: Authenticator Package Contents page



The Authenticator Package Contents page includes the following information, with links to files generated for the package:

- **Windows Installer - User Mode ([Authenticator.msi](#)):** This package installs Authenticator in "user mode" as a normal application that runs under the user's identity from the local machine. It puts the Authenticat.exe program into the appropriate location under Program Files along with your configuration data, and adds an entry to the registry to launch Authenticator when the user logs in.
- **Windows Installer - Service Mode ([Authenticator-Service.msi](#)):** This package installs Authenticator as a Windows service that runs under the LocalSystem account on the user's workstation. It puts the Authenticat_s.exe program into the appropriate location under Program Files along with your configuration data, and registers it with the Service Control Manager.
- **Windows - Logon script Mode ([Authenticator-Netdeploy.zip](#)):** The .zip file contains files for deploying Authenticator on a Windows network share. It contains the Authenticat.exe binary, a configuration file, and a VB script (.vbs) which is invoked during user login to a Windows domain. With this package, nothing is permanently copied on the user's workstation.
- **Mac Installer ([M86Authenticator.pkg.tar](#)):** This package installs Authenticator on the client computer so that it is launched when the user logs in. If multiple users are logged in, each user gets his/her own running instance.
- **Configuration** - Package configuration Options and their corresponding Values and Descriptions.

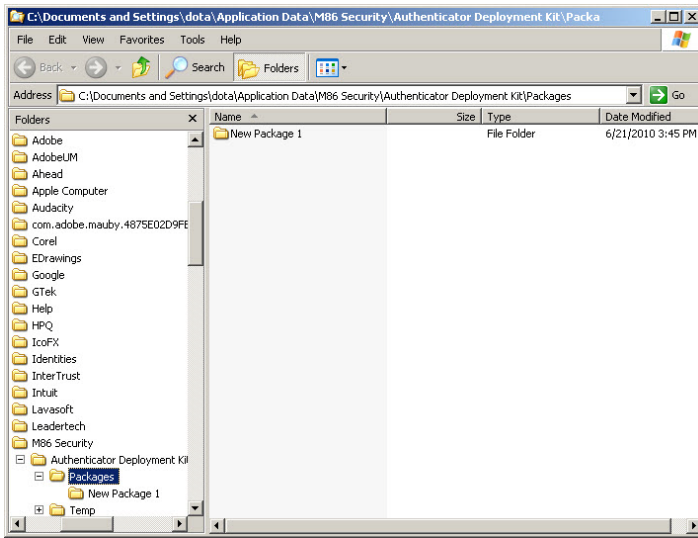


Note: More information about these tools is provided in subsequent pages in this section of the Guide.

A.5.8 View Package Configuration contents

In addition to viewing a summary of package contents using the Authenticator Package Contents page, actual package contents are accessible via the Authenticator Deployment Tool window.

1. From the Authenticator Deployment Tool window, select **File | Explore packages...** to launch the Authenticator Deployment Kit's Packages folder containing all packages created for the Authenticator:

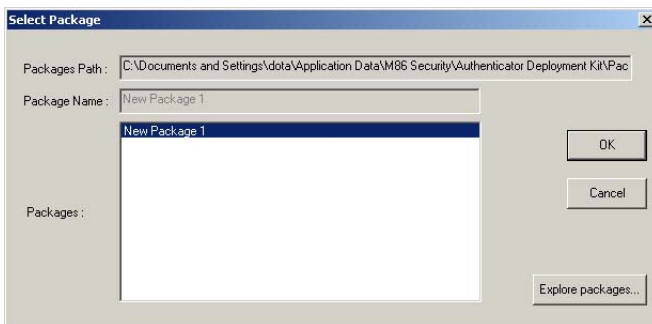


Tip: The Packages folder is also accessible from the Select Package window by clicking the **Explore packages...** button.

2. Double-click the selected package to display its contents.
3. When you are finished, click the "X" in the upper right corner of the folder to close it.

A.5.9 Edit a Package Configuration

1. From the Authenticator Deployment Tool window, select **File | Edit Package...** to open the Select Package window:



2. From the Packages list box, choose the package to be edited; this action populates the Packages Path and Package Name fields with pertinent criteria about the package.



Tip: Click **Explore packages...** to open the Authenticator Deployment Kit's Packages folder and choose the package to be edited from the available selections.

3. Click **OK** to close the Select Package window and to launch the Authenticator Package Configuration window displaying the last saved edits made for the package.



Note: The "Configuration revision" is incremented to the next sequential revision number.

4. After making your edits, choose a Save option for saving the configuration package.

A.6 Novell eDirectory Agent

Novell eDirectory Agent provides Single Sign-On (SSO) authentication for an Web Filter set up in a Novell eDirectory environment. Using Novell eDirectory Agent, the Web Filter 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.

