

advproxy - Advanced Web Proxy

Advanced Web Proxy Server for IPCop 1.4

Administrator's Guide

advproxy - Advanced Web Proxy

Administrator's Guide

© Copyright 2004-2009
Author: Marco Sondermann
m.sondermann@directbox.com
<http://www.advproxy.net>

advproxy - Advanced Web Proxy

Table of contents

- 1 Preface 5**
 - 1.1 RIGHTS AND DISCLAIMERS 5
 - 1.2 TRADEMARKS 5
 - 1.3 ACKNOWLEDGEMENTS 5
- 2 Introduction 6**
 - 2.1 OVERVIEW 6
 - 2.2 ADVANCED PROXY FEATURE LIST 6
 - 2.3 CLASSROOM EXTENSIONS FEATURE LIST 7
 - 2.4 LEGAL BASIS 8
 - 2.5 SECURITY NOTES 8
 - 2.5.1 Installation and replacement of binary files 8
 - 2.5.2 Firewall rules 8
 - 2.5.3 Passwords 8
- 3 Installation 9**
 - 3.1 INSTALLATION REQUIREMENTS 9
 - 3.2 INSTALLING OR UPDATING THE ADVANCED PROXY ADD-ON 9
 - 3.3 INSTALLING THE CLASSROOM EXTENSIONS (CRE) 9
 - 3.4 REMOVING THE ADVANCED PROXY ADD-ON 10
 - 3.5 AUTOMATIC UPDATE NOTIFICATION 10
 - 3.6 SPECIFIC PROBLEMS WITH OFFICIAL IPCOP UPDATES 10
 - 3.7 INCLUDING USER DEFINED CONFIGURATION DIRECTIVES 11
- 4 Web Proxy configuration 12**
 - 4.1 COMMON SETTINGS 12
 - 4.1.1 Enabled on <Interface> 12
 - 4.1.2 Transparent on <Interface> 12
 - 4.1.3 Proxy Port 12
 - 4.1.4 Visible hostname 12
 - 4.1.5 Cache administrator e-mail 13
 - 4.1.6 Error messages language 13
 - 4.1.7 Error messages design 13
 - 4.1.8 Suppress version information 13
 - 4.1.9 Squid Cache version 13
 - 4.2 UPSTREAM PROXY 14
 - 4.2.1 Proxy address forwarding 14
 - 4.2.2 Client IP address forwarding 14
 - 4.2.3 Username forwarding 14
 - 4.2.4 No connection oriented authentication forwarding 14
 - 4.2.5 Upstream proxy (host:port) 15
 - 4.2.6 Upstream username 15
 - 4.2.7 Upstream password 15
 - 4.3 LOG SETTINGS 16
 - 4.3.1 Enable log 16
 - 4.3.2 Log query terms 16
 - 4.3.3 Log useragents 16
 - 4.4 CACHE MANAGEMENT 17
 - 4.4.1 Memory cache size 17
 - 4.4.2 Harddisk cache size 17
 - 4.4.3 Min object size 17
 - 4.4.4 Max object size 17
 - 4.4.5 Number of level-1 subdirectories 17
 - 4.4.6 Memory replacement policy 18
 - 4.4.7 Cache replacement policy 18
 - 4.4.8 Do not cache these destinations 18
 - 4.4.9 Enable offline mode 19

advproxy - Advanced Web Proxy

- 4.5 DESTINATION PORTS.....20
- 4.6 NETWORK BASED ACCESS CONTROL.....21
 - 4.6.1 Allowed subnets.....21
 - 4.6.2 Disable internal proxy access.....21
 - 4.6.3 Disable internal proxy access to Green from other subnets.....21
 - 4.6.4 Disable internal proxy access from Blue to other subnets22
 - 4.6.5 Unrestricted IP addresses22
 - 4.6.6 Unrestricted MAC addresses.....22
 - 4.6.7 Banned IP addresses or subnets.....23
 - 4.6.8 Banned MAC addresses.....23
- 4.7 TIME RESTRICTIONS.....24
- 4.8 TRANSFER LIMITS24
- 4.9 DOWNLOAD THROTTLING.....25
 - 4.9.1 Bandwidth limits.....25
 - 4.9.2 Content based throttling.....26
- 4.10 MIME TYPE FILTER.....26
- 4.11 WEB BROWSER27
 - 4.11.1 Browser check.....27
 - 4.11.2 Client definitions.....27
- 4.12 PRIVACY28
 - 4.12.1 Fake useragent.....28
 - 4.12.2 Fake referer.....28
- 4.13 URL FILTER29
- 4.14 UPDATE ACCELERATOR.....29
- 5 Authentication configuration.....30**
 - 5.1 AUTHENTICATION METHODS OVERVIEW30
 - 5.1.1 None30
 - 5.1.2 Local Authentication30
 - 5.1.3 Authentication using identd.....30
 - 5.1.4 Authentication using LDAP.....31
 - 5.1.5 Windows authentication.....31
 - 5.1.6 RADIUS authentication.....31
 - 5.2 GLOBAL AUTHENTICATION SETTINGS.....32
 - 5.2.1 Number of authentication processes.....32
 - 5.2.2 Authentication cache TTL32
 - 5.2.3 Limit of IP addresses per user.....32
 - 5.2.4 User/IP cache TTL.....32
 - 5.2.5 Require authentication for unrestricted source addresses.....32
 - 5.2.6 Authentication realm prompt.....32
 - 5.2.7 Destinations without authentication.....33
 - 5.3 LOCAL USER AUTHENTICATION34
 - 5.3.1 User management34
 - 5.3.2 Local user manager.....35
 - 5.3.3 Create user accounts.....36
 - 5.3.4 Edit user accounts.....36
 - 5.3.5 Delete user accounts.....37
 - 5.3.6 Client side password management37
 - 5.4 IDENTD AUTHENTICATION38
 - 5.4.1 Client-side prerequisites38
 - 5.4.2 Common identd settings.....39
 - 5.4.3 User based access restrictions.....40
 - 5.5 LDAP AUTHENTICATION.....41
 - 5.5.1 Common LDAP settings42
 - 5.5.2 Bind DN settings.....43
 - 5.5.3 Group based access control.....43
 - 5.6 WINDOWS AUTHENTICATION.....44
 - 5.6.1 Common domain settings.....45

advproxy - Advanced Web Proxy

- 5.6.2 Authentication mode45
- 5.6.3 User based access restrictions46
- 5.7 RADIUS AUTHENTICATION48
 - 5.7.1 Common RADIUS settings49
 - 5.7.2 User based access restrictions49
- 6 Classroom Extensions configuration (CRE).....50**
 - 6.1.1 Classroom extensions section overview50
 - 6.1.2 Enabled50
 - 6.1.3 Supervisor password50
 - 6.1.4 Classroom group definitions50
 - 6.1.5 Supervisor IP addresses50
 - 6.2 CRE SECURITY LEVELS51
 - 6.2.1 Level 1: No password, no IP address restrictions - no security51
 - 6.2.2 Level 2: Password set, no IP address restrictions - lower security51
 - 6.2.3 Level 3: No Password, IP restrictions applied - lower security52
 - 6.2.4 Level 4: Password set, IP restrictions applied - higher security52
 - 6.3 CLASSROOM GROUP DEFINITIONS53
 - 6.3.1 Creating group definitions53
 - 6.3.2 Group labels and group names53
 - 6.3.3 Client definitions54
 - 6.4 CUSTOM ERROR MESSAGES55
- 7 Web Access Management with CRE.....57**
 - 7.1 STARTING THE WEB ACCESS MANAGEMENT INTERFACE57
 - 7.1.1 "The management interface has been disabled"57
 - 7.1.2 "There are no access groups available"57
 - 7.2 MANAGING ACCESS GROUPS58
 - 7.2.1 Enabled groups58
 - 7.2.2 Disabled groups58
 - 7.3 RESTRICTING MANAGEMENT ACCESS59
 - 7.3.1 Restricting access by password59
 - 7.3.2 Restricting access by IP address60
- 8 Enforcing proxy usage.....62**
 - 8.1 WEB PROXY STANDARD OPERATION MODES62
 - 8.1.1 Proxy service disabled62
 - 8.1.2 Proxy service enabled, running in non-transparent mode63
 - 8.1.3 Proxy service enabled, running in transparent mode64
 - 8.2 CLIENT SIDE WEB PROXY CONFIGURATION65
 - 8.2.1 Manual client configuration65
 - 8.2.2 Client pre-configuration65
 - 8.2.3 Client configuration via DNS / DHCP65
 - 8.2.4 Client configuration using group policies65
 - 8.3 MODIFYING THE FIREWALL RULES66
 - 8.3.1 Adding custom rules to iptables66
 - 8.4 REQUIREMENTS FOR MANDATORY PROXY USAGE68
 - 8.5 AUTHENTICATION AND ADDITIONAL CONTENT FILTERS69
- 9 Active Directory and LDAP authentication71**
 - 9.1.1 Configuring LDAP authentication using Microsoft Active Directory Services71
 - 9.1.2 Configuring LDAP group based access control77

advproxy - Advanced Web Proxy

1 Preface

1.1 Rights and Disclaimers

The information contained within this document may change from one version to the next.

All programs and details contained within this document have been created to the best of the authors knowledge and tested carefully. However, errors cannot be completely ruled out. Therefore the author does not express or imply any guarantees for errors within this document or consequent damage arising from the availability, performance or use of this or related material.

1.2 Trademarks

The use of names in general use, names of firms, trade names, etc. in this document, even without special notation, does not imply that such names can be considered as "free" in terms of trademark legislation and that they can be used by anyone. All trade names are used without a guarantee of free usage and might be registered trademarks. As a general rule, the author adheres to the notation of the manufacturer. Other products mentioned here could be trademarks of the respective manufacturer.

Microsoft, Windows, FrontPage, Internet Explorer and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries/regions.

Novell, NetWare and eDirectory are either registered trademarks or trademarks of Novell, Inc. in the United States and other countries.

1.3 Acknowledgements

Thanks to all the translators for doing a great job, especially

NL: Bjorn Kaag
BZ: Flavio Jose de Siqueira Cavalcanti Veras - flaviove(at)globo(dot)com
IT: Alessio Cecchi - <http://www.cecchi.biz>
FR: Stephane (pulsergene) - thetobby(at)yahoo(dot)fr
ES: Vte. Javier Garcia Mayen - neofito(at)wadalbertia(dot)org
RU: Nikolay Parukhin - parukhin(at)gmail.com

advproxy - Advanced Web Proxy

2 Introduction

2.1 Overview

The Advanced Proxy Server add-on extends the IPCop web proxy service with a lot of versatile, flexible and useful additional features.

All previous proxy settings will be imported to the Advanced Proxy, but remain untouched for all further configuration changes.

For educational institutions, the Advanced Proxy will provide the *Classroom Extensions*, an easy to use administrative interface for the teaching staff.

2.2 Advanced Proxy feature list

In addition to the default IPCop web proxy service, Advanced Proxy offers these new features:

Full GUI integration

- Seamless GUI integration for the Advanced Web Proxy configuration
- All extended options are accessible and configurable within the web based GUI

User authentication

- Local user authentication, including group based user management
- identd authentication
- LDAP authentication, including MS Active Directory, Novell eDirectory and OpenLDAP
- Windows authentication, including Windows NT4.0 or 2000/2003/2008 domains and Samba
- RADIUS authentication

Advanced access control

- Network based access control over IP and MAC addresses
- Time based access restrictions
- Download throttling
- MIME type filter
- Blocking of unauthorized browsers or client software

advproxy - Advanced Web Proxy

2.3 Classroom Extensions feature list

The Classroom Extensions (CRE) for the Advanced Proxy Server will give you the ability to delegate administrative tasks to non-administrative users. Therefore, the CRE will create a new logical role between the Admin and the users: The Supervisor.

The Supervisor may now turn on and off web access for predefined groups (e.g. specific computers in a classroom) without the need of having administrative access rights or knowledge to the IPCop GUI.

In addition to the known Advanced Proxy features, the CRE offers these features:

Full web based access management

- Predefined client groups can be turned on or off using a standard web browser
- All administrative CRE options are accessible and configurable within the web based IPCop GUI

Different security levels

- Web Access Management rights can be controlled by password and/or by network address
- No administrative privileges to the IPCop GUI required for the Web Access Management
- The Supervisor cannot override any Advanced Proxy based restriction set by the IPCop Admin

Flexible configuration

- The IPCop Admin can define client groups with MAC addresses, single IP addresses, IP ranges, subnets or even all of them.

advproxy - Advanced Web Proxy

2.4 Legal basis

Note: Some options of the Advanced Proxy may break the privacy of your clients or other legal rules.

Warning: Before you are using this software make sure that this will be in accordance with the national law or other legal regulations.

Explicit warning: In most countries, the user must agree that personal data will be logged, such as date, time, source and destination in conjunction with the username. Don't use this software in a business environment without the written agreement of the workers council.

2.5 Security notes

2.5.1 Installation and replacement of binary files

Note: This add-on installs additional executable files and libs and replaces the Squid proxy server with a special customized version (currently 2.7 STABLE 5). Squid and the auth modules were compiled from the original source code without any modifications. The configure options are shown with the 'squid -v' command. Under normal circumstances this should not affect security.

2.5.2 Firewall rules

Note: This add-on doesn't modify any firewall rules. If this will be necessary, e.g. for forced authentication, this must be done by your own. See chapter 8.3 for more information.

2.5.3 Passwords

Note: If you are using authentication, beware of the fact that passwords will be transmitted in plain text between your client and the Proxy Server. In addition, when using LDAP, NT or RADIUS authentication, the passwords may be transmitted in plain text between the Proxy Server and the authentication instance (e.g. the LDAP Server or the Domain Controller). This behaviour is by design and should not be a serious flaw in a switched local network environment.

advproxy - Advanced Web Proxy

3 Installation

3.1 Installation requirements

There are no special requirements to be met before installing this add-on.

Note: Some other add-ons which are modifying the proxy settings (especially certain filter modules) may not work after installing this add-on.

3.2 Installing or updating the Advanced Proxy add-on

Step 1: Download the installation package from <http://www.advproxy.net>

Note: Some browsers might change the file extension from .tar.gz to .tar.tar

Step 2: Copy the installation package to your IPCop box. For Windows clients, this can be done using the program WinSCP.

Note: Make sure you are using port 222 instead of port 22 for SCP

Step 3: Log in as root on the console or via SSH. For Windows clients, this can be done using the program PuTTY.

Note: Make sure you are using port 222 instead of port 22 for SSH

Step 4: Extract the installation package using the command
`tar -xzf ipcop-advproxy-version.tar.gz`

Note: Replace *version* with the version of the installation package.

Step 5: Start the installation by entering `ipcop-advproxy/install`

Step 6: Open the IPCop web GUI. Now under the Service section you will find the entry "Proxy" extended to "Advanced Proxy". Select this entry to open the Advanced Proxy GUI page.

Step 7: Change the configuration settings for your needs and restart the Proxy Server to activate the changed settings.

3.3 Installing the Classroom Extensions (CRE)

Follow the steps 1 to 4 at chapter 3.2 for installing the Advanced Proxy add-on.

Install the Classroom Extensions by entering `ipcop-advproxy/install cre`

This installs the Advanced Proxy add-on including the CRE or enables the CRE for an existing installation.

advproxy - Advanced Web Proxy

3.4 Removing the Advanced Proxy add-on

Step 1: Log in as root on the console or via SSH. For Windows clients, this can be done using the program PuTTY.

Note: Make sure you are using port 222 instead of port 22 for SSH

Step 2: Start the removal process by entering `ipcop-advproxy/uninstall`

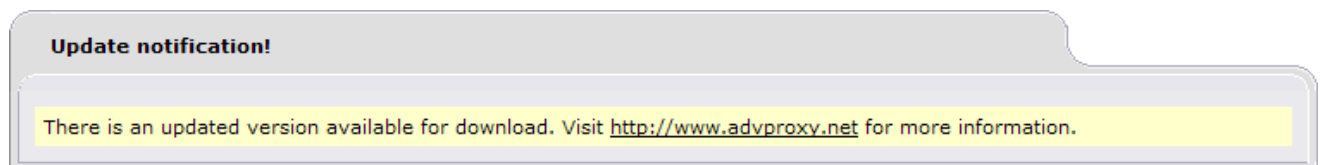
Step 3: Open the IPCop web GUI. Under the Service section select the entry "Proxy".

Step 4: All previous configuration settings are now selected by default. Restart the Proxy Server to activate the previous configuration.

3.5 Automatic update notification

The Advanced Proxy GUI checks the website www.advproxy.net at regular intervals for updates.

If there is a newer version available, an update notification will appear:



Note: The Advanced Proxy GUI will not check for updates while the RED interface is inactive.

Note: Once a newer version is detected, the notification window will appear permanently and can't be cancelled except by upgrading to the latest Advanced Proxy version.

3.6 Specific problems with official IPCop updates

Official updates are designed for unmodified installations and don't care about previous installed add-ons and the files modified by them.

After applying official updates, you may experience different kinds of problems:

The menu item for Advanced Proxy disappears after applying an update

Some official updates will replace the file `/var/ipcop/header.pl` and reset all menu entries to default.

This can be fixed by re-installing the add-on again. There is no need to uninstall the add-on first, because it refreshes all necessary menu modifications and keeps the current add-on settings.

Advanced Proxy doesn't operate properly after applying an update

It may be possible that some binary files necessary for Advanced Proxy will be replaced.

This can be fixed by re-installing the add-on again. There is no need to uninstall the add-on first, because it installs all required files again and keeps the current add-on settings.

advproxy - Advanced Web Proxy

3.7 Including user defined configuration directives

Custom directives for the web proxy configuration (e.g. for integrating Ad-Zap or parent proxy bypassing) can now be added to the file `/var/ipcop/proxy/advanced/acls/include.acl`

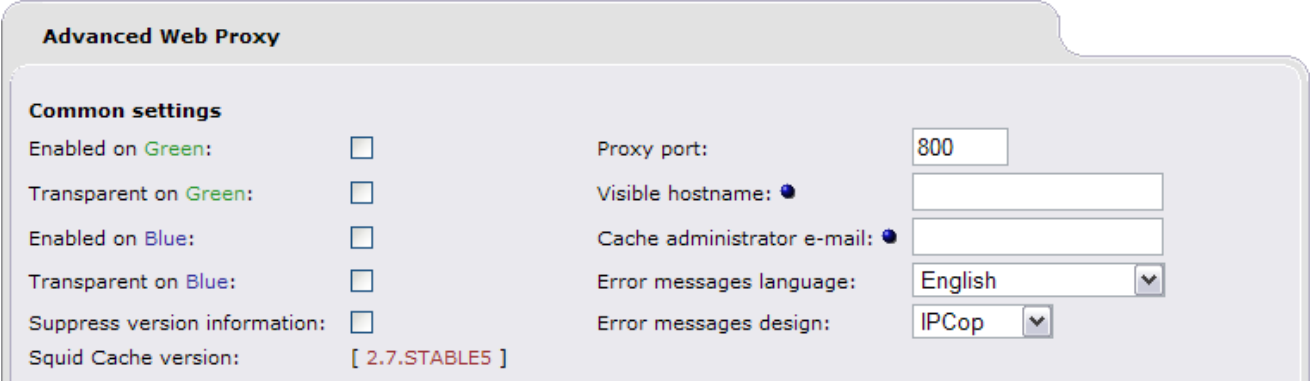
Note: The ACL file `/var/ipcop/proxy/acl` will not be processed by the Advanced Proxy.

advproxy - Advanced Web Proxy

4 Web Proxy configuration

4.1 Common settings

The common settings are essential parameters related to the proxy service.



The screenshot shows the 'Advanced Web Proxy' configuration window. Under the 'Common settings' section, there are several options:

- Enabled on Green:
- Transparent on Green:
- Enabled on Blue:
- Transparent on Blue:
- Suppress version information:
- Squid Cache version: [2.7.STABLE5]
- Proxy port: 800
- Visible hostname:
- Cache administrator e-mail:
- Error messages language: English (dropdown)
- Error messages design: IPCop (dropdown)

4.1.1 Enabled on <Interface>

This enables the Proxy Server to listen for requests on the selected interface (GREEN or BLUE).

Note: If the proxy service is disabled, all client requests will be forwarded directly to the destination address without passing the proxy service and therefore the requests will bypass all configured ACLs.

4.1.2 Transparent on <Interface>

If the transparent mode is enabled, all requests for the destination port 80 will be forwarded to the Proxy Server without the need of any special configuration changes to your clients.

Note: Transparent mode works only for destination port 80. All other requests (e.g. port 443 for SSL) will bypass the Proxy Server.

Note: When using any type of authentication, the Proxy may not run in transparent mode.

Note: To enforce the usage of the Proxy Server in non-transparent mode, you will have to block all outgoing ports usually used for http traffic (80, 443, 8000, 8080, etc.).

4.1.3 Proxy Port

This is the port the Proxy Server will listen for client requests. The default is 800.

Note: In transparent mode, all client requests for port 80 will automatically be redirected to this port.

Note: In non-transparent mode, make sure that your clients are configured to use this port. Otherwise they will bypass the Proxy Server and all ACLs will be ignored.

4.1.4 Visible hostname

If you want to present a special hostname in error messages or for upstream proxy servers (see 4.2.1), then define this. Otherwise, the real hostname of your IPCop will be used.

advproxy - Advanced Web Proxy

4.1.5 Cache administrator e-mail

This mail address will be shown on the Proxy Server error messages.

4.1.6 Error messages language

Select the language in which the Proxy Server error messages will be shown to the clients.

4.1.7 Error messages design

Select the design style in which the Proxy Server error messages will be shown to the clients.

There are two different designs: IPCop and Standard.

IPCop design:



The requested URL could not be retrieved

While trying to retrieve the URL: <http://www.advproxy.net/>

The following error was encountered:

- **Access Denied.**

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is [webmaster](#).

Generated Sun, 13 Aug 2006 20:00:00 GMT by ipcop. (squid)



Standard design:

ERROR

The requested URL could not be retrieved

While trying to retrieve the URL: <http://www.advproxy.net/>

The following error was encountered:

- **Access Denied.**

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is [webmaster](#).

Generated Sun, 13 Aug 2006 20:00:00 GMT by ipcop. (squid)

Note: When a *Visible hostname* (see 4.1.4) is defined, the standard design will be used.

4.1.8 Suppress version information

This disables the Squid Cache version information to be used in the error messages or in the HTTP header.

4.1.9 Squid Cache version

This read-only item shows the release of the installed Squid Cache binary.

advproxy - Advanced Web Proxy

4.2 Upstream proxy

These settings may be required for chained proxy environments.

| Upstream proxy | |
|--|---|
| Proxy address forwarding: <input type="checkbox"/> | Upstream proxy (host:port) <input type="text"/> |
| Client IP address forwarding: <input type="checkbox"/> | Upstream username: <input type="text"/> |
| Username forwarding: <input type="checkbox"/> | Upstream password: <input type="text"/> |
| No connection oriented authentication forwarding: <input type="checkbox"/> | |

4.2.1 Proxy address forwarding

This enables the HTTP VIA header field. If enabled, this information will be added to the HTTP header:

```
1.0 ipcop.localdomain:800 (Squid/2.7.STABLE5)
```

Note: If the last proxy in chain doesn't strip this field, it will be forwarded to the destination host!

This field will be suppressed by default.

4.2.2 Client IP address forwarding

This enables the HTTP X-FORWARDED-FOR header field. If enabled, the internal client IP address will be added to the HTTP header.

```
192.168.1.37
```

This can be useful for source based ACLs or logging on remote proxy servers.

Instead of forwarding "unknown", this field will be completely suppressed by default.

Note: If the last proxy in chain doesn't strip this field, it will be forwarded to the destination host!

4.2.3 Username forwarding

If any type of authentication is activated for Advanced Proxy, this enables the forwarding of the login name.

This can be useful for user based ACLs or logging on remote proxy servers.

Note: This is for ACL or logging purposes only and doesn't work, if the upstream proxy requires a real login.

Note: This forwarding is limited to the username, the password will not be forwarded.

4.2.4 No connection oriented authentication forwarding

This disables the forwarding of Microsoft connection oriented authentication (NTLM and Kerberos).

advproxy - Advanced Web Proxy

4.2.5 Upstream proxy (host:port)

If you are using a parent cache, so enter the IP address and port of this upstream Proxy. If no value for "port" is given, the default port 80 will be used.

4.2.6 Upstream username

Enter the username for the upstream Proxy Server (only if required).

Note: You can enter `PASS` for the username to forward the users credentials to a parent proxy using basic HTTP authentication. The username `PASS` must be entered in upper case:

| Upstream proxy | |
|--|---|
| Proxy address forwarding: <input type="checkbox"/> | Upstream proxy (host:port) <input checked="" type="radio"/> <input type="text" value="192.168.1.240:8080"/> |
| Client IP address forwarding: <input type="checkbox"/> | Upstream username: <input checked="" type="radio"/> <input type="text" value="PASS"/> |
| Username forwarding: <input type="checkbox"/> | Upstream password: <input checked="" type="radio"/> <input type="text"/> |
| No connection oriented authentication forwarding: <input type="checkbox"/> | |

Note: If you enter a password, the username forwarding (see 4.2.3) will be disabled.

4.2.7 Upstream password

Enter the password for the upstream Proxy Server (only if required).

advproxy - Advanced Web Proxy

4.3 Log settings

These options are for enabling the Advanced Proxy log files.

| Log settings | | | |
|--------------|--------------------------|------------------|--------------------------|
| Log enabled: | <input type="checkbox"/> | Log query terms: | <input type="checkbox"/> |
| | | Log useragents: | <input type="checkbox"/> |

4.3.1 Enable log

This enables the Web Proxy logging feature. All client requests will be written to a log file and can be viewed within the GUI under "Logs / Proxy Logs".

4.3.2 Log query terms

The part of the URL containing dynamic queries will be stripped by default before logging. Enabling the option "Log query terms" will turn this off and the complete URL will be logged.

Note: Enabling "Log query terms" may break the privacy of your clients!

4.3.3 Log useragents

Enabling "Log useragent" writes the useragent string to the log file `/var/log/squid/useragent.log`

This log file option should only be activated for debugging purposes and the result is not shown within the GUI based log viewer.

advproxy - Advanced Web Proxy

4.4 Cache management

The cache management settings control the caching parameters for Advanced Proxy.

The screenshot shows the 'Cache management' configuration panel. It includes the following settings:

- Memory cache size (MB): 2
- Min object size (KB): 0
- Number of level-1 subdirectories: 16 (dropdown)
- Memory replacement policy: LRU (dropdown)
- Cache replacement policy: LRU (dropdown)
- Enable offline mode:
- Harddisk cache size (MB): 50
- Max object size (KB): 4096
- Do not cache these destinations (one per line): [Empty text area]

4.4.1 Memory cache size

This is the amount of physical RAM to be used for negative-cached and in-transit objects. This value should not exceed more than 50% of installed RAM. The minimum for this value is 1MB, the default is 2 MB.

Note: This parameter does not specify the maximum process size. It only places a limit on how much additional RAM the Web Proxy will use as a cache of objects.

4.4.2 Harddisk cache size

This is the amount of disk space (MB) to use for cached objects. The default is 50 MB. Change this to suit your configuration. Do not put the size of your disk drive here. Instead, if you want Squid to use the entire disk drive, subtract 20% and use that value.

Note: Setting the cache size to 0 will turn off the harddisk cache.

4.4.3 Min object size

Objects smaller than this size will not be saved on disk. The value is specified in kilobytes, and the default is 0 KB, which means there is no minimum.

4.4.4 Max object size

Objects larger than this size will not be saved on disk. The value is specified in kilobytes, and the default is 4MB. If you wish to increase speed more than you want to save bandwidth you should leave this low.

4.4.5 Number of level-1 subdirectories

The default value for the harddisk cache level-1 subdirectories is 16.

Each level-1 directory contains 256 subdirectories, so a value of 256 level-1 directories will use a total of 65536 directories for the harddisk cache. This will significantly slow down the startup process of the proxy service but can speed up the caching under certain conditions.

Note: The recommended value for level-1 directories is 16. You should increase this value only when it's necessary.

advproxy - Advanced Web Proxy

4.4.6 Memory replacement policy

The memory replacement policy parameter determines which objects are purged from memory, when memory space is needed. The default policy for memory replacement on IPCop is LRU.

Possible replacement policies are:

LRU : Squid's original list based **Last Recently Used** policy

The LRU policies keep recently referenced objects. i.e., it replaces the object that has not been accessed for the longest time.

heap GDSF : **Greedy-Dual Size Frequency**

The heap GDSF policy optimizes object-hit rate by keeping smaller popular objects in cache. So it has a better chance of getting a hit. It achieves a lower byte hit rate than LFUDA though, since it evicts larger (possibly popular) objects.

heap LFUDA : **Least Frequently Used with Dynamic Aging**

The heap LFUDA (Least Frequently Used with Dynamic Aging) policy keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate since one large, popular object will prevent many smaller, slightly less popular objects from being cached.

heap LRU : **Last Recently Used** policy implemented using a heap

Works like LRU, but uses a heap instead.

Note: If using the LFUDA replacement policy, the value of *Max object size* should be increased above its default of 4096 KB to maximize the potential byte hit rate improvement of LFUDA.

4.4.7 Cache replacement policy

The cache replacement policy parameter decides which objects will remain in cache and which objects are evicted (replaced) to create space for the new objects. The default policy for cache replacement on IPCop is LRU.

See chapter 4.4.6 for details.

For more information about the GDSF and LFUDA cache replacement policies see

<http://www.hpl.hp.com/techreports/1999/HPL-1999-69.html> and

<http://fog.hpl.external.hp.com/techreports/98/HPL-98-173.html> .

4.4.8 Do not cache these destinations

A list of sites which cause the request to not be satisfied from the cache and the reply to not be cached. In other words, use this to force objects to never be cached.

Example:

Entire domains and subdomains

```
*.advproxy.net
*.google.com
```

Single hosts

```
www.advproxy.net
www.google.com
```

advproxy - Advanced Web Proxy

IP addresses

81.169.145.75
74.125.39.103

URLs

www.advproxy.net/download
www.google.com/images

Note: You can enter all of these destination types in any order.

| Cache management | | | |
|-----------------------------------|------------------------------------|--|-----------------------------------|
| Memory cache size (MB): | <input type="text" value="2"/> | Harddisk cache size (MB): | <input type="text" value="50"/> |
| Min object size (KB): | <input type="text" value="0"/> | Max object size (KB): | <input type="text" value="4096"/> |
| Number of level-1 subdirectories: | <input type="text" value="16"/> ▼ | Do not cache these destinations (one per line): ● | |
| Memory replacement policy: | <input type="text" value="LRU"/> ▼ | <input type="text" value="*.advproxy.net"/> <input type="text" value="81.169.145.75"/> <input type="text" value="www.urlfilter.net/download"/> <input type="text" value="news.google.com"/> | |
| Cache replacement policy: | <input type="text" value="LRU"/> ▼ | | |
| Enable offline mode: | <input type="checkbox"/> | | |

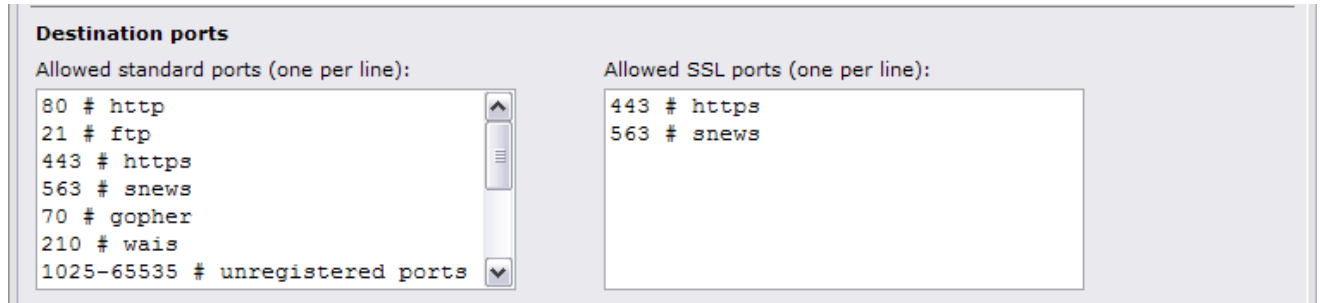
4.4.9 Enable offline mode

Enabling this option will turn off the validation of cached objects. This gives access to more cached information (stale cached versions, where the origin server should have been contacted).

advproxy - Advanced Web Proxy

4.5 Destination ports

This enumerates the allowed destination ports for standard HTTP and SSL encrypted HTTPS requests.



Note: The ports can be defined as a single port number or a range of ports.

Default standard ports:

```
80      # http
21      # ftp
443     # https
563     # snews
70      # gopher
210     # wais
1025-65535 # unregistered ports
280     # http-mgmt
488     # gss-http
591     # filemaker
777     # multiling http
800     # Squids port (for icons)
```

Default SSL ports:

```
443    # https
563    # snews
```

advproxy - Advanced Web Proxy

4.6 Network based access control

This defines the access control for accessing the Proxy Server based on the client network address.

Network based access control

Allowed subnets (one per line):

```
192.168.1.0/255.255.255.0
192.168.2.0/255.255.255.0
```

Disable internal proxy access:

Disable internal proxy access to Green from other subnets:

Disable internal proxy access from Blue to other subnets:

Unrestricted IP addresses (one per line): ●

Unrestricted MAC addresses (one per line): ●

Banned IP addresses (one per line): ●

Banned MAC addresses (one per line): ●

4.6.1 Allowed subnets

All listed subnets are allowed to access the Proxy Server. By default, the subnets for GREEN and BLUE (if available) are listed here.

You can add other subnets like subnets behind GREEN in larger environments to this list. All subnets not listed here will be blocked for web access.

4.6.2 Disable internal proxy access

This option prevents direct HTTP access through the internal proxy service to local web servers at those subnets as defined in section 4.6.1. This selection overrides the following two options which manage HTTP access to GREEN and from BLUE.

4.6.3 Disable internal proxy access to Green from other subnets

This prevents direct HTTP access through the internal proxy service to web servers on GREEN from any other subnet (e.g. BLUE).

Example:

While proxy access is enabled for GREEN and BLUE, usually all requests will be forwarded to RED. But when a client from BLUE wants to access a web server on GREEN, the Proxy Server takes the internal shortcut between the BLUE and the GREEN interface, regardless of any firewall rules.

advproxy - Advanced Web Proxy

Note: To protect your servers on GREEN, it's recommended to enable this option and use *Blue Access* or *DMZ pinholes* if necessary.

4.6.4 Disable internal proxy access from Blue to other subnets

This prevents direct HTTP access through the internal proxy service from BLUE to web servers on any other subnet (e.g.GREEN).

Example:

While proxy access is enabled for GREEN and BLUE, usually all requests will be forwarded to RED. But when a client from BLUE wants to access a web server on GREEN, the Proxy Server takes the internal shortcut between the BLUE and the GREEN interface, regardless of any firewall rules.

Note: This option is only available with a BLUE interface installed.

Note: If enabled, clients on BLUE can only access web servers on BLUE or RED.

4.6.5 Unrestricted IP addresses

All client IP addresses in this list will override the following restrictions:

- Time restrictions
- Size limits for download requests
- Download throttling
- Browser check
- MIME type filter
- Authentication (will be required by default for these addresses, but can be turned off)
- Concurrent logins per user (only available if authentication is enabled)

4.6.6 Unrestricted MAC addresses

All client MAC addresses in this list will override the following restrictions:

- Time restrictions
- Size limits for download requests
- Download throttling
- Browser check
- MIME type filter
- Authentication (will be required by default for these addresses, but can be turned off)
- Concurrent logins per user (only available if authentication is enabled)

Using MAC addresses instead of IP addresses can be useful if the DHCP service is enabled without having fixed leases defined.

MAC addresses can be entered in either one of these forms:

00-00-00-00-00-00 or 00:00:00:00:00:00

Note: The Proxy Server can only determine MAC addresses from clients configured for the subnets of the GREEN, BLUE or ORANGE interfaces.

advproxy - Advanced Web Proxy

4.6.7 Banned IP addresses or subnets

All requests from these clients (IP addresses or subnets) in this list will be blocked.

4.6.8 Banned MAC addresses

All requests from these clients in this list will be blocked.

Using MAC addresses instead of IP addresses can be useful if the DHCP service is enabled without having fixed leases defined.

MAC addresses can be entered in either one of these forms:

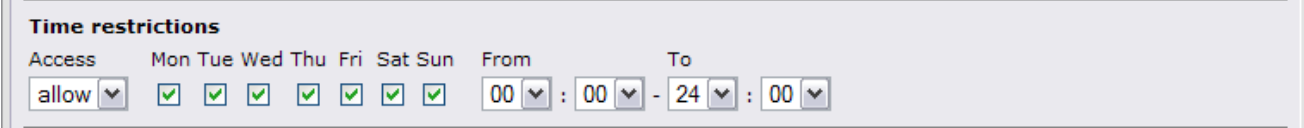
00-00-00-00-00-00 or 00:00:00:00:00:00

Note: The Proxy Server can only determine MAC addresses from clients configured for the subnets of the GREEN, BLUE or ORANGE interfaces.

advproxy - Advanced Web Proxy

4.7 Time restrictions

This defines the operational time of the Web Proxy.



Time restrictions

Access: allow

Mon: Tue: Wed: Thu: Fri: Sat: Sun:

From: 00 : 00 - To: 24 : 00

The option “allow” allows web access and the option “deny” blocks web access within the selected time. The choice of “allow” or “deny” will depend on the time rules you want to apply.

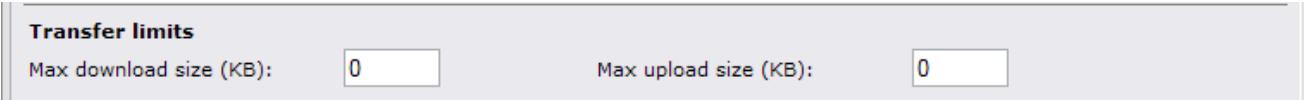
The default is set to allow access every day around the clock.

Note: Time restrictions will not be effective for these clients:

- Unrestricted source IP addresses
- Unrestricted source MAC addresses
- Members of the group “Extended” if the Proxy uses “Local authentication”

4.8 Transfer limits

This allows you to enter limitations of the size for each download and/or upload request.



Transfer limits

Max download size (KB): 0

Max upload size (KB): 0

The values are given in KB. A reason for transfer limits could be that you want to prevent downloading large files, such as CD images.

The default is set to 0 KB for upload and download. This value turns off any limitation.

Note: These limits refer to each single request. It's not the total amount for all requests.

Note: Download limits will not be effective for these clients:

- Unrestricted source IP addresses
- Unrestricted source MAC addresses
- Members of the group “Extended” if the Proxy Server uses “Local authentication”

Note: Upload limits will be effective for all clients.

advproxy - Advanced Web Proxy

4.9 Download throttling

The download bandwidth can be limited in general, per host and depending on the content.

Download throttling

Overall limit on Green: Limit per host on Green:

Overall limit on Blue: Limit per host on Blue:

Enable content based throttling:

Binary files: CD images: Multimedia:

Note: Download throttling works on a per machine basis and not per user

Throttling will not be effective for these clients:

- Unrestricted source IP addresses
- Unrestricted source MAC addresses

4.9.1 Bandwidth limits

Limits can be defined per interface as an overall limit and per host. The used bandwidth for all hosts will be limited by the overall limit.