A.6.1 Environment requirements

A.6.1.1 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

A.6.1.2 Client workstations

To use this option, all end users must log in the network. The following OS have been tested:

- Windows 2003 / 2008 Professional/
- Windows XP / Vista / 7
- Macintosh

A.6.1.3 Novell clients

The following Novell clients have been tested:

- Windows: Version 4.91 SP2
- Macintosh: Prosoft NetWare client Version 2.0

A.6.1.4 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

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

A.6.1.5 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

A.6.2 Novell eDirectory setup

The eDirectory Agent uses the LDAP eDirectory domain configuration setup in the Web Filter 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.

A.6.3 Web Filter setup and event logs

When using a Novell eDirectory server and choosing to use the Novell eDirectory Agent option in the Web Filter:

- 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.
 - 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.
- When choosing the Novell eDirectory Agent option, the Authenticator option must be disabled.



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.

Appendix B: Obtain, Export an SSL Certificate

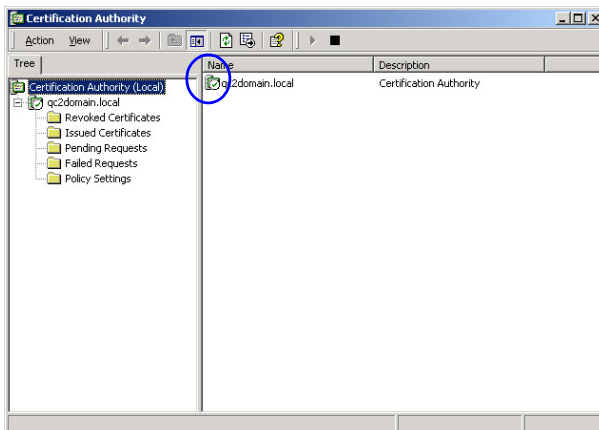
When using Web-based authentication, the LDAP server's SSL certificate needs to be exported and saved to the hard drive, then uploaded to the Web Filter so that the Web Filter will recognize LDAP server as a trusted source.

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.

B.1 Export an Active Directory SSL Certificate

B.1.1 Verify certificate authority has been installed

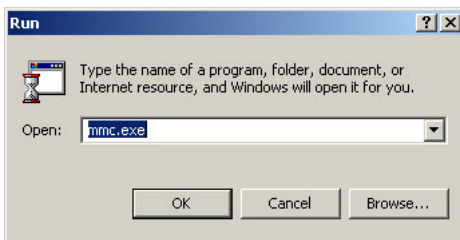
1. From the console of the LDAP server, go to **Start | Programs | Administrative Tools | Certification Authority** to open the Certification Authority window:



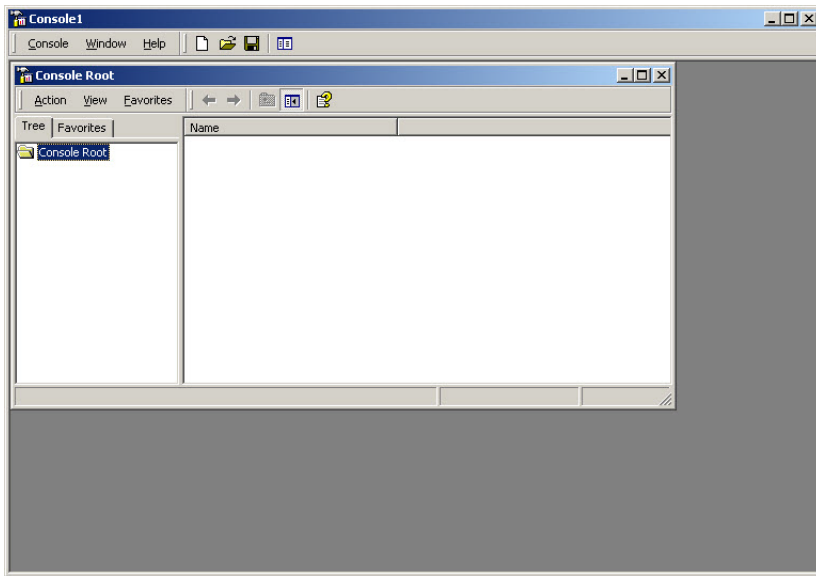
2. Verify that the certificate authority has been installed on this server and is up and running—indicated by a green check mark on the server icon.

B.1.2 Locate Certificates folder

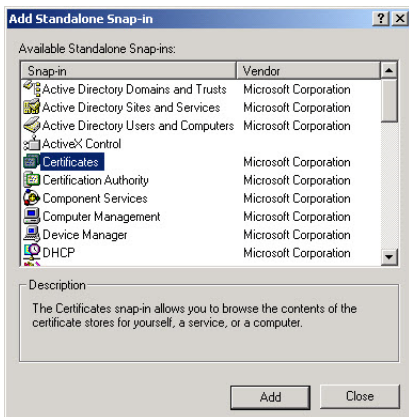
1. Go to **Start | Run** to open the Run dialog box. In the **Open** field, type in **mmc.exe** to specify that you wish to access the Microsoft Management Console:



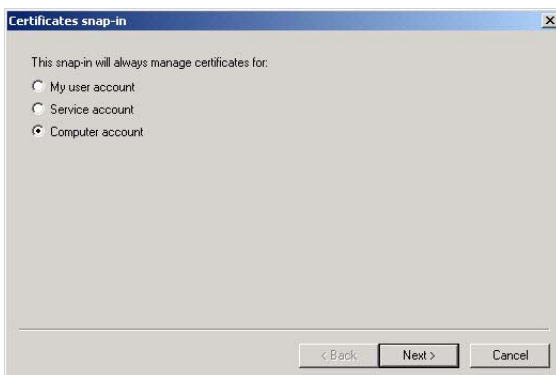
2. Click **OK** to open the Console window:



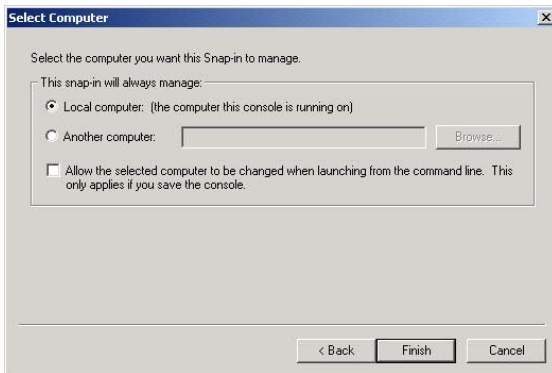
3. From the toolbar, click Console to open the menu. Select Add/Remove Snap-in to open the Add/Remove Snap-in dialog box.
4. Click **Add** to open the Add Standalone Snap-in dialog box:



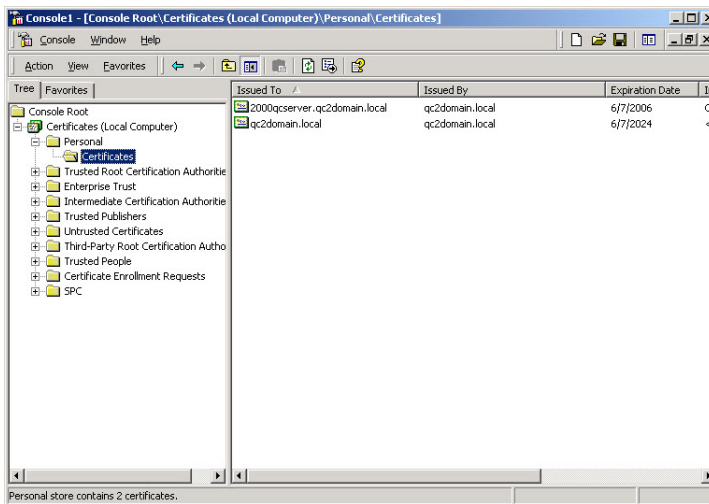
5. Select Certificates, and click **Add** to open the Certificates snap-in wizard dialog box:



- Choose "Computer account", and click **Next** to go to the Select Computer wizard page:



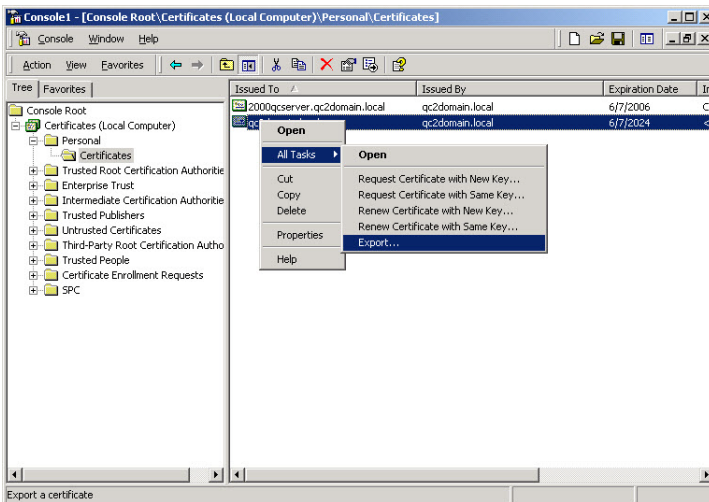
- Choose "Local computer: (the computer this console is running on)", and click **Finish** to close the wizard dialog box.
- Click **Close** to close the Add Standalone Snap-in dialog box. Click **OK** to close the Add/Remove Snap-in dialog box.
- Notice that the snap-in has now been added to the Console Root folder:



B.1.3 Export the master certificate for the domain

- 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 menu, and select **All Tasks | Export**:



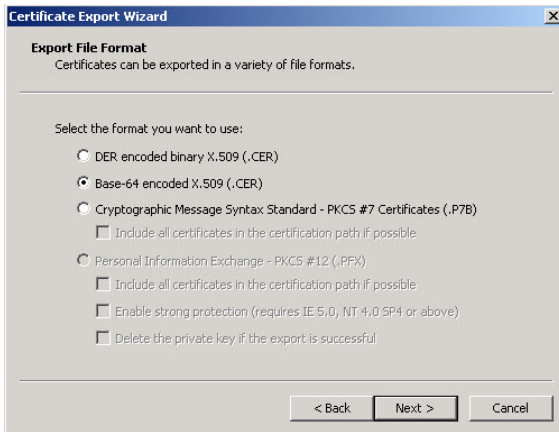
This action launches the Certificate Export Wizard:



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



4. Select "No, do not export the private key", and click **Next** to go to the Export File Format page of the wizard:



5. Select "Base-64 encoded X.509 (.CER)" and click **Next** to go to the File to Export page of the wizard:



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:



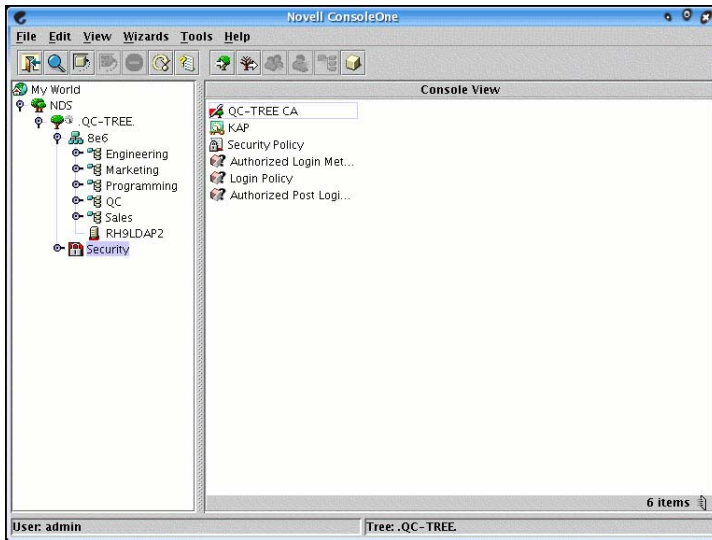
7. Notice that the specified settings display in the list box, indicating the certificate has been successfully copied from the console to your disk. Click **Finish** to close the wizard dialog box.

8. Close the Console.

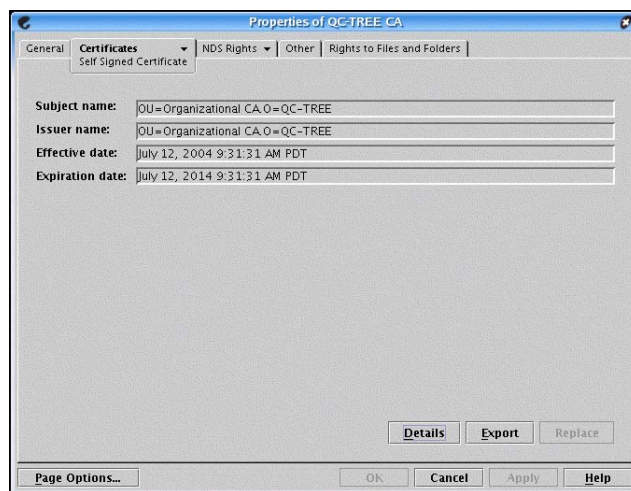
The certificate can now be uploaded to the Web Filter.

B.2 Export a Novell SSL Certificate

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):



2. Find the tree's folder and right-click it to open the menu. Select Properties to open the 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 window:



5. Select "File in binary DER format" for the Output format. The path of the certificate displays in the File-name field.
6. Click **Export** to open another 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 Web Filter.

B.3 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 Web Filter. 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 Web Filter 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.

C.1 OpenLDAP Server Scenario

C.1.1 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 Web Filter.

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.

D.1 Username Formats



Note: For examples of valid username entries, see File Format: Rules and Examples in this appendix, or go to

http://www.trustwave.com/software/8e6/hlp/r3000/files/2group_textfile_user.html

D.2 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.trustwave.com/software/8e6/hlp/r3000/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

<https://www.trustwave.com/web-security/web-filtering/database-categories>

- **Filter Option codes:**

- 0x1 = Exception URL Query (always enabled)
- 0x2 = X Strikes Blocking
- 0x4 = Google/Bing/Yahoo!/Youtube/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:

- a. Type in the username.
- b. Press the Tab key on your keyboard to leave a space.
- c. 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.trustwave.com/software/8e6/hlp/r3000/files/2group_textfile_format_ldap.html for examples of LDAP filtering profile entries. Quota profile entries are included in these pages.

D.3 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.

D.3.1 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.

D.3.1.1 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=WIN2003-79AHM, 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 "WIN2003-79AHM", 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.

D.3.1.2 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.

D.3.1.3 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.

D.3.1.4 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.

D.3.2 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 (,).