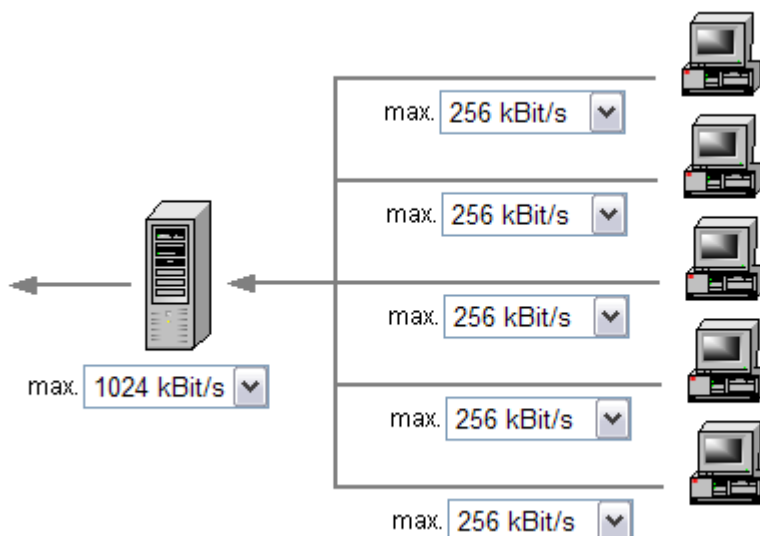
Example:

The following settings

Download throttling

Overall limit on Green: Limit per host on Green:

will result in this configuration:



advproxy - Advanced Web Proxy

4.9.2 Content based throttling

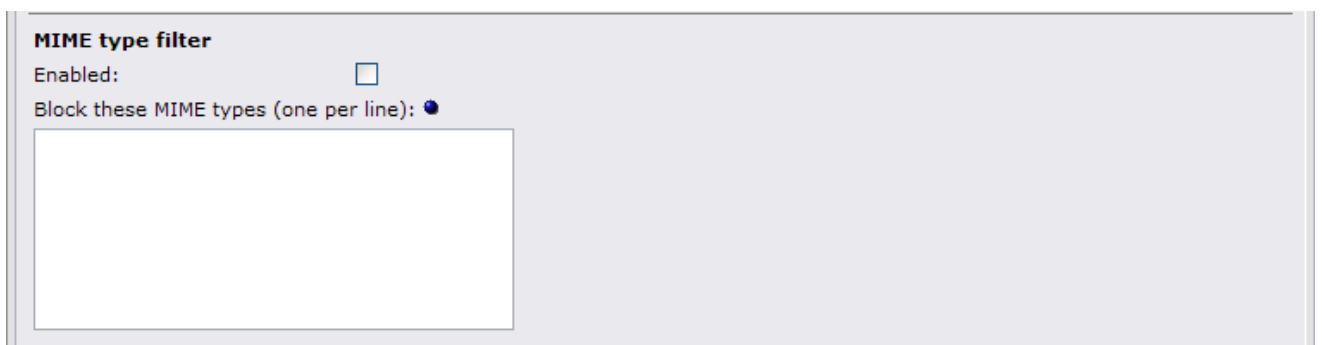
By default, throttling affects all kind of traffic, but throttling can be limited to some types of content:

- *Binary files*: executables, archives, etc.
- *CD images*: CD and DVD image files
- *Multimedia*: audio and video files

Note: Selecting one of these options disables throttling for all other types of traffic.

4.10 MIME type filter

The MIME type filter can be configured to block content depending on its MIME type.



If enabled, the filter checks all incoming headers for their MIME type. If the requested MIME type is listed to be blocked, the access to this content will be denied. This way you can block content, no matter of the given file name extension.

Examples:

Add this MIME type if you want to block the download of PDF files:

```
application/pdf
```

Add these MIME types if you want to block the download of MPEG and QuickTime video files:

```
video/mpeg  
video/quicktime
```

Note: The MIME type are processed as regular expressions. This means, the MIME type

```
javascript
```

will block content with the MIME types

```
application/x-javascript  
text/javascript
```

Note: MIME type blocking will not be effective for these clients:

- Unrestricted source IP addresses
- Unrestricted source MAC addresses
- Members of the group "Extended" if the Proxy Server uses "Local authentication"

advproxy - Advanced Web Proxy

4.11 Web browser

This allows you to control which client software may have access to web sites.

| Web browser | | | |
|---------------------------------|--------------------------|-----------------|--------------------------|
| Enable browser check: | <input type="checkbox"/> | | |
| Allowed clients for web access: | | | |
| AOL: | <input type="checkbox"/> | AvantBrowser: | <input type="checkbox"/> |
| Firefox: | <input type="checkbox"/> | FrontPage: | <input type="checkbox"/> |
| Gecko compatible: | <input type="checkbox"/> | GetRight: | <input type="checkbox"/> |
| Go!Zilla: | <input type="checkbox"/> | Google Chrome: | <input type="checkbox"/> |
| Google Earth: | <input type="checkbox"/> | Google Toolbar: | <input type="checkbox"/> |
| Internet Explorer: | <input type="checkbox"/> | Java: | <input type="checkbox"/> |
| Konqueror: | <input type="checkbox"/> | Lynx: | <input type="checkbox"/> |
| MacOSX Update: | <input type="checkbox"/> | Media Player: | <input type="checkbox"/> |
| Netscape: | <input type="checkbox"/> | Opera: | <input type="checkbox"/> |
| Safari: | <input type="checkbox"/> | WGA: | <input type="checkbox"/> |
| Wget: | <input type="checkbox"/> | Windows Update: | <input type="checkbox"/> |
| apt-get: | <input type="checkbox"/> | | |

4.11.1 Browser check

If this option is enabled, only the selected clients will be able to pass the Proxy Server. All other requests will be blocked.

Note: Browser based access control will not be effective for these clients:

- Unrestricted source IP addresses
- Unrestricted source MAC addresses
- Members of the group "Extended" if the Proxy Server uses "Local authentication"

4.11.2 Client definitions

The most important web clients are already listed. You can create your own definitions by editing the file `/var/ipcop/proxy/advanced/useragents` and adding the browser specific information there.

Adding custom clients could be necessary if you want to allow your AntiVirus software to download updated definitions. If you don't know the useragent of this software, you can enable the useragent logging in the section "Log settings" and watch the file `/var/log/squid/useragent.log`

The syntax for client definitions is:

name, display, (regexp)

name is required for internal processing of the Advanced Proxy and should be a short name in alphanumeric capital letters without spaces.

display is the string which appears in the GUI list and should contain the common name for this client.

(regexp) is a regular expression which matches the browser useragent string and must always be enclosed with brackets.

The values are separated by commas.

advproxy - Advanced Web Proxy

4.12 Privacy

This allows the modification of some HTTP header fields to protect your privacy.



4.12.1 Fake useragent

By default, the useragent of the currently used web browser will be submitted to external web servers. Some dynamic websites generate the content depending on the submitted useragent string. This string will also be logged to the Web Server log files.

With the "Fake useragent" option you have the ability to rewrite this string for all your clients. For outgoing requests the useragent header field will be changed by the Proxy Server and submitted to external sites instead of the original useragent string. This can be useful to protect your privacy or to enforce a desired level of compatibility.

Examples:

The following string will make external servers believe that all your clients are using the Firefox browser:

Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.3) Gecko/20041002 Firefox/0.10

Even though it's possible to enter a free defined string, a useragent like

Mozilla/1.0 (compatible; web enabled game console)

will probably lead to difficulties to display some websites in a correct manner.

4.12.2 Fake referer

When clicking a hyperlink, the source URL will be submitted to the destination website. This can be turned off by entering a user defined string. This string will be submitted instead of the real referring URL. This can be useful to protect your privacy.

Examples:

This replaces the source URL with a reference to the Advanced Proxy:

Referer blocked by Advanced Proxy (http://www.advproxy.net)

To anonymize your referer, you can enter a string like this:

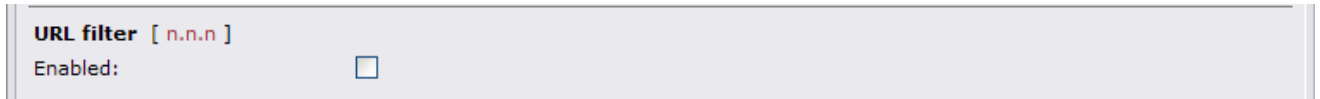
http://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Note: This violates the HTTP standard and may sometimes lead to difficulties. Some websites are blocking requests with an invalid referer to protect themselves against so called deep links or the abuse by "stealing" graphics from their website.

advproxy - Advanced Web Proxy

4.13 URL filter

This enables the URL filter add-on.



The red number between the square brackets indicates the version number of the installed URL filter.

This is an optional configuration item and is only available if the URL filter add-on is installed.

The URL filter add-on integrates in the Advanced Proxy but is not part of the Advanced Proxy package and must be installed separately.

You can download the URL filter at <http://www.urlfilter.net>

4.14 Update accelerator

This enables the Update accelerator add-on.



The red number between the square brackets indicates the version number of the installed Update accelerator.

This is an optional configuration item and is only available if the Update accelerator add-on is installed.

The Update accelerator add-on integrates in the Advanced Proxy but is not part of the Advanced Proxy package and must be installed separately.

You can download the Update accelerator at <http://update-accelerator.advproxy.net>

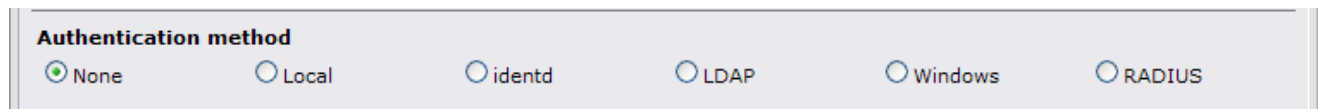
advproxy - Advanced Web Proxy

5 Authentication configuration

Note: When using authentication and enabling the web proxy log files, the requesting user name will be logged in addition to the requested URL. Before enabling log files while using authentication, make sure not to violate existing laws.

5.1 Authentication methods overview

The Advanced Proxy offers a variety of methods for user authentication.



5.1.1 None

Authentication is disabled. Users don't need to authenticate when accessing web sites.

5.1.2 Local Authentication

This authentication method is the preferred solution for SOHO environments. Users need to authenticate when accessing web sites by entering a valid username and password. The user management resides on the IPCop Proxy Server. Users are categorized into three groups: *Extended*, *Standard* and *Disabled*.

5.1.3 Authentication using identd

This authentication method is the preferred solution for environments where

- *Authentication must be a "hidden" process without entering username and password*
- *Proxy service must operate in transparent mode*
- *Usernames will be used only for logging rather than for authentication*

The identd authentication method requires an identd service or daemon running on the client.

advproxy - Advanced Web Proxy

5.1.4 Authentication using LDAP

This authentication method is the preferred solution for medium and large network environments. Users will have to authenticate when accessing web sites by entering a valid username and password. The credentials are verified against an external Server using the Lightweight Directory Access Protocol (LDAP).

LDAP authentication will be useful if you have already a directory service in your network and don't want to maintain additional user accounts and passwords for web access.

Advanced Proxy works with these types of LDAP Servers:

- *Active Directory* (Windows 2000, 2003 and 2008 Server)
- *Novell eDirectory* (NetWare 5.x und NetWare 6)
- *LDAP Version 2 and 3* (OpenLDAP)

As an option, membership for a certain group can be required.

Note: The protocol LDAPS (Secure LDAP) is not supported by Advanced Proxy.

5.1.5 Windows authentication

This authentication method is the preferred solution for small and medium network environments. Users will have to authenticate when accessing web sites. The credentials are verified against an external Server acting as a Domain Controller. This can be a

- Windows NT 4.0 Server or Windows 2000/2003/2008 Server (even with Active Directory enabled)
- Samba 2.x / 3.x Server (running as Domain Controller)

Advanced Proxy works with Windows integrated authentication (transparent) or with standard authentication (explicit with username and password).

You can maintain lists with authorized user names (whitelist) or unauthorized user names (blacklist).

Note: Workgroup based authentication may probably work, but is neither recommended nor supported.

5.1.6 RADIUS authentication

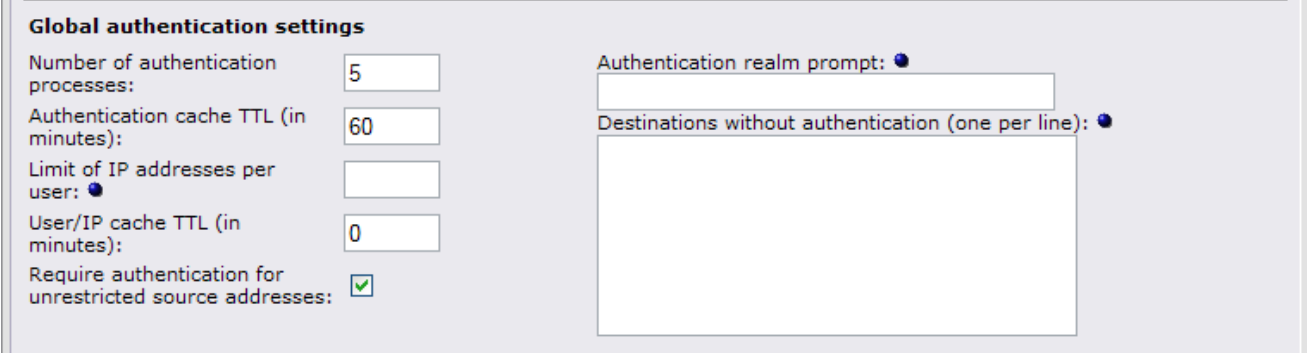
This authentication method is the preferred solution for small and medium network environments. Users will have to authenticate when accessing web sites. The credentials are verified against an external RADIUS server.

You can maintain lists with authorized user names (whitelist) or unauthorized user names (blacklist).

advproxy - Advanced Web Proxy

5.2 Global authentication settings

The global authentication settings are available for all authentication methods except for the identd method.



The screenshot shows the 'Global authentication settings' configuration page. It contains several input fields and a checkbox:

- Number of authentication processes:** Input field with value 5.
- Authentication cache TTL (in minutes):** Input field with value 60.
- Limit of IP addresses per user:** Input field (empty).
- User/IP cache TTL (in minutes):** Input field with value 0.
- Require authentication for unrestricted source addresses:** Checked checkbox.
- Authentication realm prompt:** Input field (empty).
- Destinations without authentication (one per line):** Text area (empty).

5.2.1 Number of authentication processes

The number of background processes listening for requests. The default value is 5 and should be increased if authentication takes too long or Windows integrated authentication falls back to explicit authentication.

5.2.2 Authentication cache TTL

Duration in minutes how long credentials will be cached for each single session. If this time expires, the user has to re-enter the credentials for this session. The default is set to 60 minutes, the minimum will be 1 minute. The TTL will always be reset when the user sends a new request to the Proxy Server within a session.

Note: If the user opens a new session, the credentials must always be entered, even if the TTL has not expired for another session.

5.2.3 Limit of IP addresses per user

Number of source IP addresses a user can be logged in at a time. The IP address will be released after the time defined at *User/IP cache TTL*.

Note: This takes no effect if running Local authentication and the user is a member of the *Extended* group.

5.2.4 User/IP cache TTL

Duration in minutes, how long relations between each user name and the used IP address will be cached. The default value is 0 (disabled).

A value greater than 0 is only reasonable while using a limit for concurrent IP addresses per user.

5.2.5 Require authentication for unrestricted source addresses

By default authentication is required even for unrestricted IP addresses. If you don't want to require authentication for these addresses, untick this box.

5.2.6 Authentication realm prompt

This text will be shown in the authentication dialog. The default is "IPCop Advanced Proxy Server".

advproxy - Advanced Web Proxy

5.2.7 Destinations without authentication

This allows you to define a list of destinations that can be accessed without authentication.

Note: Any domains listed here are destination DNS domains and not source Windows NT domains.

Example:

Entire domains and subdomains

```
*.advproxy.net  
*.google.com
```

Single hosts

```
www.advproxy.net  
www.google.com
```

IP addresses

```
81.169.145.75  
74.125.39.103
```

URLs

```
www.advproxy.net/download  
www.google.com/images
```

Note: You can enter all of these destination types in any order.

Example for Windows Update:

To allow access to Windows Update without authentication add these destinations to the list:

```
*.download.microsoft.com  
*.windowsupdate.com  
windowsupdate.microsoft.com
```

advproxy - Advanced Web Proxy

5.3 Local user authentication

The Local user authentication lets you manage user accounts locally without the need for external authentication servers.

Authentication method

None Local identd LDAP Windows RADIUS

Global authentication settings

Number of authentication processes:

Authentication cache TTL (in minutes):

Limit of IP addresses per user:

User/IP cache TTL (in minutes):

Require authentication for unrestricted source addresses:

Authentication realm prompt:

Destinations without authentication (one per line):

Local user authentication

Min password length:

Bypass redirection for members of the group 'Extended':

[User management](#)

5.3.1 User management

The integrated user manager can be executed from the main settings page.

Local user authentication

Min password length:

Bypass redirection for members of the group 'Extended':

[User management](#)

Min password length

Enter the minimum required length of passwords. The default is set 6 alphanumeric characters.

Bypass redirection for members of the group extended

If any redirector (e.g. like the URL filter add on) is installed, all members of the group *Extended* will bypass this redirector.

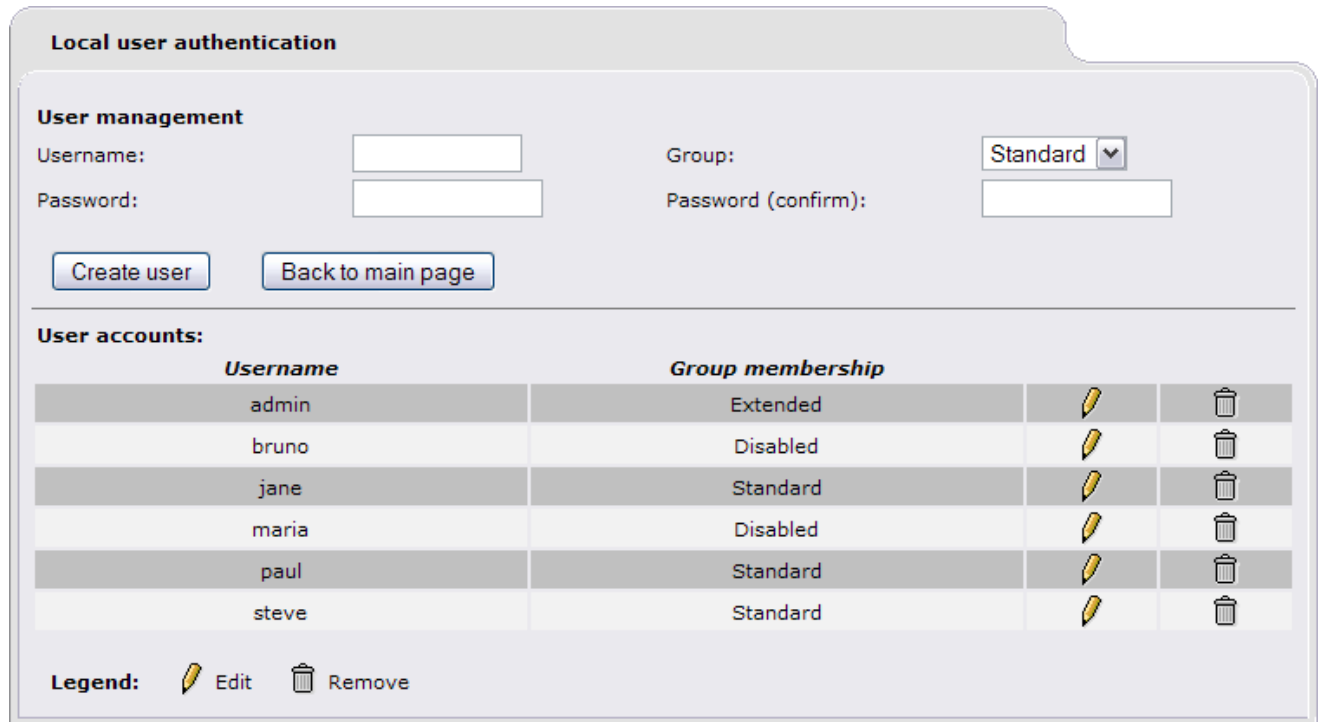
User management

This button opens the local user manager.

advproxy - Advanced Web Proxy

5.3.2 Local user manager

The user manager is the interface for creating, editing and deleting user accounts.



Within the user manager page, all available accounts are listed in alphabetically order.

Group definitions

You can select between three different groups:

Standard The default for all users. All given restrictions apply to this group.

Extended Use this group for unrestricted users. Members of this group will bypass any time and filter restrictions.

Disabled Members of this group are blocked. This can be useful if you want to disable an account temporarily without losing the password.

Proxy service restart requirements

The following changes to user accounts will require a restart of the proxy service:

- a new user account was added and the user is not a member of the *Standard* group
- the group membership for a certain user has been changed

The following changes to user accounts will not require a restart of the proxy service:

- a new user account was added and the user is a member of the *Standard* group
- the password for a certain user has been changed
- an existing user account has been deleted

advproxy - Advanced Web Proxy

5.3.3 Create user accounts

Username

Enter the username for the user. If possible, the name should contain only alphanumeric characters.

Group

Select the group membership for this user.

Password

Enter the password for the new account.

Password (confirm)

Confirm the previously entered password.

Create user

This button creates a new user account. If this username already exists, the account for this username will be updated with the new group membership and password.

Back to main page

This button closes the user manager and returns to the Advanced Proxy main page.

5.3.4 Edit user accounts

An user account can be edited by clicking on the pencil icon. When editing an user account, only the group membership or password can be changed.

While editing an account, the referring entry will be marked with a yellow bar.

The screenshot shows the 'Local user authentication' interface. At the top, there is a 'User management' section with input fields for 'Username' (containing 'maria'), 'Group' (a dropdown menu set to 'Disabled'), 'Password' (masked with dots), and 'Password (confirm)' (masked with dots). Below these fields are three buttons: 'Update user', 'Reset', and 'Back to main page'. Underneath is a 'User accounts:' section containing a table with columns for 'Username' and 'Group membership'. The table lists several users: admin (Extended), bruno (Disabled), jane (Standard), maria (Disabled), paul (Standard), and steve (Standard). Each row has a pencil icon for editing and a trash can icon for removal. The row for 'maria' is highlighted in yellow. A legend at the bottom left shows a pencil icon for 'Edit' and a trash can icon for 'Remove'.

| Username | Group membership | | |
|----------|------------------|--|--|
| admin | Extended | | |
| bruno | Disabled | | |
| jane | Standard | | |
| maria | Disabled | | |
| paul | Standard | | |
| steve | Standard | | |

To save the changed settings, use the button [Update user].

Note: The username can not be modified. This field is read-only. If you need to rename a user, delete this user and create a new account.

advproxy - Advanced Web Proxy

5.3.5 Delete user accounts

An user account can be deleted by clicking on the trashcan icon. The account will be deleted immediately.

5.3.6 Client side password management

Users may change their passwords if needed. The interface can be invoked by entering this URL:

```
http://ipcop-green-ip:81/cgi-bin/chpasswd.cgi
```

Note: Replace *ipcop-green-ip* with the GREEN IP address of your IPCop.

The web page dialog requires the username, the current password and the new password (twice for confirmation):

Change web access password

Username:

Current password:

New password:

New password (confirm):

Advanced Proxy running on IPCop

Web page dialog language

The language for this dialog will be the same language that you have selected for the internal IPCop GUI. If you want to appear this dialog in another language than your IPCop GUI, you can force a certain language by editing the file `/home/httpd/cgi-bin/chpasswd` and clamping the language to a language supported by the Advanced Proxy.

advproxy - Advanced Web Proxy

5.4 identd authentication

This authentication method uses a client-side running identd for user authentication. Unlike other authentication methods, identd comes without the "Global authentication settings" section.

The screenshot shows the configuration page for the 'identd' authentication method. At the top, under 'Authentication method', 'identd' is selected with a radio button. Below this, the 'Common identd settings' section includes: 'Require identd authentication' (unchecked), 'Require authentication for unrestricted source addresses' (checked), 'Ident timeout (in seconds)' (input field with '10'), 'Ident aware hosts (one per line)' (text area with '192.168.1.0/255.255.255.0'), and 'Destinations without authentication (one per line)' (text area). The 'User based access restrictions' section has 'Enabled' (unchecked), 'Use positive access control' (selected), and 'Use negative access control' (unselected). Below these are two text areas for 'Authorized users (one per line)' and 'Unauthorized users (one per line)'.

In addition to the authentication you can define positive or negative user based access control lists.

5.4.1 Client-side prerequisites

Most Linux based clients already have an ident daemon (identd) installed by default.

For Windows clients, there are several free identd implementations available. This one works for Windows XP and Vista: <http://rndware.info/content/Windows+Ident+Server>

Note: Port 113 (TCP) must be opened on client based firewalls.

advproxy - Advanced Web Proxy

5.4.2 Common identd settings

Common identd settings

Require identd authentication:

Ident timeout (in seconds):

Ident aware hosts (one per line):
192.168.1.0/255.255.255.0

Require authentication for unrestricted source addresses:

Destinations without authentication (one per line):

Require identd authentication

By default, identd authentication will not be mandatory. This configuration can be useful for logging purposes. If you want to use identd for enforced authentication, this option must be enabled. Access for clients which don't authenticate using identd will be denied.

Note: The proxy cannot run in transparent mode when using identd authentication.

Require authentication for unrestricted source addresses

If "Require ident authentication" is enabled, authentication will be also required for unrestricted IP addresses. If you don't want to require authentication for unrestricted addresses, untick this box.

Ident timeout

Maximum time in seconds for the Proxy to wait for ident lookups to be completed.

Ident aware hosts

This enables ident lookups for the listed client addresses. Client addresses that are not listed here will not receive ident requests.

Note: Unlisted clients will gain access without authentication, even if the option "Require ident authentication" is enabled.

Destinations without authentication

This allows you to define a list of destinations that can be accessed without authentication.

Note: Any domains listed here are destination DNS domains and not source Windows NT domains.

Example:

Entire domains and subdomains

```
*.advproxy.net  
*.google.com
```

Single hosts

```
www.advproxy.net  
www.google.com
```

IP addresses

```
81.169.145.75
```

advproxy - Advanced Web Proxy

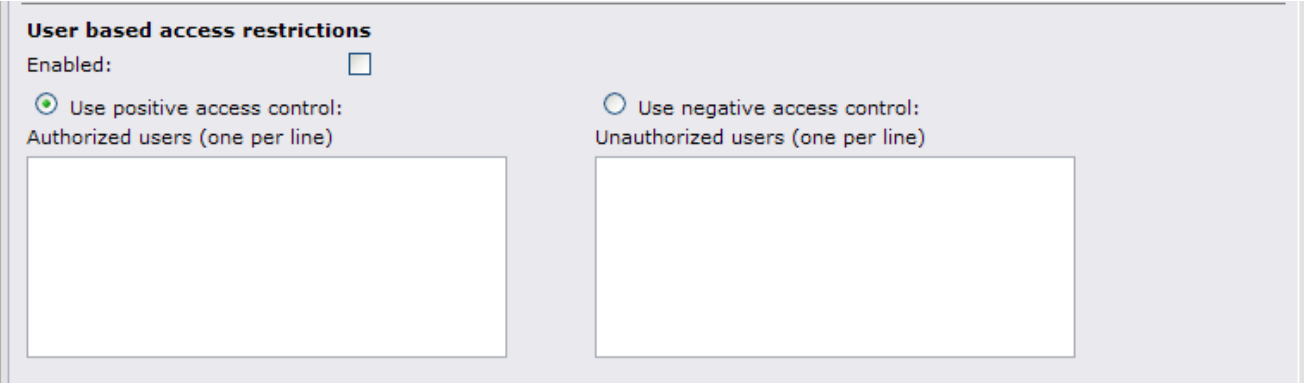
74.125.39.103

URLs

www.advproxy.net/download
www.google.com/images

Note: You can enter all of these destination types in any order.

5.4.3 User based access restrictions



User based access restrictions

Enabled:

Use positive access control:
Authorized users (one per line)

Use negative access control:
Unauthorized users (one per line)

Enabled

Enables access control lists for authorized or unauthorized users.

Use positive access control / Authorized users

These listed users will be allowed for web access. For all other users, access will be denied.

Use negative access control / Unauthorized users

These listed users will be blocked for web access. For all other users, access will be allowed.

advproxy - Advanced Web Proxy

5.5 LDAP authentication

This authentication method uses an existing directory infrastructure for user authentication.

| | | | | | |
|---|-------------------------------------|---|---|-------------------------------|------------------------------|
| Authentication method | | | | | |
| <input type="radio"/> None | <input type="radio"/> Local | <input type="radio"/> identd | <input checked="" type="radio"/> LDAP | <input type="radio"/> Windows | <input type="radio"/> RADIUS |
| Global authentication settings | | | | | |
| Number of authentication processes: | <input type="text" value="5"/> | Authentication realm prompt: | <input type="text"/> | | |
| Authentication cache TTL (in minutes): | <input type="text" value="60"/> | Destinations without authentication (one per line): | <input type="text"/> | | |
| Limit of IP addresses per user: | <input type="text"/> | | | | |
| User/IP cache TTL (in minutes): | <input type="text" value="0"/> | | | | |
| Require authentication for unrestricted source addresses: | <input checked="" type="checkbox"/> | | | | |
| Common LDAP settings | | | | | |
| Base DN: | <input type="text"/> | LDAP type: | <input type="text" value="Active Directory"/> | | |
| LDAP Server: | <input type="text"/> | Port: | <input type="text" value="389"/> | | |
| Bind DN settings | | | | | |
| Bind DN username: | <input type="text"/> | Bind DN password: | <input type="text"/> | | |
| Group based access control | | | | | |
| Required group: | <input type="text"/> | | | | |

If you are unsure about your internal directory structure, you can examine your LDAP server using the command line based *ldapsearch* tool.

Windows clients can use the free and easy to use Softerra LDAP browser for this: <http://www.ldapbrowser.com>

advproxy - Advanced Web Proxy

5.5.1 Common LDAP settings

| Common LDAP settings | | | |
|----------------------|----------------------|------------|---|
| Base DN: | <input type="text"/> | LDAP type: | Active Directory <input type="button" value="v"/> |
| LDAP Server: | <input type="text"/> | Port: | 389 |

Base DN

This is base where to start the LDAP search. All subsequent Organizational Units (OUs) will be included.

Refer to your LDAP documentation for the required format of the base DN.

Example Base DN for Active Directory:

```
cn=users,dc=ads,dc=local
```

This will search for users in the group *users* in the domain *ads.local*

Example Base DN for eDirectory:

```
ou=users,o=acme
```

This will search for users in the Organizational Unit *users* (and below) in the Organization *acme*

Note: If the Base DN contains spaces, you must “escape” these spaces using a backslash.

Example for a Base DN containing spaces:

```
cn=internet\ users,dc=ads,dc=local
```

LDAP type

You can select between different types of LDAP implementations:

- Active Directory (ADS)
- Novell eDirectory (NDS)
- LDAP v2 and v 3

LDAP Server

Enter the IP address of your LDAP Server.

Port

Enter the port your LDAP Server is listening to LDAP requests. The default is 389.

Note: The protocol LDAPS (Secure LDAP, port 636) is not supported by Advanced Proxy.

advproxy - Advanced Web Proxy

5.5.2 Bind DN settings

| | |
|--|--|
| Bind DN settings | |
| Bind DN username: <input type="text"/> | Bind DN password: <input type="text"/> |

Bind DN username

Enter the full distinguished name for a Bind DN user.

Note: A Bind DN user is required for Active Directory and eDirectory.

Note: The Bind DN user must be allowed to browse the directory and read all user attributes.

Note: If the Bind DN username contains spaces, you must "escape" these spaces using a backslash.

Bind DN password

Enter the password for the Bind DN user.

5.5.3 Group based access control

| | |
|--------------------------------------|--|
| Group based access control | |
| Required group: <input type="text"/> | |

Required group (optional)

Enter the full distinguished name of a group for authorized Internet users.

In addition to a correct authentication, a membership within this group will be required for web access.

Note: If the group name contains spaces, you must "escape" these spaces using a backslash.

advproxy - Advanced Web Proxy

5.6 Windows authentication

This authentication method uses an existing domain environment for user authentication.

Authentication method

None Local identd LDAP Windows RADIUS

Global authentication settings

Number of authentication processes: Authentication realm prompt:

Authentication cache TTL (in minutes): Destinations without authentication (one per line):

Limit of IP addresses per user:

User/IP cache TTL (in minutes):

Require authentication for unrestricted source addresses:

Common domain settings

Domain: PDC hostname: BDC hostname:

Authentication mode

Enable Windows integrated authentication:

User based access restrictions

Enabled:

Use positive access control: Use negative access control:

Authorized domain users (one per line) Unauthorized domain users (one per line)

In addition to the authentication you can define positive or negative user based access control lists.

advproxy - Advanced Web Proxy

5.6.1 Common domain settings

Common domain settings
Domain: PDC hostname: BDC hostname:

Domain

Enter the name of the domain you want to use for authentication. If you are running a Windows 2000 or Windows 2003 Active Directory, you'll have to enter the NetBIOS domain name.

PDC hostname

Enter the NetBIOS hostname of the Primary Domain Controller here. If you are running a Windows 2000 or Windows 2003 Active Directory, you can enter the name of any Domain Controller.

Note: For Windows 2000 and above the Primary Domain Controller is not assigned to a specific server. The Active Directory PDC emulator is a logical role and can be assigned to any server.

Important: The PDC hostname must be resolvable for the IPCop Server. This can be done by adding the hostname at "Services / Edit Hosts" (recommended) or by editing the file /etc/hosts directly.

BDC hostname (optional)

Enter the NetBIOS hostname of the Backup Domain Controller here. If you are running a Windows 2000 or Windows 2003 Active Directory, you can enter the name of any Domain Controller.

If the PDC doesn't respond to authentication requests, the authentication process will ask the BDC instead.

Important: The BDC hostname must be resolvable for the IPCop Server. This can be done by adding the hostname at "Services / Edit Hosts" (recommended) or by editing the file /etc/hosts directly.

5.6.2 Authentication mode

Authentication mode
Enable Windows integrated authentication:

Enable Windows integrated authentication

If enabled, the user will not be asked for username and password. The credentials of the currently logged in user will automatically be used for authentication. This option is enabled by default.

If integrated authentication is disabled, the user will be requested explicitly for username and password.

advproxy - Advanced Web Proxy

5.6.3 User based access restrictions

User based access restrictions
Enabled:
 Use positive access control: Authorized domain users (one per line)
 Use negative access control: Unauthorized domain users (one per line)

Enabled

Enables access control lists for authorized or unauthorized users.

Use positive access control / Authorized domain users

These listed users will be allowed for web access. For all other users, access will be denied.

Use negative access control / Unauthorized domain users

These listed users will be blocked for web access. For all other users, access will be allowed.

Note: If Windows integrated authentication is enabled, the username must be entered with the domain name as a prefix for the username, separated by a backslash.

Example for user based access control lists using integrated authentication:

Authentication mode
Enable Windows integrated authentication:
User based access restrictions
Enabled:
 Use positive access control: Authorized domain users (one per line)
 Use negative access control: Unauthorized domain users (one per line)
domain\administrator
domain\bruno
domain\jane
domain\maria
domain\paul
domain\steve

Note: When using integrated authentication, the user must be logged in to the domain, otherwise the name of the local workstation instead of the domain name will be added to the username.

advproxy - Advanced Web Proxy

Example for user based access control lists using explicit authentication:

The screenshot shows a configuration panel with the following sections:

- Authentication mode**
Enable Windows integrated authentication:
- User based access restrictions**
Enabled:
 - Use positive access control:
Authorized domain users (one per line)
`administrator`
`bruno`
`jane`
`maria`
`paul`
`steve`
 - Use negative access control:
Unauthorized domain users (one per line)

Note: Explicit authentication grants access to the user, even though the user is not logged in to the domain, as long as the username will be the same and the local workstation password and the domain password does match.

advproxy - Advanced Web Proxy

5.7 RADIUS authentication

This authentication method uses an existing RADIUS server for user authentication.

Authentication method

None Local identd LDAP Windows RADIUS

Global authentication settings

| | | | |
|---|-------------------------------------|---|----------------------|
| Number of authentication processes: | <input type="text" value="5"/> | Authentication realm prompt: ● | <input type="text"/> |
| Authentication cache TTL (in minutes): | <input type="text" value="60"/> | Destinations without authentication (one per line): ● | <input type="text"/> |
| Limit of IP addresses per user: ● | <input type="text"/> | | |
| User/IP cache TTL (in minutes): | <input type="text" value="0"/> | | |
| Require authentication for unrestricted source addresses: | <input checked="" type="checkbox"/> | | |

Common RADIUS settings

| | | | |
|----------------|----------------------|----------------|-----------------------------------|
| RADIUS Server: | <input type="text"/> | Port: | <input type="text" value="1812"/> |
| Identifier: ● | <input type="text"/> | Shared secret: | <input type="text"/> |

User based access restrictions

Enabled:

Use positive access control:
Authorized users (one per line)

Use negative access control:
Unauthorized users (one per line)

In addition to the authentication you can define positive or negative user based access control lists.

advproxy - Advanced Web Proxy

5.7.1 Common RADIUS settings

| | | | |
|--|----------------------|----------------|-----------------------------------|
| Common RADIUS settings | | | |
| RADIUS Server: | <input type="text"/> | Port: | <input type="text" value="1812"/> |
| Identifier: <input checked="" type="radio"/> | <input type="text"/> | Shared secret: | <input type="text"/> |

RADIUS Server

Enter the IP address of the RADIUS Server you want to use for authentication.

Port

Enter the port that will be used to communicate with the RADIUS Server. The default is port 1812, some RADIUS servers may use the deprecated port 1645 instead.

Identifier

This is an optional field and can be used to identify your IPCop for the RADIUS Server. If this is left empty, the IP address of your IPCop will be used for identification.

Shared secret

This is the shared secret for the authentication of your IPCop against the RADIUS Server. This must be the same password that you have entered at your RADIUS Server.

5.7.2 User based access restrictions

| | |
|---|--|
| User based access restrictions | |
| Enabled: <input type="checkbox"/> | |
| <input checked="" type="radio"/> Use positive access control: | <input type="radio"/> Use negative access control: |
| Authorized users (one per line) | Unauthorized users (one per line) |
| <input type="text"/> | <input type="text"/> |

Enabled

Enables access control lists for authorized or unauthorized users.

Use positive access control / Authorized users

These listed users will be allowed for web access. For all other users, access will be denied.

Use negative access control / Unauthorized users

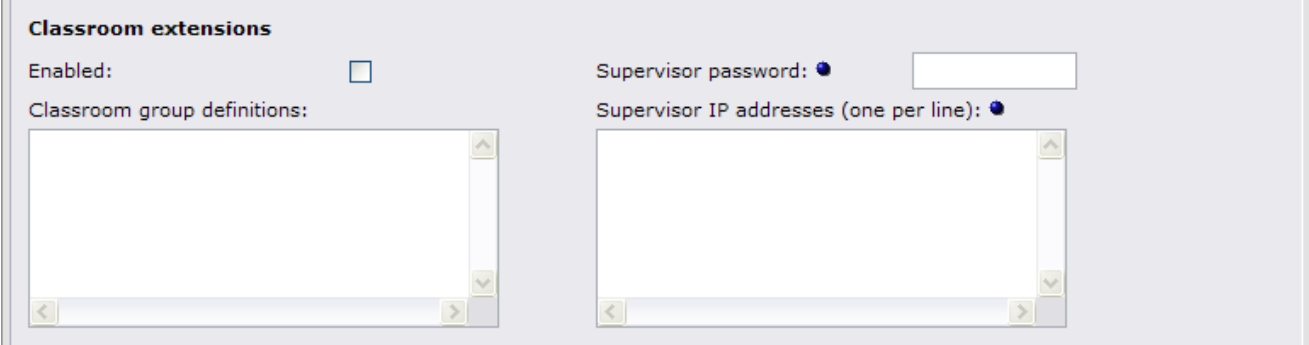
These listed users will be blocked for web access. For all other users, access will be allowed.

advproxy - Advanced Web Proxy

6 Classroom Extensions configuration (CRE)

6.1.1 Classroom extensions section overview

The classroom extensions section will appear in the Advanced Proxy GUI after the CRE supplement has been installed (see chapter 3.3). These are the administrative parameters related to the classroom extensions.