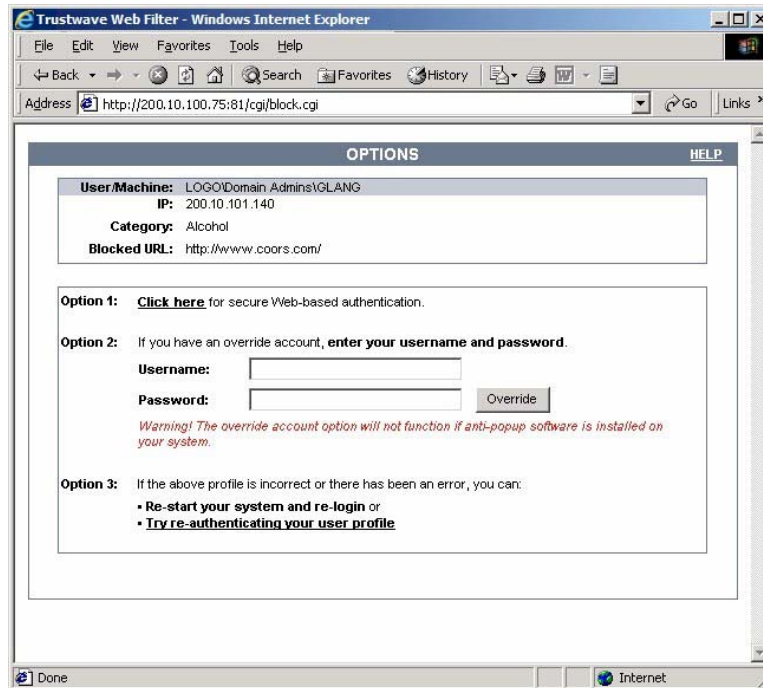
When translated, these strings of code mean:

- 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 suffix ".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:



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).

E.1 Yahoo! Toolbar Pop-up Blocker

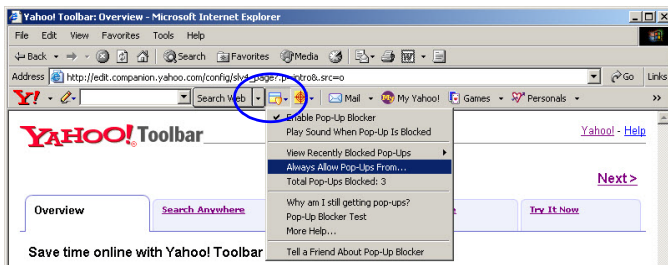
E.1.1 If pop-up blocking is enabled

1. In the Options page, 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.

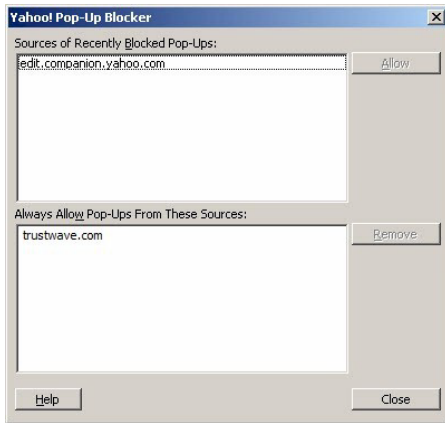
E.1.2 Add override account to the white list

If the override account window was previously blocked by the Yahoo! Toolbar, it can be 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:



2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:



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.

E.2 Google Toolbar Pop-up Blocker

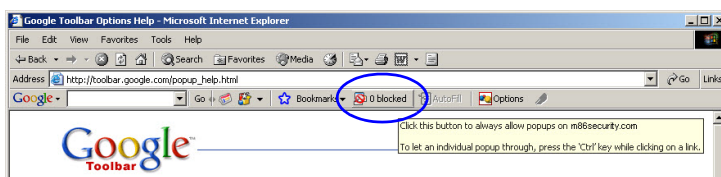
E.2.1 If pop-up blocking is enabled

1. In the Options page, 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.

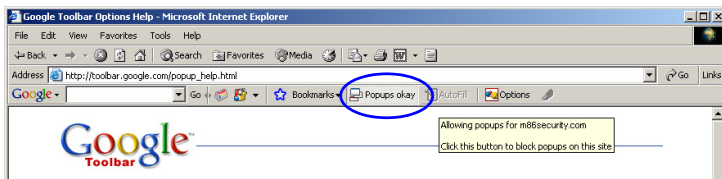
E.2.2 Add override account to the white list

To add the override account window to the white list so that it will always be allowed to pass:

1. Go to the Google Toolbar and click the Pop-up blocker button:



2. Clicking this button toggles to the Pop-ups okay button, adding the override account window to your white list:



E.3 AdwareSafe Pop-up Blocker

E.3.1 If pop-up blocking is enabled

1. In the Options page, 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.

E.3.2 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.