6.1.2 Enabled

This enables the Supervisor management interface for the classroom extensions.

Note: After disabling the CRE and restarting the Proxy Server, all groups will be allowed for web access.

6.1.3 Supervisor password

When setting this password, all Supervisor users must have to enter this password for managing web access. This is an optional configuration item.

Note: For security reasons, either a Supervisor password or Supervisor IP addresses should be defined.

6.1.4 Classroom group definitions

Define your classroom group definitions here. See chapter 6.3 for more details about this.

6.1.5 Supervisor IP addresses

This allows you to define certain IP addresses that will be able to manage web access. This is an optional configuration item.

This can be used to increase security or to simplify management if you don't want to configure a Supervisor password.

Note: All machines not listed here will get the management interface in view-only mode.

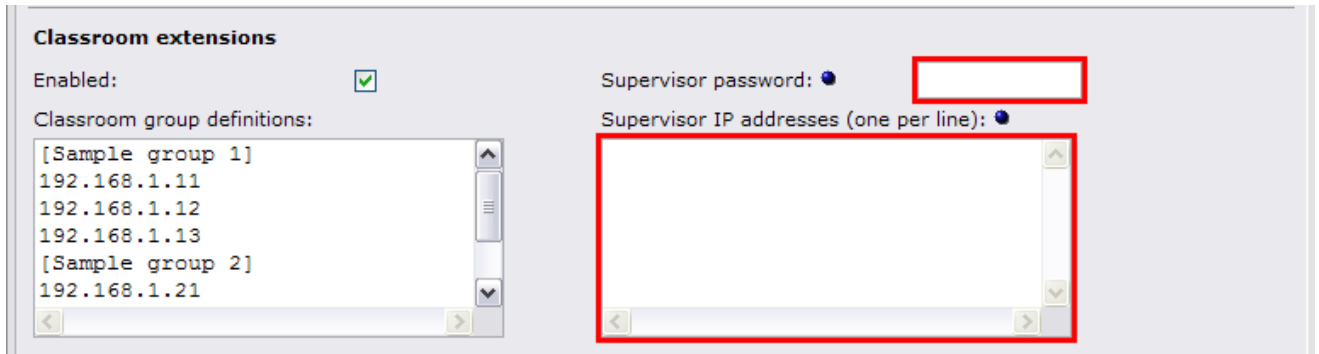
advproxy - Advanced Web Proxy

6.2 CRE security levels

6.2.1 Level 1: No password, no IP address restrictions - no security

All clients will be able to manage web access without any restriction. This is not recommended for production environments.

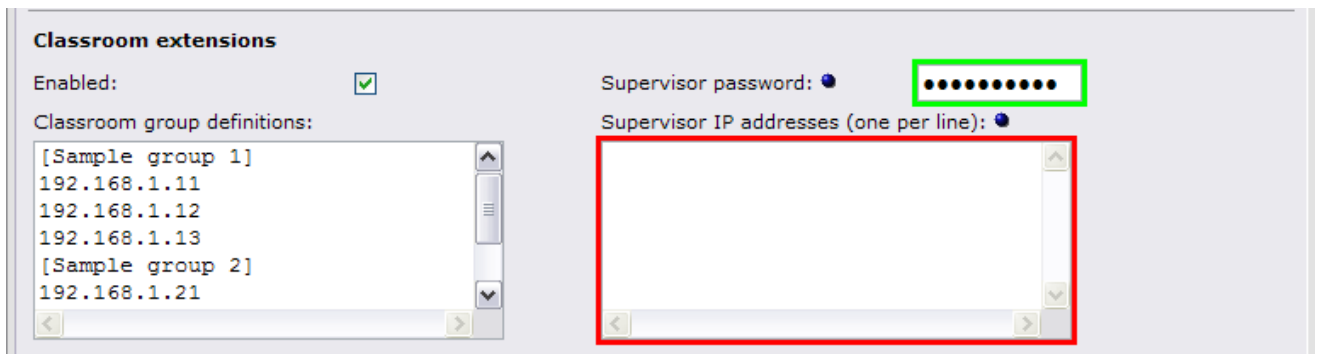
Note: Use this for debugging or testing purposes only!



6.2.2 Level 2: Password set, no IP address restrictions - lower security

All clients will be able to manage web access, but a password will be required to save the changes.

This security level is recommended in an environment without special Supervisor computers.

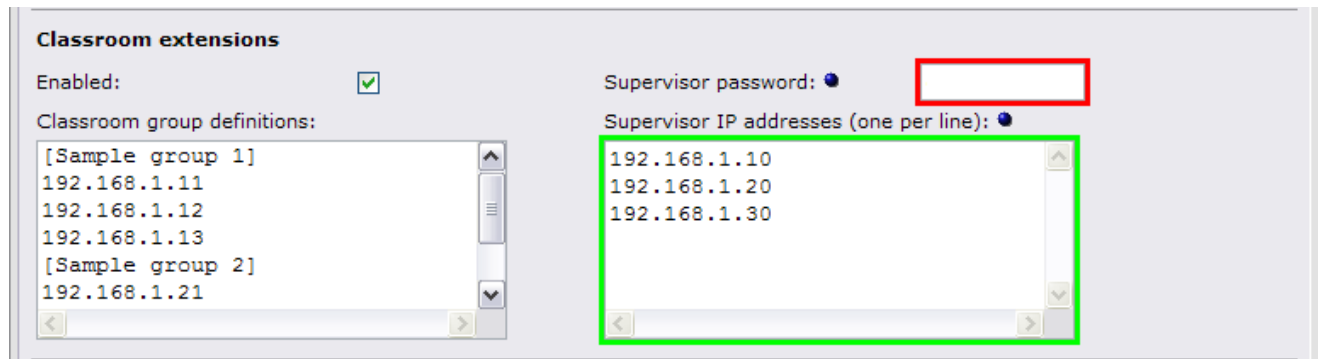


advproxy - Advanced Web Proxy

6.2.3 Level 3: No Password, IP restrictions applied - lower security

All clients listed here will be able to change the web access settings. The clients will be identified by their IP address, a password is not required to save the changes.

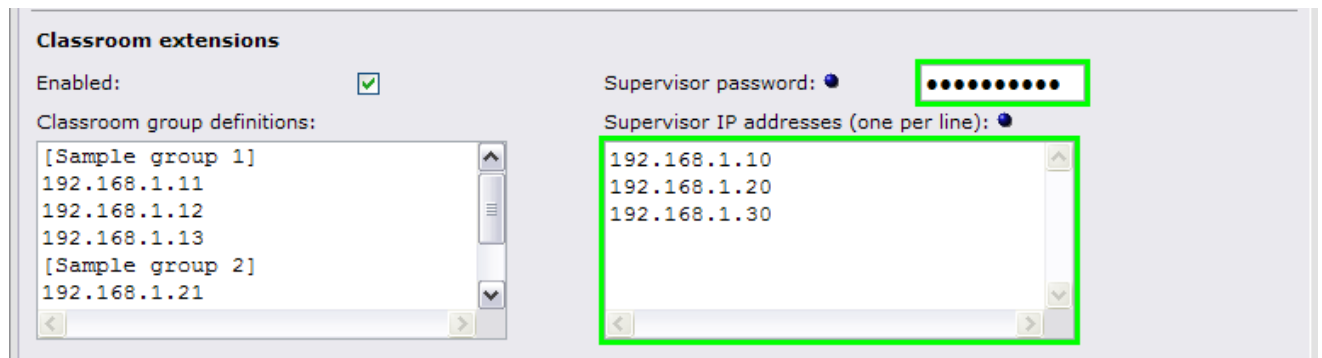
Note: If the client IP address is not listed here, the web access management interface will appear in a view-only mode.



6.2.4 Level 4: Password set, IP restrictions applied - higher security

This is the highest security level for the web access management interface. Only the listed clients can change the settings, a password will be required to save the changes.

Note: If the client IP address is not listed here, the web access management interface will appear in a view-only mode.



advproxy - Advanced Web Proxy

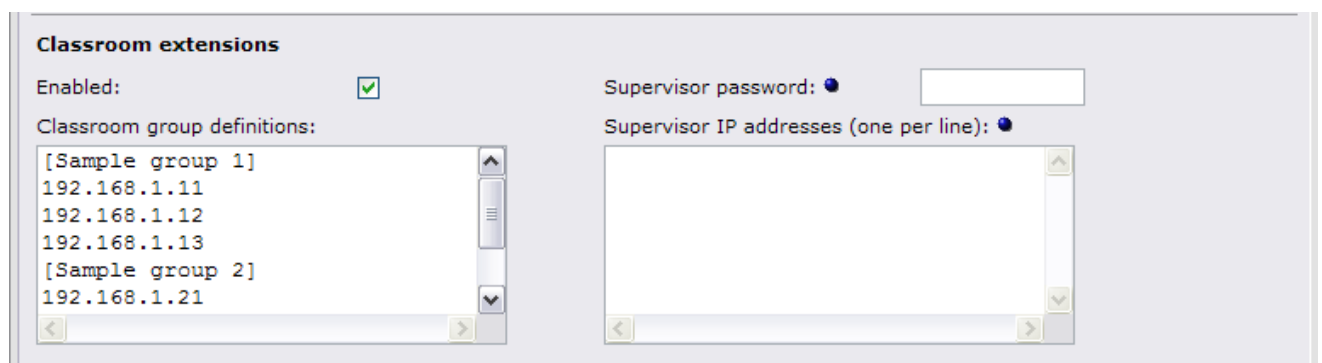
6.3 Classroom group definitions

6.3.1 Creating group definitions

A classroom group definition looks like this:

```
[groupname]
client MAC address or client IP address or IP range or IP subnet
client MAC address or client IP address or IP range or IP subnet
client MAC address or client IP address or IP range or IP subnet
```

Example:



Note: Access will be granted for new groups by default.

6.3.2 Group labels and group names

Each group has a name. This name will be taken from the group definition label. A group name must be unique.

Group label

A label is a group name included in square brackets. All clients listed below this label belong to this group.

Group name

A group name is the name that will be shown in the web access management interface. The group name is the part of a label between the square brackets.

Note: A group name may contain square brackets, but must be included in a pair of additional square brackets for the group label.

The classroom group definitions may have an unlimited number of group labels.

advproxy - Advanced Web Proxy

6.3.3 Client definitions

Each group can have an unlimited number of client definitions. You can use mixed client definitions within a group, but each definition must be in a single line.

Examples:

Single host (MAC address)

00:00:12:AB:34:CD

Single host (IP address)

192.168.1.11

Host range

192.168.1.11-192.168.1.19

Subnet (netmask notation)

192.168.1.32/255.255.255.240

Subnet (CIDR notation)

192.168.1.32/28

advproxy - Advanced Web Proxy

6.4 Custom error messages

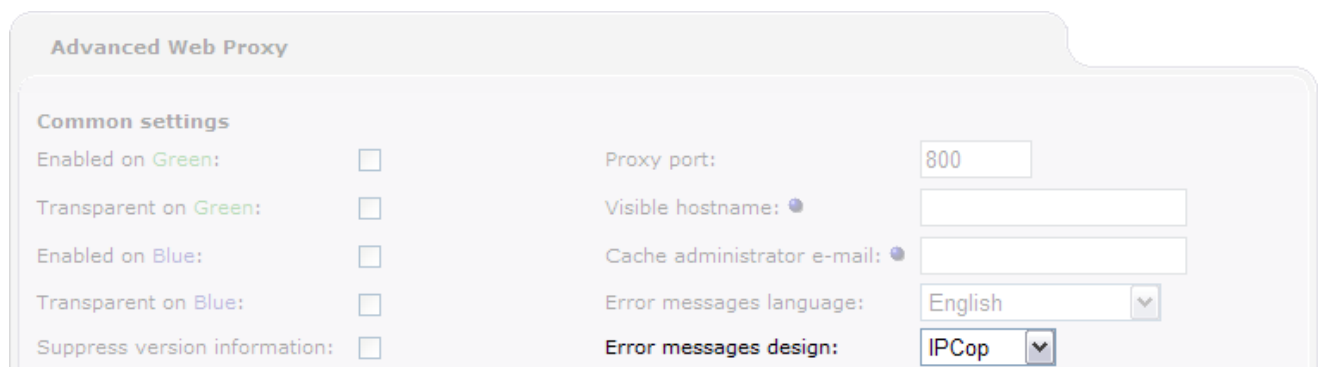
If a client will be blocked by the CRE restrictions, the default "Access denied" message will appear:



Creating custom error messages

You can use the HTML file named `ERR_ACCESS_DISABLED` that will be shown instead.

Depending on the selected error messages design, the destination path may vary:



For the IPCop design add this file to the directory

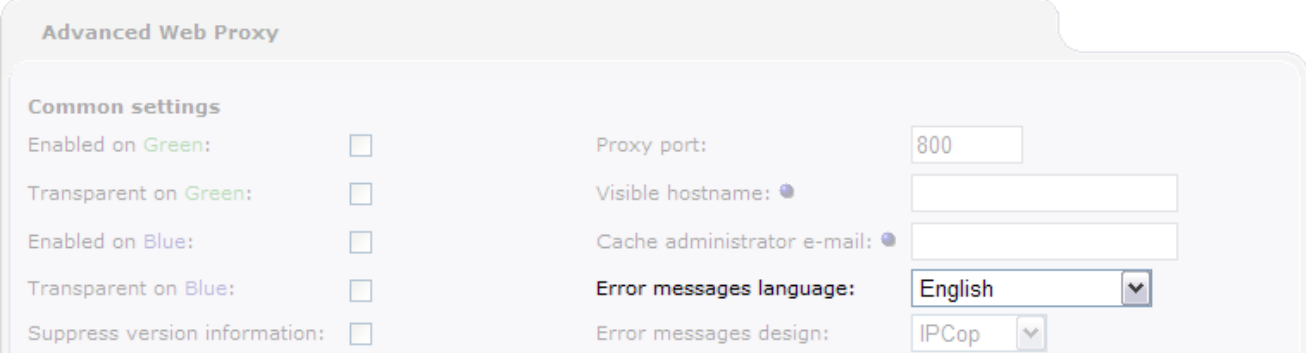
```
/usr/lib/squid/advproxy/errors.ipcop/language/
```

or for the standard design to the directory

```
/usr/lib/squid/advproxy/errors/language/
```

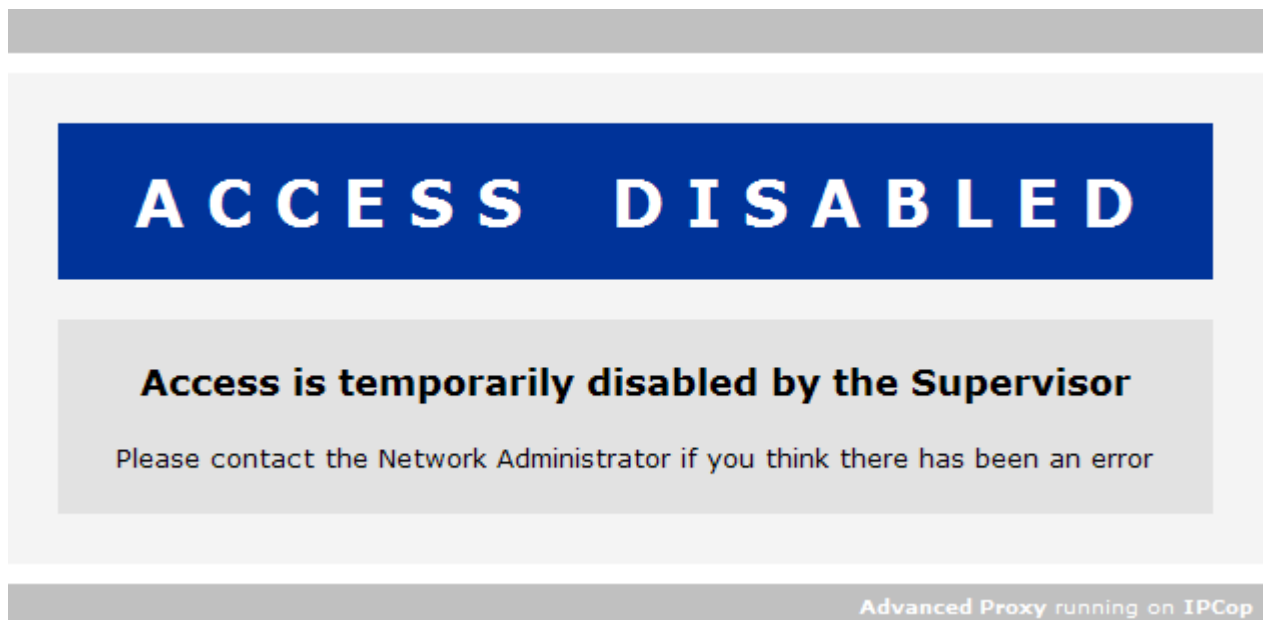
advproxy - Advanced Web Proxy

Note: Replace *language* with the language you have selected at the Advanced Proxy GUI:



The screenshot shows the 'Advanced Web Proxy' configuration interface. Under the 'Common settings' section, there are two columns of options. The left column contains four checkboxes: 'Enabled on Green', 'Transparent on Green', 'Enabled on Blue', and 'Transparent on Blue', all of which are currently unchecked. Below these is another checkbox for 'Suppress version information', also unchecked. The right column contains four input fields: 'Proxy port' with the value '800', 'Visible hostname' with an empty field, 'Cache administrator e-mail' with an empty field, 'Error messages language' with a dropdown menu set to 'English', and 'Error messages design' with a dropdown menu set to 'IPCop'.