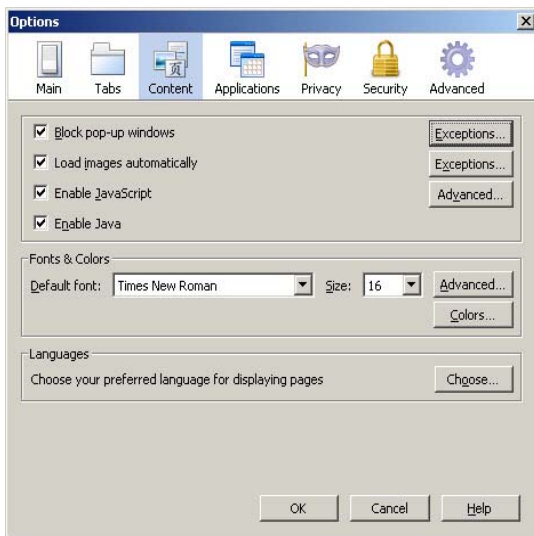
1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.
2. In the Options page, enter your **Username** and **Password**.
3. Click the **Override** button to open the override account pop-up window.
4. Go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # pop-ups blocked. This action turns on pop-up blocking again.

E.4 Mozilla Firefox Pop-up Blocker

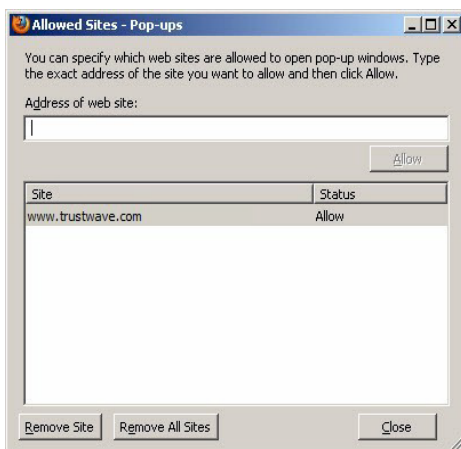
E.4.1 Add override account to the white list

1. From the Firefox browser, go to the toolbar and select **Tools | Options** to open the Options dialog box.

2. Click the Content tab at the top of this box to open the Content section:



3. With the "Block pop-up windows" check box checked, click the **Exceptions...** button at right to open the Allowed Sites - Pop-ups box:



4. Enter the **Address of the web site** to let the override account window pass.
5. Click **Allow** to add the URL to the list box section below.
6. Click **Close** to close the Allowed Sites - Pop-ups box.
7. Click **OK** to close the Options dialog box.

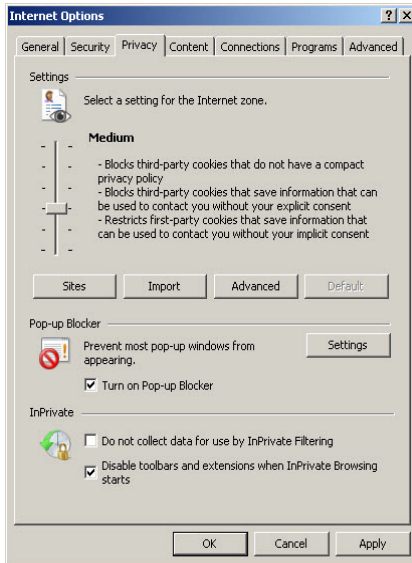
E.5 Windows XP SP2 Pop-up Blocker

E.5.1 Set up pop-up blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

E.5.1.1 Use the Internet Options dialog box

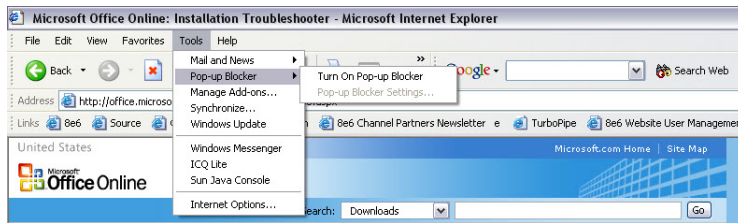
1. From the IE browser, go to the toolbar and select **Tools | Internet Options** to open the Internet Options dialog box.
2. Click the Privacy tab:



3. In the Pop-up Blocker frame, check "Turn on Pop-up Blocker".
4. Click **Apply** and then click **OK** to close the dialog box.

E.5.1.2 Use the IE toolbar

In the IE browser, go to the toolbar and select **Tools | Pop-up Blocker | Turn On Pop-up Blocker**:



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.

E.5.2 Temporarily disable pop-up blocking

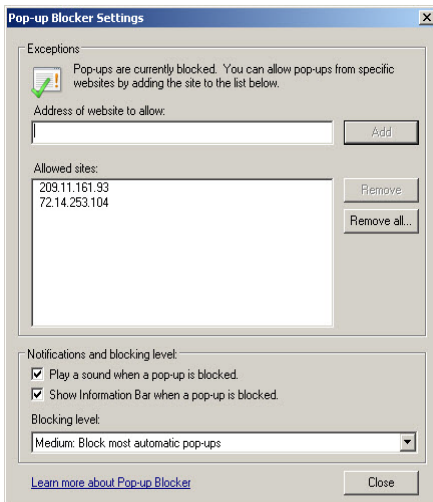
1. In the Options page, enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

E.5.3 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.