Example: `/usr/lib/squid/advproxy/errors.ipcop/English/ERR_ACCESS_DISABLED`



Note: This file is already included in the Advanced Proxy installation archive but not installed by default.

advproxy - Advanced Web Proxy

7 Web Access Management with CRE

7.1 Starting the Web Access Management Interface

The Web Access Management Interface can be started from every client computer:

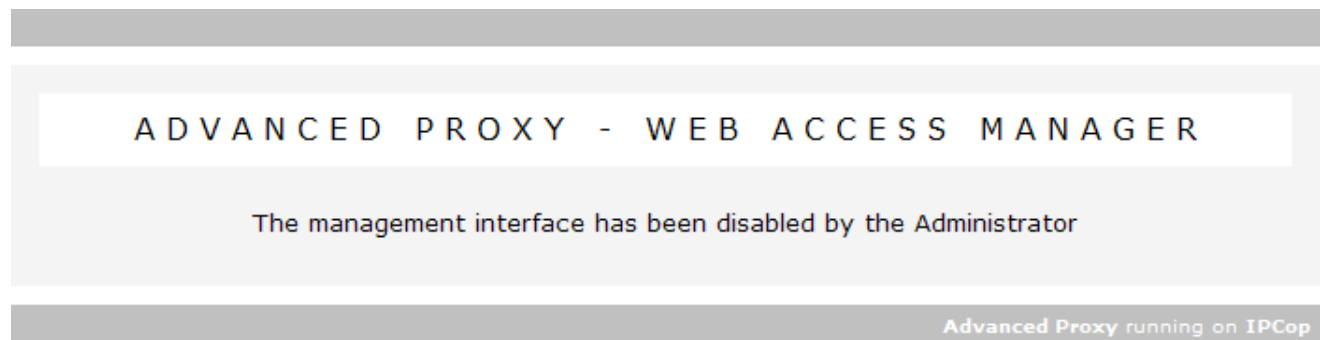
Open a web browser and enter the URL

<https://192.168.1.1:445/cgi-bin/webaccess.cgi>

(Replace the address 192.168.1.1 with the IP address of your IPCop)

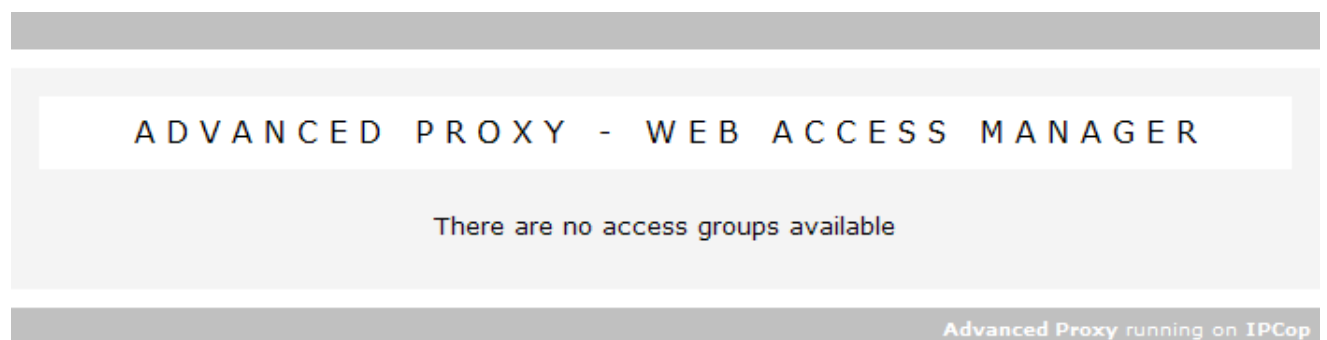
7.1.1 "The management interface has been disabled"

If the Web Access Management Interface has not been yet enabled by the Admin, you'll see this text:



7.1.2 "There are no access groups available"

If the Web Access Management Interface has been enabled, but the Admin didn't define any group, you'll see this text:



advproxy - Advanced Web Proxy

7.2 Managing access groups

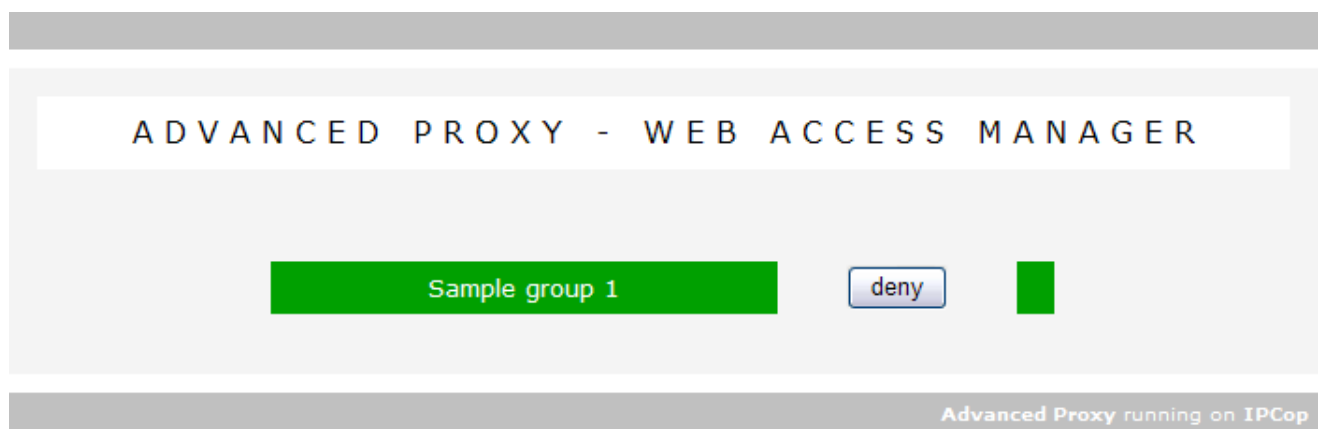
The Supervisor will be able to turn web access on or off for the predefined groups. Web access is enabled for each group by default.

The access can be controlled by clicking the button belonging to the target group.

By default, there are no restrictions and the access can be managed from all clients.

7.2.1 Enabled groups

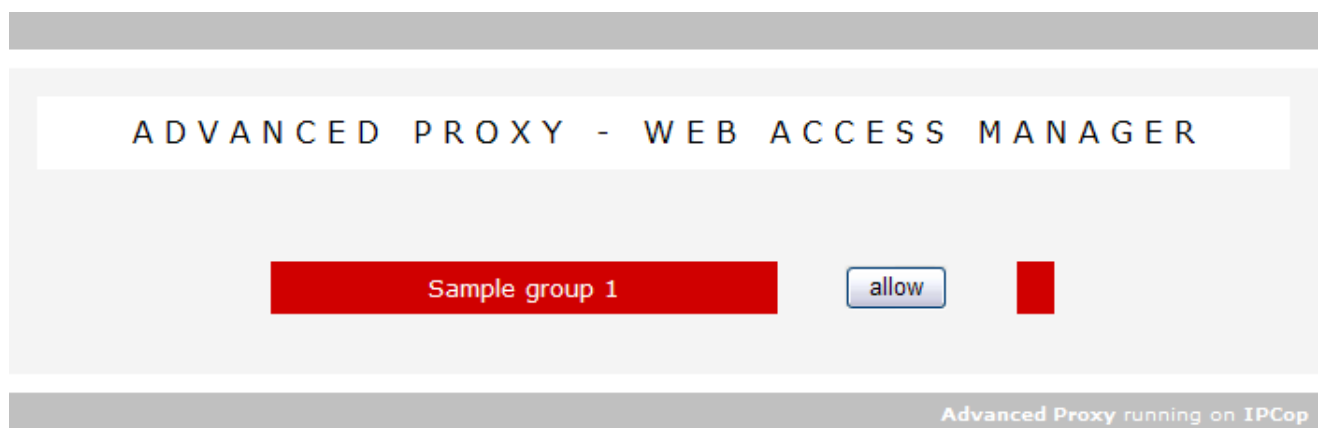
Enabled groups will be marked as green and the toggle button will be shown as "deny":



Note: New groups are enabled and marked as green by default.

7.2.2 Disabled groups

Disabled groups will be marked as red and the toggle button will be shown as "allow":



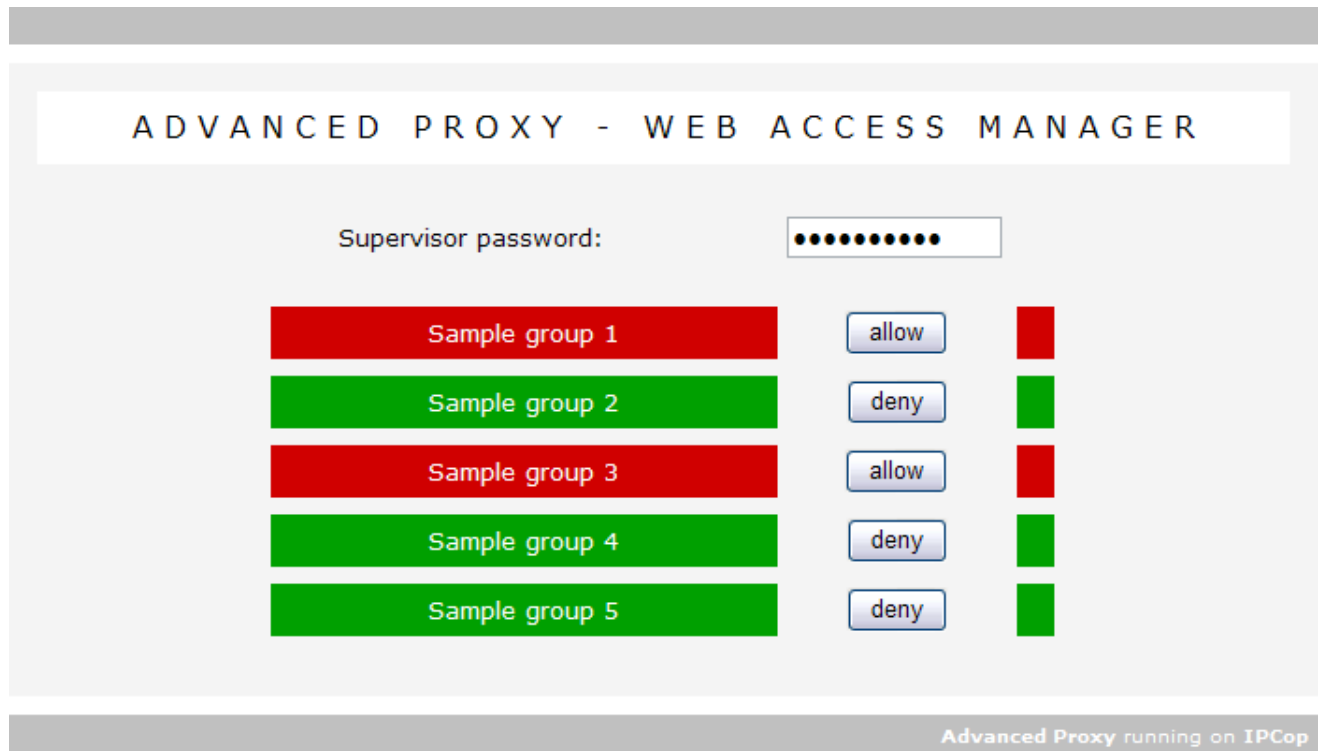
advproxy - Advanced Web Proxy

7.3 Restricting management access

The access to the management interface can - and should - be restricted.

7.3.1 Restricting access by password

If the Admin has set a password at the Advanced Proxy GUI, all clients must enter this password before they can change access for certain groups.



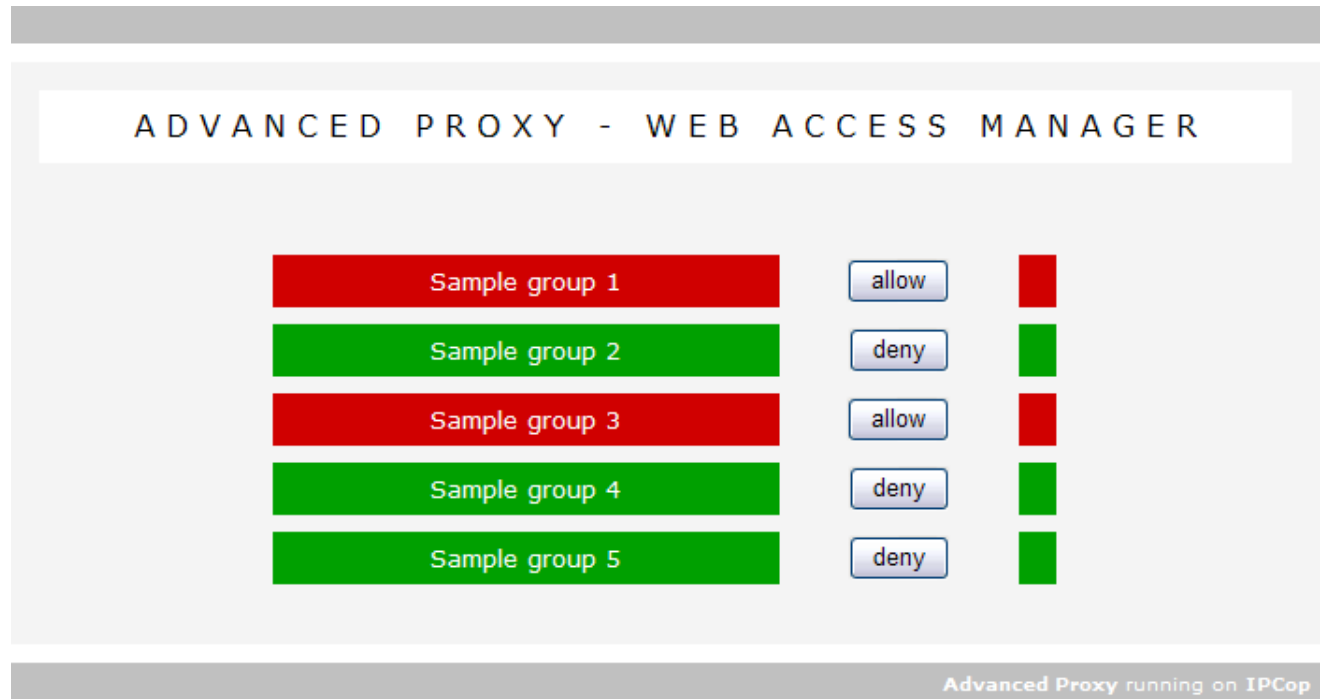
Note: The password must be entered again for each transaction.

advproxy - Advanced Web Proxy

7.3.2 Restricting access by IP address

7.3.2.1 Management mode

If the management interface is opened by a client with a listed Supervisor IP address (see chapter 6.1.5), the interface appears in the management mode:

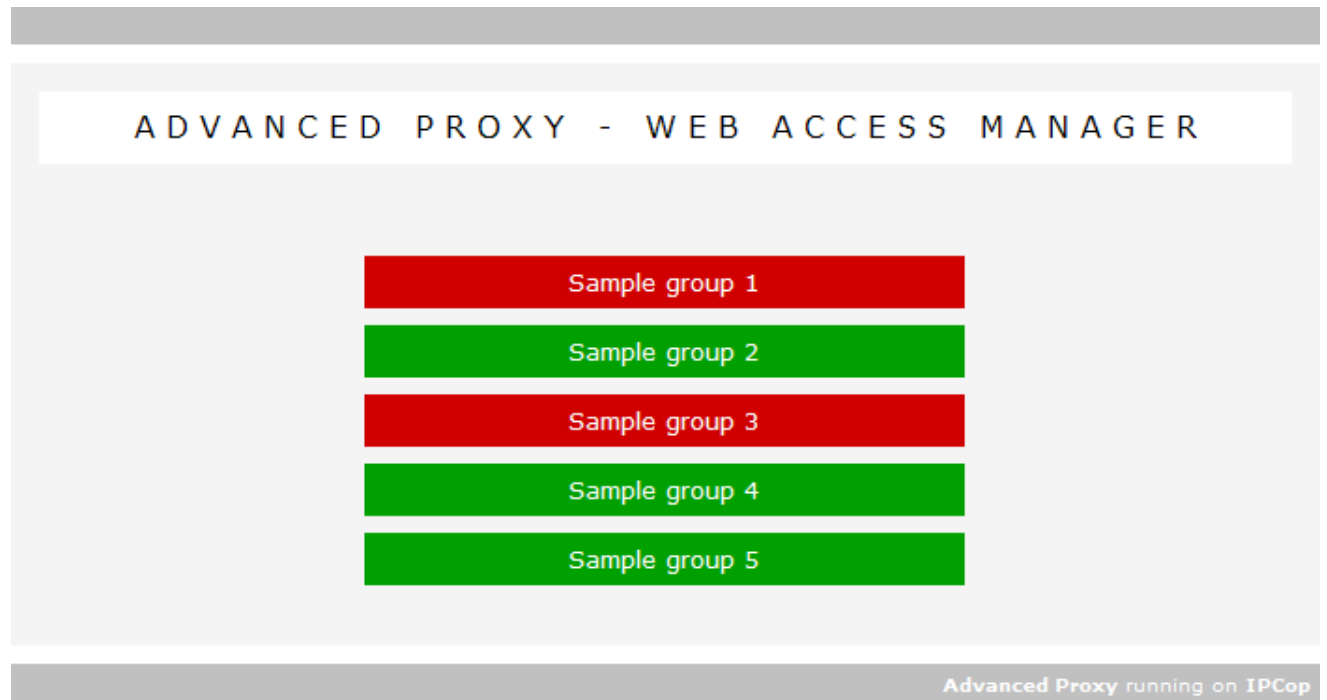


If the Admin has set a password at the Advanced Proxy GUI, the management will be the same as described in chapter 7.3.1.

advproxy - Advanced Web Proxy

7.3.2.2 View-only mode

If the management interface is opened by a client with an unlisted Supervisor IP address (see chapter 6.1.5), the interface appears in the view-only mode:



advproxy - Advanced Web Proxy

8 Enforcing proxy usage

For different reasons, it may be required that all clients should be enforced to use the proxy service. The reasons could be mandatory logging, filtering or authentication.

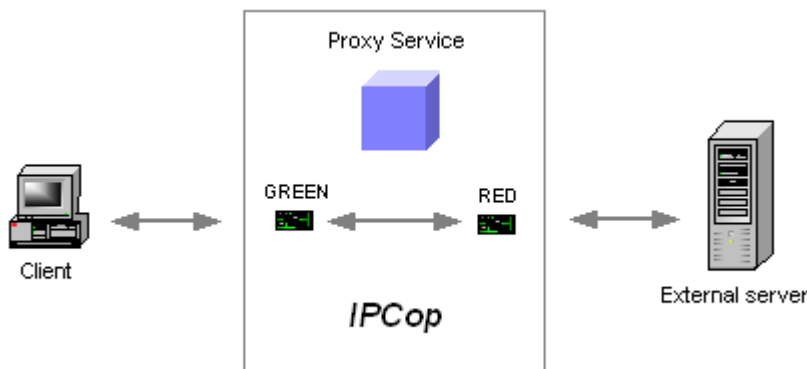
8.1 Web Proxy standard operation modes

8.1.1 Proxy service disabled

IPCop proxy settings:

| | |
|--|---|
| Enabled on Green: <input type="checkbox"/> | Enabled on Green: <input type="checkbox"/> |
| Transparent on Green: <input type="checkbox"/> | Transparent on Green: <input checked="" type="checkbox"/> |

Client access: Disabling the proxy service gives direct access for all clients.



Result: The proxy service will never be used. Logging, filtering and authentication will not be available.

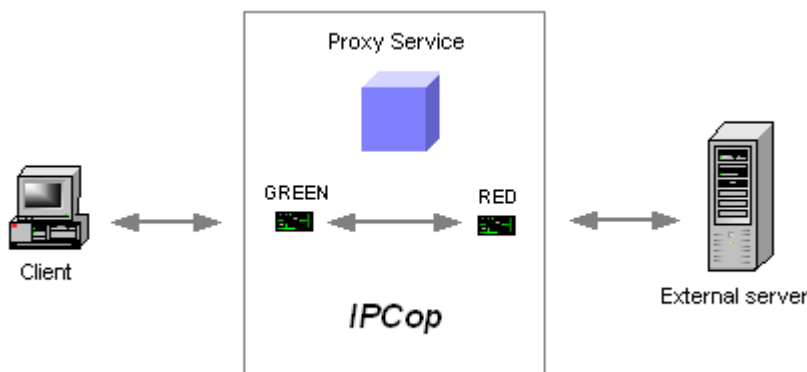
advproxy - Advanced Web Proxy

8.1.2 Proxy service enabled, running in non-transparent mode

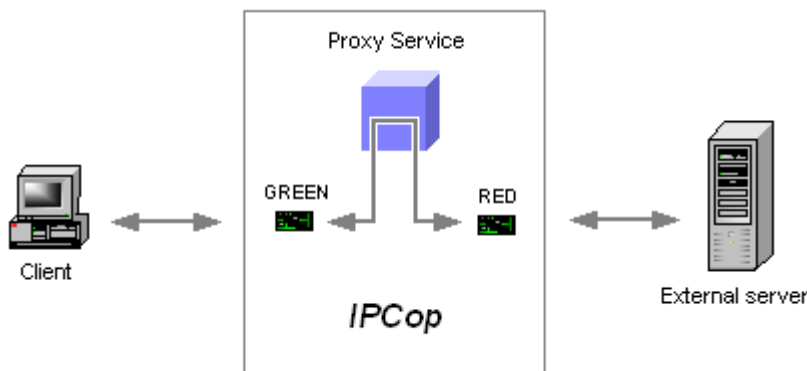
IPCop proxy settings:

| | |
|-----------------------|-------------------------------------|
| Enabled on Green: | <input checked="" type="checkbox"/> |
| Transparent on Green: | <input type="checkbox"/> |

Client access: All clients without explicit proxy configuration will bypass the proxy service.