E.5.3.1 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:



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

E.5.3.2 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.

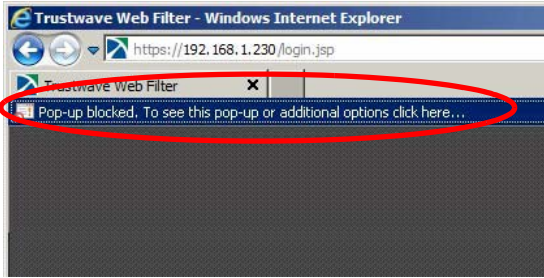
Set up the Information Bar

1. Go to the toolbar and select **Tools | Pop-up Blocker | Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box.
2. In the Notifications and Filter Level frame, click the check box for "Show Information Bar when a pop-up is blocked."
3. Click **Close** to close the dialog box.

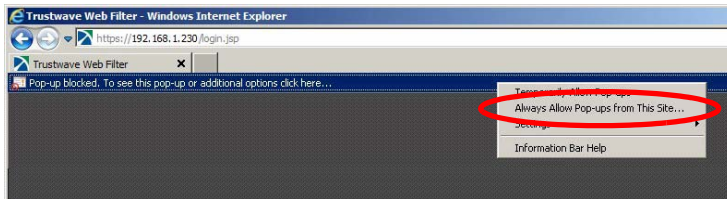
Access your override account

1. In the Options page, 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...":



3. Click the Information Bar for settings options:



4. Select Always Allow Pop-ups from This Site—this action opens the Allow pop-ups from this site? 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 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.

Index

Numerics

3-try login script132

A

Account tab68

active filtering profiles18

Administrator window56

ADS, definition135

alert box, terminology11

Alias List tab70

Alias Name70

always allowed20

Anonymous Bind68

Assign to user79

attribute, definition135

authentication

 activate on network112

 activate Web-based for Global Group121

 activated Web-based for IP group113

 configuration procedures25

 net use based module diagram142

 net use based process141

 servlet35

 setup procedures141

 test net use settings112

 test settings103

 test Web-based settings104

Authentication Form Customization51

authentication method, definition135

Authentication Request Form 47, 103, 111

 figure103

authentication server15

 definition135

 function in net use based process142

 login scripts144

Authentication Settings window37

authentication solution

 single user compatibility chart23

 system deployment options on a network ..24

Authentication SSL Certificate window38

Authenticator 23, 149

authmodule.log58

B

Backup Domain Controller (BDC)136

Block page45

block page17, 18

Block Page Authentication44

Block Page Customization53

block setting20

 definition135

button, terminology11

C

category

 custom categories19

 library19

Category Profile

 domain84

Category tab

 domain84

check box, terminology12

Citrix Virtual Desktop Infrastructure (VDI)149

Common Customization48

common name (cn), definition135

container16, 21

Container Details window82

container, definition135

Create CSR41

Create LDAP Domain dialog box59

custom categories19

D

dialog box, terminology12

directory service, definition135

directory, definition135

Distinguished Name (DN)

 definition135

 LDAP protocol143

Distinguished Name Auto Discovery69

DNS, definition135

domain

 definition136

 delete profile71

domain component (dc), definition136

domain controller, definition136

Domain Name Service (DNS)	135	group administrator, definition	136
dynamic group	16	group name, definition	136
dynamic group, definition	136	group objects	61
E		Group tab	61
edirAgent.log	57	Group/Member Details window	82
eDirectory	151, 160	H	
edirEvent.log	58	HTTPS	29
Enable/Disable Authentication window	34	I	
entry, definition	136	IANA	143
environment requirements	29	individual IP member	
eth0, eth1	31	profile type	17
Exception URL window	89	Internet Explorer	30
F		invisible mode	31, 33
field, terminology	12	definition	136
file formats	173	IP group	15
filter option codes	173	diagram	15
filter options	86	IPC share	142
filter setting	21	J	
definition	136	Java applet	36
filtering		Java Plug-in	29
category codes	172	Java Runtime Environment	29, 37
LDAP group, member, container, workstation		Java Virtual Machine	29
18		JavaScript	29
profile components	18	L	
profile types	16	LAN Settings window	32
rules	21	LAN1, LAN2	33, 38
static profiles	17	LDAP	
user, machine	18	Active Directory Service usage	145
Firefox	30	authentication protocol	23
firewall mode	31, 33	definition	136
definition	136	domain diagram	16
frame, terminology	12	domain groups	15
G		name resolution method	143
gateway IP address	33	server customizations	170
global administrator, definition	136	server setup	145
global filtering profile	18	LDAP Browser window	71
global group	15	LDAP domain	
Google Chrome	30	add	59
grid, terminology	12	add groups, users	71
group		LDAP domain window	60
global	15	LDAP host, definition	137
IP	15	LDAP Query Base	65
LDAP	15	LDAP Type	60
types of	14		