Client access: All clients configured for proxy usage will use the proxy for all destination ports (80, 443, 8080, etc.) and even for browser based FTP access.



Result: It depends on the client configuration whether the proxy service will be used or not. Unconfigured clients will bypass logging, filtering and authentication.

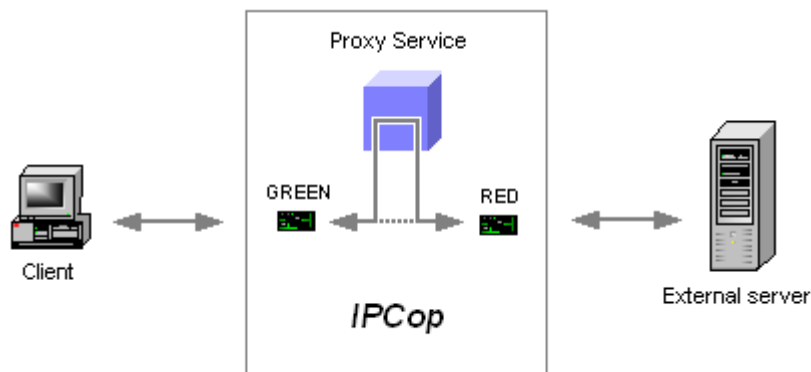
advproxy - Advanced Web Proxy

8.1.3 Proxy service enabled, running in transparent mode

IPCop proxy settings:

| | |
|-----------------------|-------------------------------------|
| Enabled on Green: | <input checked="" type="checkbox"/> |
| Transparent on Green: | <input checked="" type="checkbox"/> |

Client access: All requests with destination port 80 will be internally redirected to the proxy service. Requests with other destination ports (e.g. 443 for https) will bypass the proxy service.



Result: Not all but most requests will pass the proxy service. Therefore filtering, logging and authentication will not be reliable.

advproxy - Advanced Web Proxy

8.2 Client side Web Proxy configuration

There are different ways to configure the clients to use the Web Proxy service. Here are some examples:

8.2.1 Manual client configuration

Configuring clients by applying all proxy settings manually:

- Time-consuming and unreliable
- Configuration required per user

8.2.2 Client pre-configuration

Distributing pre-configured browser clients:

- Only reasonable for medium to large environments
- Works only for the configured client software

IEAK for IE 7: <http://www.microsoft.com/windows/ieak/>

CCK for Mozilla: <http://www.mozilla.org/projects/cck/>

8.2.3 Client configuration via DNS / DHCP

Centralized client configuration using DNS and/or DHCP:

- Complex implementation
- Require custom proxy.pac or wpad.dat files
- Flexible configuration
- Most browsers support this configuration method

More info: <http://www.web-cache.com/Writings/Internet-Drafts/draft-ietf-wrec-wpad-01.txt>

8.2.4 Client configuration using group policies

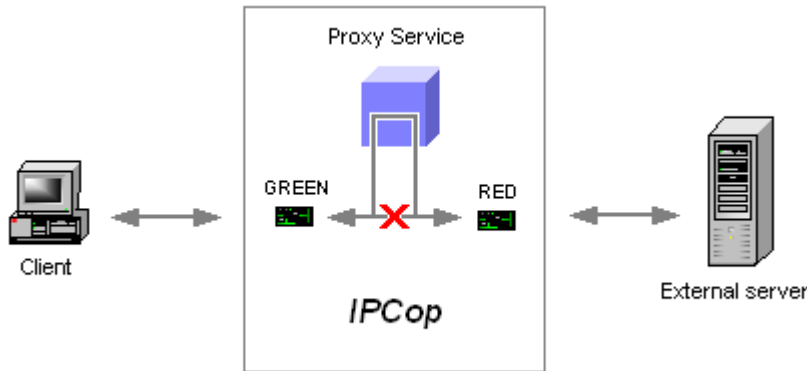
Centralized client configuration using group policies:

- Complex implementation
- Only reasonable for medium to large environments
- Requires a centralized network management system (Active Directory, ZENworks, etc.)
- Flexible and mandatory configuration
- Works only for Win32 clients and certain browser types

advproxy - Advanced Web Proxy

8.3 Modifying the firewall rules

All possible proxy operation modes allow further direct web access for unconfigured clients. Therefore, the firewall may not forward any request for those ports usually used for web access:



Note: This will be the only way to prevent bypassing the proxy service for unauthorized access.

8.3.1 Adding custom rules to iptables

Custom rules can be applied by adding them to the file `/etc/rc.d/rc.firewall.local`

The following example drops all direct access from inside to the destination ports 80 and 443 outside.

```
#!/bin/sh
# Used for private firewall rules

# See how we were called.
case "$1" in
  start)
    ## add your 'start' rules here
    /sbin/iptables -A CUSTOMFORWARD -i eth0 -o ppp0 -p tcp -m mport --dports 80,443 -j DROP
    ;;
  stop)
    ## add your 'stop' rules here
    /sbin/iptables -D CUSTOMFORWARD -i eth0 -o ppp0 -p tcp -m mport --dports 80,443 -j DROP
    ;;
  reload)
    $0 stop
    $0 start
    ## add your 'reload' rules here
    ;;
  *)
    echo "Usage: $0 {start|stop|reload}"
    ;;
esac
```

Note: Replace `ppp0` with the name of your RED interface if `ppp0` is not your RED interface.

Note: Replace `eth0` with the name of your GREEN interface if `eth0` is not your GREEN interface.

Note: You can add more lines for additional interfaces (e.g. `eth1` for a wireless network)

Note: The rules must be reloaded after this modification: `/etc/rc.d/rc.firewall.local reload`

Note: The recommended ports to be blocked for web access are: 80,81,443,3128,6588,8000,8080,8181

advproxy - Advanced Web Proxy

Note: Adding port 21 (FTP) forces web browser based FTP clients to pass the proxy but prevents most native FTP clients from establishing connections with external FTP hosts.

advproxy - Advanced Web Proxy

8.4 Requirements for mandatory proxy usage

To enforce proxy usage, these requirements must be met:

Proper client configuration

The client must be configured to use the proxy service. See chapter 8.2

Correct proxy operation mode

The proxy must operate in non-transparent mode. See chapter 8.1.2

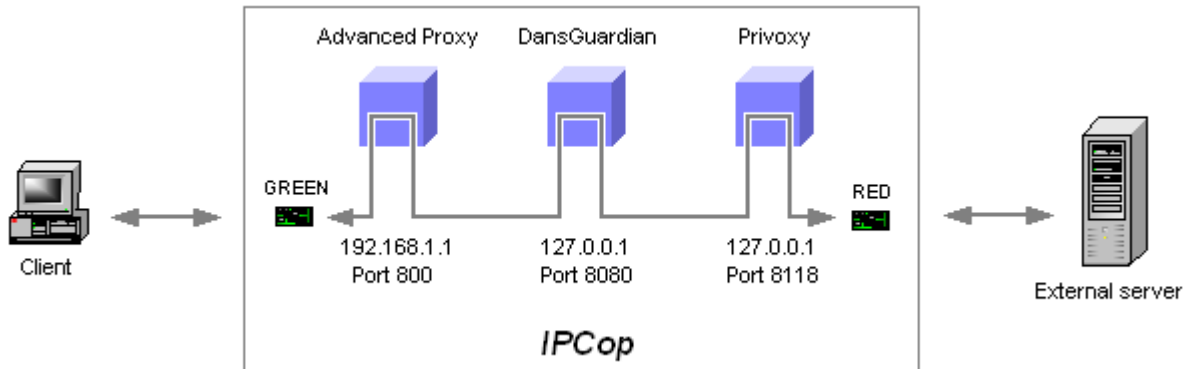
Blocking of direct web access

All direct web access needs to be blocked. See chapter 8.3

advproxy - Advanced Web Proxy

8.5 Authentication and additional content filters

If you are running content filters like DansGuardian and/or Privoxy with authentication enabled, Advanced Proxy must be the first proxy in this chain:



Advanced Proxy settings:

| Upstream proxy | | | |
|-------------------------------|-------------------------------------|-----------------------------|---|
| Proxy address forwarding: | <input type="checkbox"/> | Upstream proxy (host:port): | <input type="text" value="127.0.0.1:8080"/> |
| Client IP address forwarding: | <input checked="" type="checkbox"/> | Upstream username: | <input type="text"/> |
| Username forwarding: | <input checked="" type="checkbox"/> | Upstream password: | <input type="text"/> |

These settings enables client IP address and username forwarding from Advanced Proxy to DansGuardian.

DansGuardian settings:

Required settings for dansguardian.conf

```
# the IP that DansGuardian listens on.
filterip = 127.0.0.1

# the port that DansGuardian listens to.
filterport = 8080

# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1

# the port DansGuardian connects to proxy on
proxyport = 8118

# if on it uses the X-Forwarded-For: <clientip> to determine the client
# IP. This is for when you have squid between the clients and DansGuardian.
usexforwardedfor = on
```

advproxy - Advanced Web Proxy

Privoxy settings:

Required settings for config

```
# 4.1. listen-address
# =====
#
listen-address 127.0.0.1:8118

# 5.1. forward
# =====
#
forward          /          .
```

Note: The syntax for forwarding is *forward <slash> <dot>* to forward all requests to it's external destination.

Recommended settings for default.action

```
#####
# Defaults
#####
{ \
..
+hide-forwarded-for-headers \
..
}
/ # Match all URLs
```

advproxy - Advanced Web Proxy

9 Active Directory and LDAP authentication

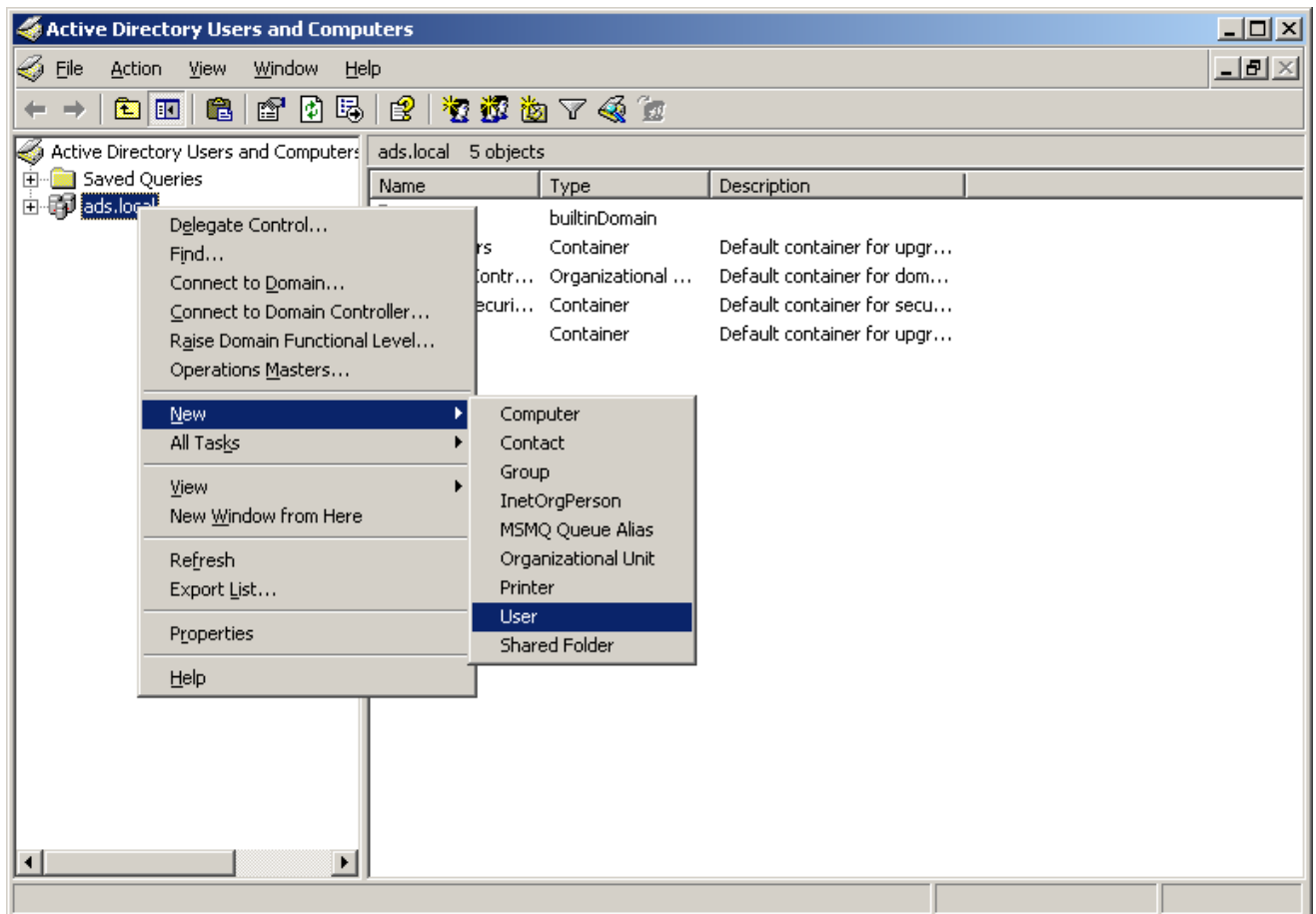
The following guidance is a step-by-step instruction for configuring the authentication using Microsoft Active Directory Services via LDAP for Advanced Proxy running on IPCop.

9.1.1 Configuring LDAP authentication using Microsoft Active Directory Services

Step 1: Create the Bind DN user account

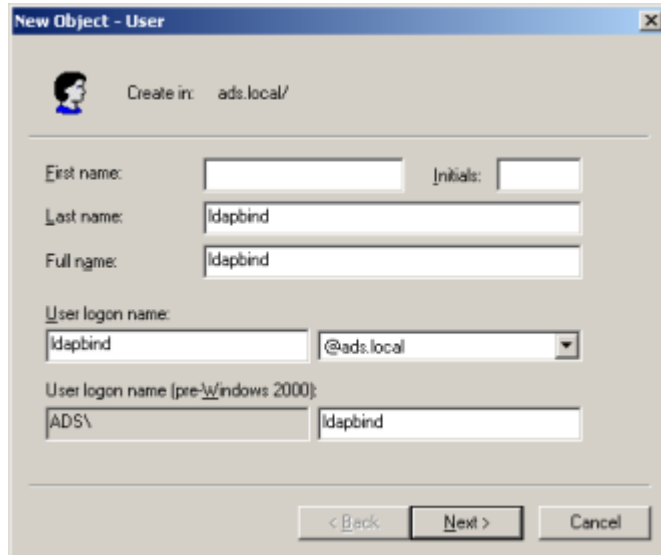
Open the MMC snap-in *Active Directory Users and Computers*.

Right click on the domain and select *New > User* from the menu.



advproxy - Advanced Web Proxy

Enter the name for the Bind DN user. Make sure that the username does not contain spaces or special characters.



New Object - User

Create in: ads.local/

First name: Initials:

Last name:

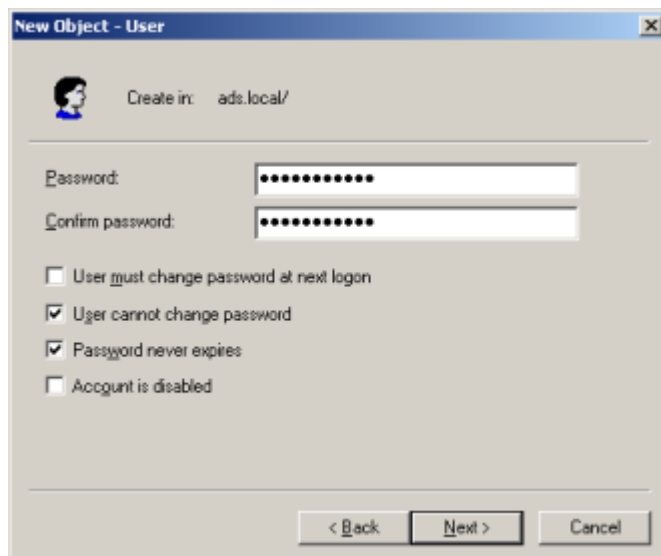
Full name:

User logon name: @ads.local

User logon name (pre-Windows 2000):

< Back Next > Cancel

Enter the password for the Bind DN user and select the options *User cannot change password* and *Password never expires*. Make sure that the option *User must change password at next logon* is unchecked.



New Object - User

Create in: ads.local/

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

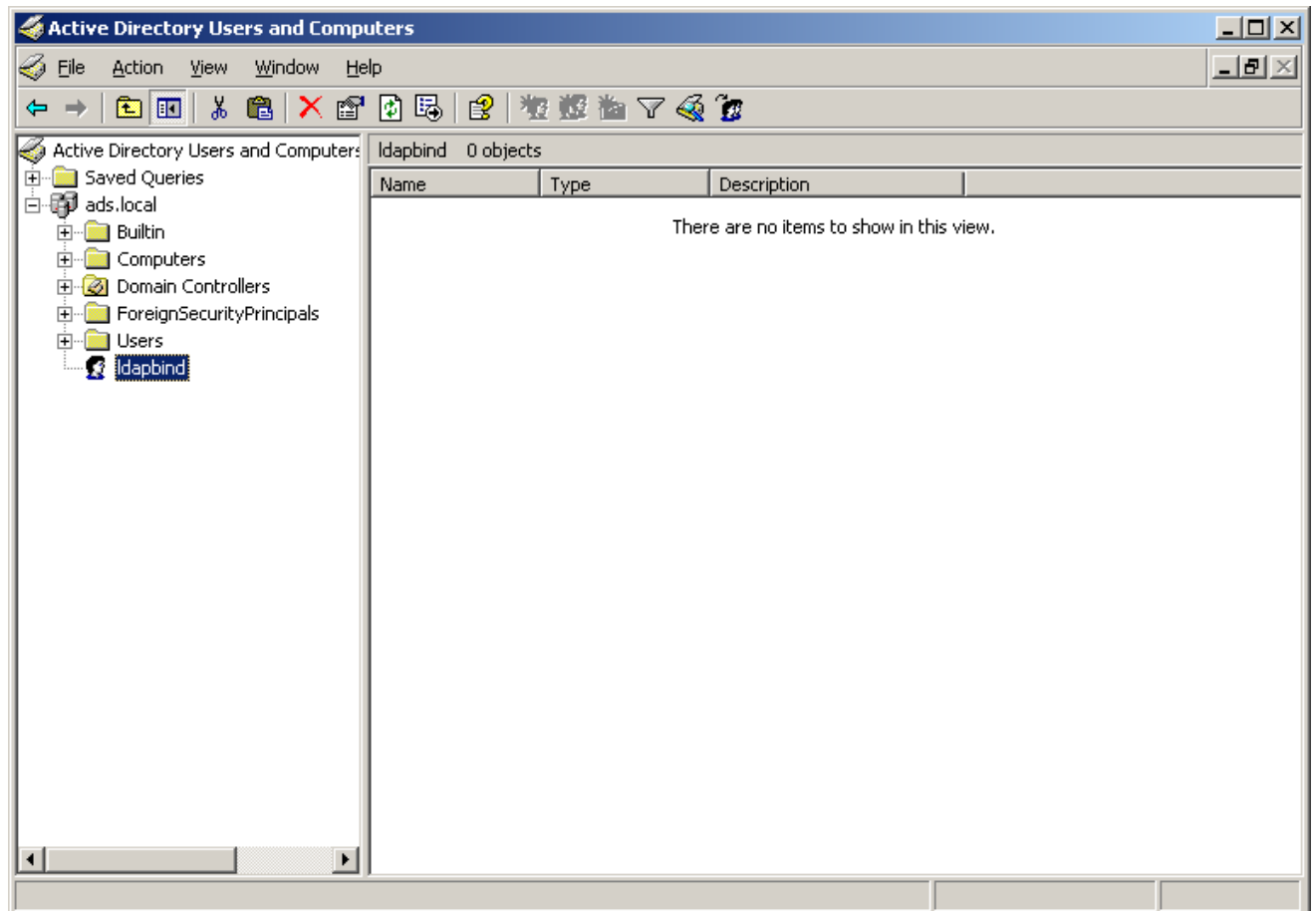
advproxy - Advanced Web Proxy

Complete the Wizard to create the Bind DN user. The Active Directory username will be

ldapbind@ads.local

and the LDAP DN will be

cn=ldapbind,dc=ads,dc=local

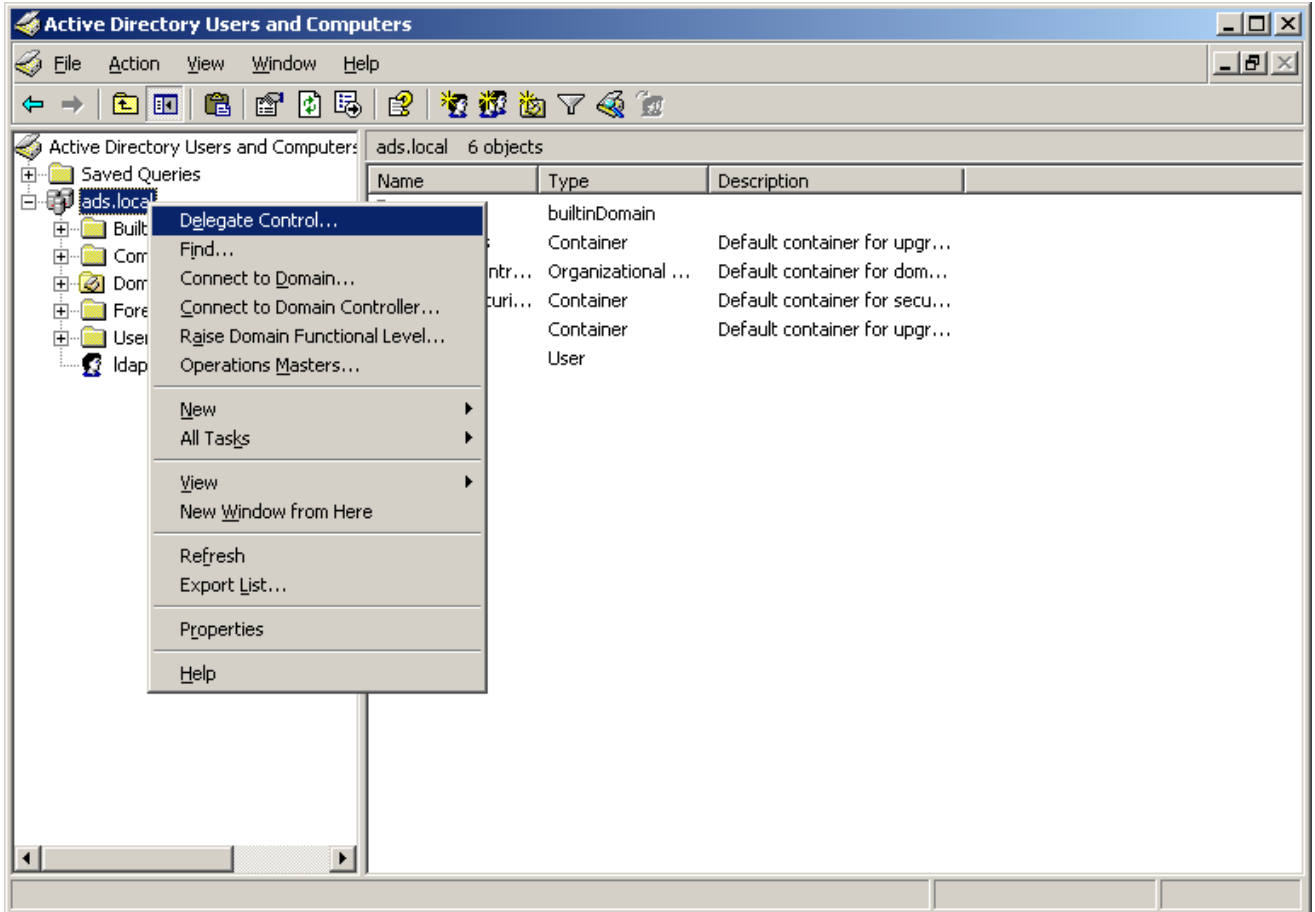


This account will be used to bind the Advanced Proxy to the LDAP server. This is necessary because Active Directory doesn't allow anonymous browsing.

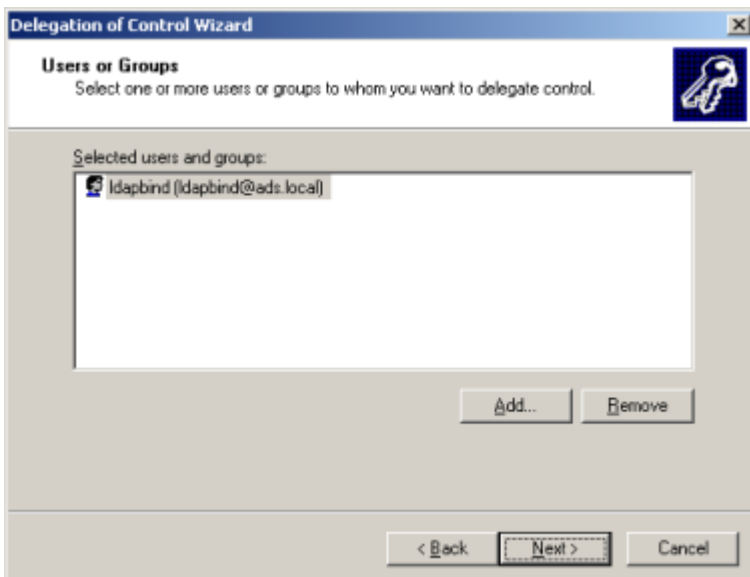
advproxy - Advanced Web Proxy

Step 2: Grant appropriate access rights to the Bind DN user

Right click the domain and select *Delegate Control* from the menu.

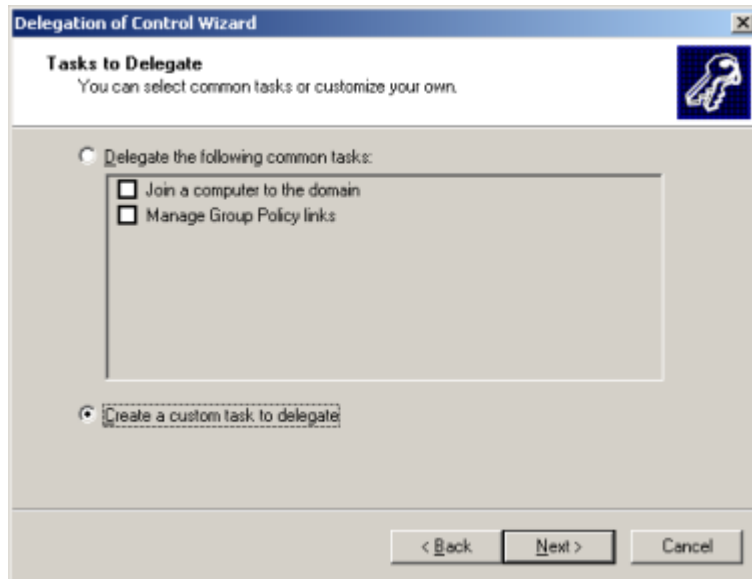


Start the Control Delegation Wizard and select the Idapbind user account.

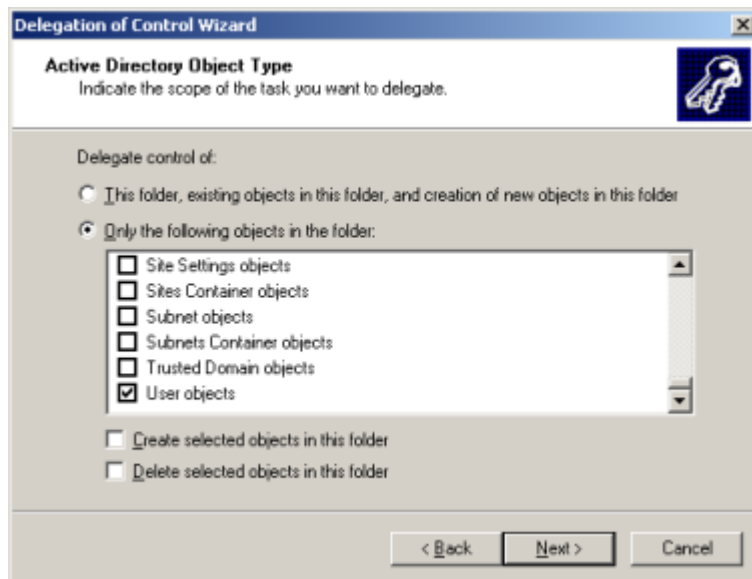


advproxy - Advanced Web Proxy

Select *Create a custom task to delegate*.

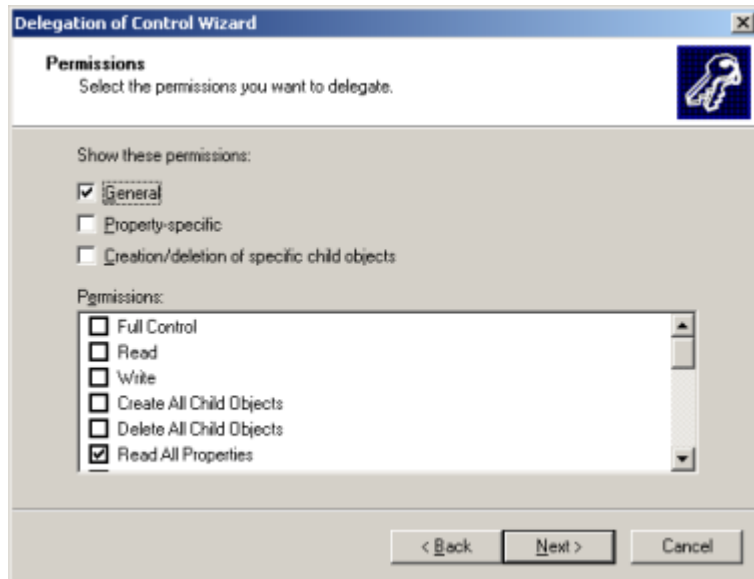


Restrict delegation to *User objects*.



advproxy - Advanced Web Proxy

Set permissions to *Read All Properties*.



Now complete the Control Delegation Wizard.

Step 3: Configure Advanced Proxy for LDAP authentication

Open the Advanced Proxy GUI page, select LDAP from the section *Authentication method* and hit *Save*.

Note: If you are configuring LDAP authentication for the first time, Advanced Proxy may complain about the missing *LDAP Base DN*.

Now enter the following LDAP settings into the Advanced Proxy GUI:

- *Base DN:* The start where the LDAP search begins
- *LDAP type:* Active Directory
- *LDAP Server:* The IP address of your Windows LDAP Server
- *Port:* The port your Windows Server listens to LDAP requests
- *Bind DN username:* The LDAP DN of the Bind DN user
- *Bind DN password:* The password for the Bind DN user

| Common LDAP settings | | | |
|----------------------|--|-------------------|---|
| Base DN: | <input type="text" value="cn=users,dc=ads,dc=local"/> | LDAP type: | <input type="text" value="Active Directory"/> |
| LDAP Server: | <input type="text" value="192.168.1.240"/> | Port: | <input type="text" value="389"/> |
| Bind DN settings | | | |
| Bind DN username: | <input type="text" value="cn=ldapbind,dc=ads,dc=local"/> | Bind DN password: | <input type="password" value="••••••••"/> |

Save the settings and restart the Advanced Proxy by clicking the *Save and restart* button. Congratulations, LDAP authentication is working now ...

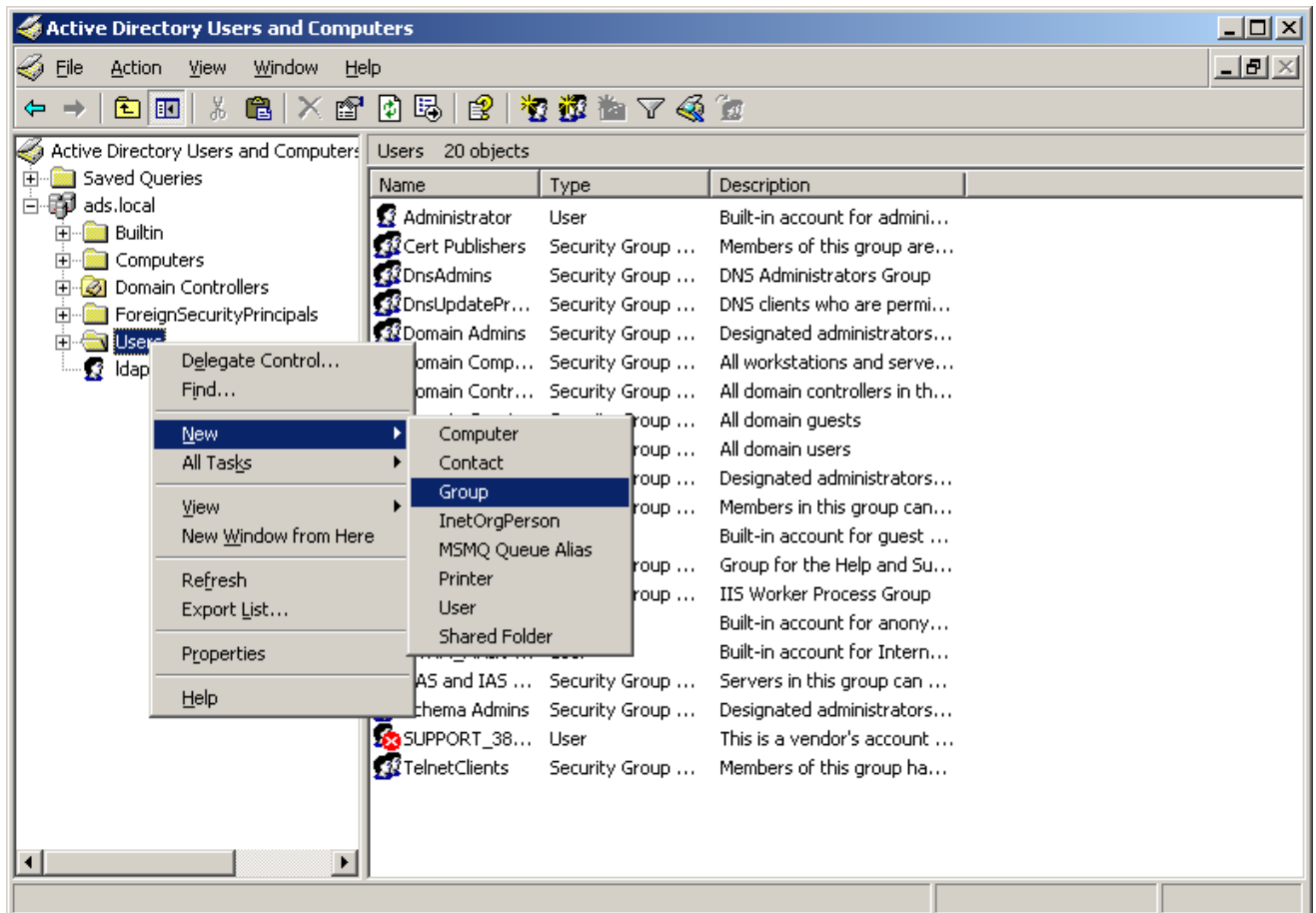
advproxy - Advanced Web Proxy

9.1.2 Configuring LDAP group based access control

Step 1: Create a group for authorized users

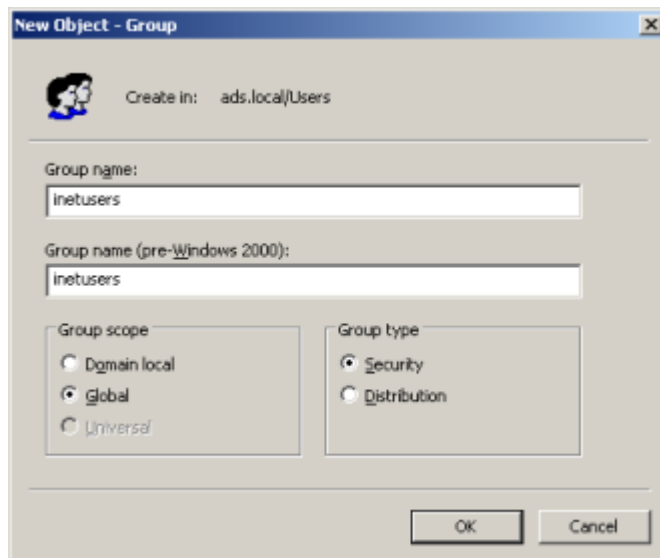
Open the MMC snap-in *Active Directory Users and Computers*.

Right click on the Users folder and select *New > Group* from the menu.

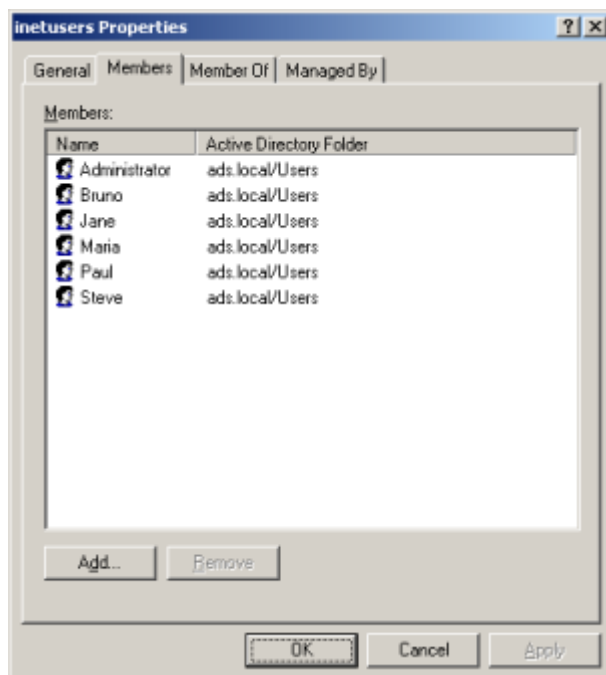


advproxy - Advanced Web Proxy

Enter the name for the new group.



Add all authorized users to this group.



Note: It's possible to add users from different Organizational Units to this group.

advproxy - Advanced Web Proxy

Step 2: Configure LDAP authentication with group based access control

Open the Advanced Proxy GUI page, select LDAP from the section Authentication method and hit Save.

Note: If you are configuring LDAP authentication for the first time, Advanced Proxy may complain about the missing *LDAP Base DN*.

Now enter the following LDAP settings into the Advanced Proxy GUI:

- *Base DN:* The start where the LDAP search begins
- *LDAP type:* Active Directory
- *LDAP Server:* The IP address of your Windows LDAP Server
- *Port:* The port your Windows Server listens to LDAP requests
- *Bind DN username:* The LDAP DN of the Bind DN user
- *Bind DN password:* The password for the Bind DN user
- *Required group:* The DN for a group with authorized user accounts

| | | | |
|-----------------------------------|--|-------------------|---|
| Common LDAP settings | | | |
| Base DN: | <input type="text" value="cn=users,dc=ads,dc=local"/> | LDAP type: | <input type="text" value="Active Directory"/> |
| LDAP Server: | <input type="text" value="192.168.1.240"/> | Port: | <input type="text" value="389"/> |
| Bind DN settings | | | |
| Bind DN username: | <input type="text" value="cn=ldapbind,dc=ads,dc=local"/> | Bind DN password: | <input type="password" value="....."/> |
| Group based access control | | | |
| Required group: | <input type="text" value="cn=inetusers,cn=users,dc=ads,dc=local"/> | | |

Save the settings and restart the Advanced Proxy by clicking the Save and restart button. From now on, only members of the given group will be able to access the proxy ...