library categories	19	NetBIOS Domain Name	65
list box, terminology	12	NetBIOS name	37
lock profile	17	Netscape Directory Server	60
profile type	18	Network Address Translation (NAT), definition	137
lockout profile	22	NIC device	38
log		Novell	23, 60, 67, 141, 143, 151, 163
view files	57	Novell eDirectory Agent	23, 160
login (or logon) script		O	
definition	137	Open Directory	16, 23, 34, 60, 141, 150
examples	144	open setting	20
usage	142	definition	137
M		OpenLDAP	23, 72
machine name, definition	137	server customizations	170
Macintosh	29, 30	Operation Mode window	31
Manually Add Group dialog box		Options page	46
LDAP	75	organizational unit (ou), definition	137
Manually Add Member dialog box		override account	
LDAP	74	AdwareSafe popup blocking	179
Manually Add Workstation dialog box		block page authentication	44
LDAP	74	definition	137
master IP group	15	Google Toolbar popup blocking	178
filtering profile	17	Mozilla Firefox popup blocking	179
methods		override popup blockers	177
name resolution	143	profile type	18
Microsoft Active Directory		Windows XP SP2 popup blocking	180
Mixed Mode	60, 141	Yahoo! Toolbar popup blocking	177
Native Mode	60, 141	P	
minimum filtering level	20	PDC	
definition	137	definition	138
N		pop-up blocking, disable	177
name resolution		pop-up box/window, terminology	13
definition	137	primary IP address	33
methods	143	Primary Domain Controller (PDC)	136
NAT		profile string	
definition	137	definition	138
navigation panel		elements	171
terminology	12	Profile window	83
nested group	62	protocol	
net use		definition	138
command	132	proxy server	
definition	137	definition	138
syntax	144	pull-down menu, terminology	13
NetBIOS		Q	
definition	137	quota	
name lookup, definition	137		

definition	138	Sub Admin	138
format	173	sub-group	
R		definition	139
radio button, terminology	13	sub-topic	
Radius profile	17	terminology	13
re-authentication		Sun IPlanet	60
block page authentication	44	Sun One	23, 60
net use based process	143	T	
Redirect URL tab		TAR profile	17
domain	86	text box, terminology	13
requirements		Threat Analysis Reporter	22
network	29	Tier 1	
router mode	31, 33	net use based authentication	26, 35, 113, 141
definition	138	Tier 1 and Tier 2 Script	147
rule	20	Tier 2	
criteria	171	time-based, Web-based authentication	145
definition	138	Tier 2 Script	147
rules		Tier 2, Tier 3	
LDAP server setup	145	Web-based authentication	26, 35, 112
S		Tier 3	
Safari	29, 30	session-based, Web-based authentication	148
screen, terminology	13	tiers	
search engine, definition	138	definition	139
secondary IP address	33	Web-based authentication	112
Server tab	64	time profile	
service port	19	add	94
definition	138	definition	139
session-based authentication (Tier 3)	23	profile type	18
Set Group Priority window		time-based authentication (Tier 2)	23
LDAP domain	73	time-based profile	35, 44
Single Sign-On		topic	
Novell eDirectory authentication	160	terminology	13
Tier 1 authentication	141	tree	
single sign-on authentication (Tier 1)	23	terminology	14
SSL certificate	39	Trustwave supplied category	19
Active Directory	163	U	
Novell	168	Upload User/Group Profile window	
obtain, export from LDAP server	163	LDAP domain	76
Sun One	169	URL, definition	139
SSL settings	65	Usage Graphs	104
SSL tab	66	usage logs	57
SSO	160	user objects	62
static filtering profiles	17	User tab	62
static group	15	username formats	171
static group, definition	138		

V

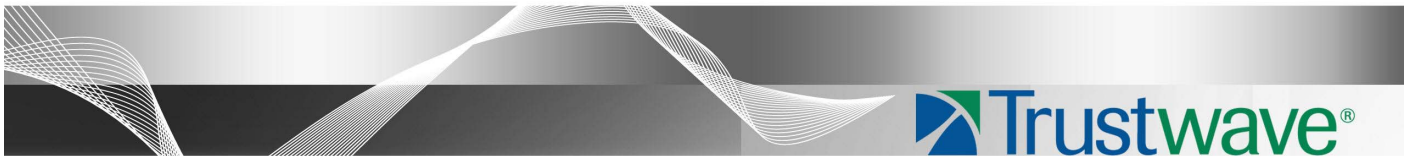
View Log File window57
virtual IP address 38, 144
 definition139

W

warn setting20
warn setting, definition139
Web-based authentication 25, 34, 38
 block page authentication44
 SSL certificate26
Web-based, definition139
white list, definition139
window, terminology14
Windows 729, 30
Windows Vista29, 30
Windows XP30
WINS Server38
workstation objects63
workstation requirements29
Workstation tab63

Y

YouTube Video Control87



About Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit <https://www.trustwave.com>.