ACL
Compliance Director™

Network Compliance Solution

Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES

User Manual

Cyber Operations Inc.
http://www.CyberOperations.com
153 Cahaba Valley Parkway
Pelham, AL 35124
Ph: 205-403-2923
Fax: 205-403-6508

Table of Contents

Figures

Introduction

Thanks

Thanks for purchasing ***ACL Compliance Director***, and we hope you enjoy all the time it will save you while managing your organizations network access policies. Please let us *know if there is any way you feel this product, its documentation, or its support could be* improved to better meet your needs.

About ACL Compliance Director

ACL Compliance Director is a system which allows your organization to store, control, and implement all of your organization's network access policies for different brands and types of networking devices from one centrally managed database with revision history and access control. It also provides you advanced tools for creating, analyzing, and deploying your access control policies, including comparison, searching, conflict detection, hierarchal lists, and simultaneous synchronization of devices with the database. The web-based interface allows access from any platform, and allows you to configure the system to suit your organization's needs.

System Requirements

ACL Compliance Director is a web based application for Linux which uses an SQL based database for its data storage and a separate authentication server. The backend database is PostgreSQL, version 8.0 or later. Currently TACACS+, Radius, LDAP, and Unix account based methods of authentication and authorization are supported..

ACL Compliance Director is compatible with Cisco IOS based routers, Juniper routers, Cisco PIX firewalls, Cisco ASA devices, Aruba mobility controllers, Force 10 routers, and Netscreen firewalls. You can also deploy via Cyber Operations FLM-ANT sensors.

Customization is available. If you have integration requirements for other Linux distributions or UNIX variants, you require the use of another database system, you need to integrate with a different authorization system, or you need support for another type of router or firewall please contact us at Cyber Operations so that we can assist you.

Additional Resources

In addition this user manual there is also a tutorial for beginning user tutorial that will be offered to new users as an option when the log into ***ACL Compliance Director***, and there is also an online FAQ as well as other resources available at http://www.cyberoperations.com .

Setup

Install the Software

Initial Installation

Installing ***ACL Compliance Director*** on a server simply consists of unpacking the gzip'ed tar file containing the distribution, then running the provided install script. Below is an example of the required commands you would need to run with root access.

```
tar –zxf acd.tar.gz
cd acd
./installacd
```

This will install to the directory **/usr/local/acd** by default. You can specify an alternate installation directory by passing it as a parameter to the **installacd** command.

Updating an Existing Installation

ACL Compliance Director has a built in auto-update mechanism. To check for and install an upgrade to the system, simply run the command **/usr/local/acd/acdupdate** assuming that you installed to the default directory. This will download and install any updates to the software.

Setup the Database

Currently PostgreSQL is the only supported database type. Assuming you have PostgreSQL installed and configured for the user *myuser* on hostname *myhost*, then you can create the initial database named *acl* by using the following commands:

```
createdb acl
psql -h myhost -d acl -U myuser -f /usr/local/acd/setup.sql
```

This is assuming that **createdb** and **psql** are in your path; they are usually installed somewhere like **/usr/local/pgsql/bin**. This is also assuming that you installed ***ACL Compliance Director*** to the default location of **/usr/local/acd/.** This will execute the SQL commands in **/usr/local/acd/setup.sql** which will setup the required tables.

You must also edit your configuration file, at **/etc/aclserver.conf** to specify the hostname, database name, username, and password to access your database. The following example entries would be used for a database named **acl** on the host **myhost** for access using the username **myuser** and the password **mypassword**.

```
DatabaseAddress = myhost
DatabaseName = acl
DatabaseUser = myuser
DatabasePassword = mypassword
```

Upgrade the Database

If you are upgrading from ***ACL Compliance Director*** build 5032 or earlier, then the database schema has changed for the 'targets' table. If the '**DatabaseUser**' you have configured for accessing the database has the ALTER privilege on the 'targets' table, then the database will be upgraded automatically. Otherwise, you must run the SQL commands in the file **/usr/local/acd/update.sql** in order to correctly update the database tables.

Setup the Web Server

This documentation assumes that you are using Apache as your web server, and that you are not hosting any other domains or content on the same system as ***ACL Compliance Director.*** For other situations, please see the documentation for Apache or your web server.

Assuming that you would have installed to **/usr/local/acd** you would need to add the following lines to your **httpd.conf** file.

```
ScriptAlias /cgi-bin/ "/usr/local/acd/cgi-bin/"

<Directory "/usr/local/acd/cgi-bin/">
   AllowOverride None
   Options None
   Order allow,deny
   Allow from all
</Directory>
```

Your **httpd.conf** file's location will vary depending on your installation of Apache, but it is typically located somewhere like **/etc/httpd/conf/httpd.conf**, **/usr/local/apache2/conf/httpd.conf**, or similar. After modifying Apache's configuration, you will need to tell it to restart using the **apachectl** command, like this:

```
apachectl restart
```

Configure Authorization

Before you can begin using ***ACL Compliance Director*** your must configure your systems authorization. To specify the type of authorization system, you must set the **AuthType** configuration entry in **/etc/aclserver.conf** . This must be one of the values: **tacacs**, **radius**, **ldap**, or **unix**.

TACACS+

For TACACS+ based authentication, besides setting **AuthType** to **tacacs**, you must set the configuration entry **TacServer1** at a minimum. This entry specifies your server's hostname and the server key, for example:

```
AuthType=tacacs
TacServer1 = tacplus.mydomain.com    "My Server Secret"
```

You can set an additional TACACS+ server for use by setting the **TacServer2** configuration entry in the same format.

Radius

For Radius based authorization, you must set the **AuthType** and **RadServer1** configuration entries at a minimum, and similarly to TACACS+ authorization you can specify an additional server using the **RadServer2** entry. Below is an example.

```
AuthType=radius
RadServer1 = radius.mydomain.com    "My Server Secret"
```

LDAP

For LDAP based authorization, you must set the **AuthType**, **LDAPServer**, and **LDAPBaseDN** configuration entries. For example, if your company name was Acme and you had a base **dn** value for your LDAP server based on your domain name as is typically done, you would have these entries. Currently TLS/SSL is not supported for communicating with an LDAP server, and SASL is required.

```
AuthType=ldap
LDAPServer=ldap.acme.com
LDAPBaseDN=dc=acme,dc=com
```

Local Password File

You can authenticate users based on a local password file, in the same format as a Unix password by setting **AuthType=unix** in the **/etc/aclserver.conf** configuration file. You must also set the path of the password file by setting the **UnixPasswordFile** configuration entry. If you wish to limit the commands that specific users are authorized to run, you should also set the **UnixAuthEnabled** configuration entry to the value “1”. Below is an example of typical configuration values for password file authentication and authorization.

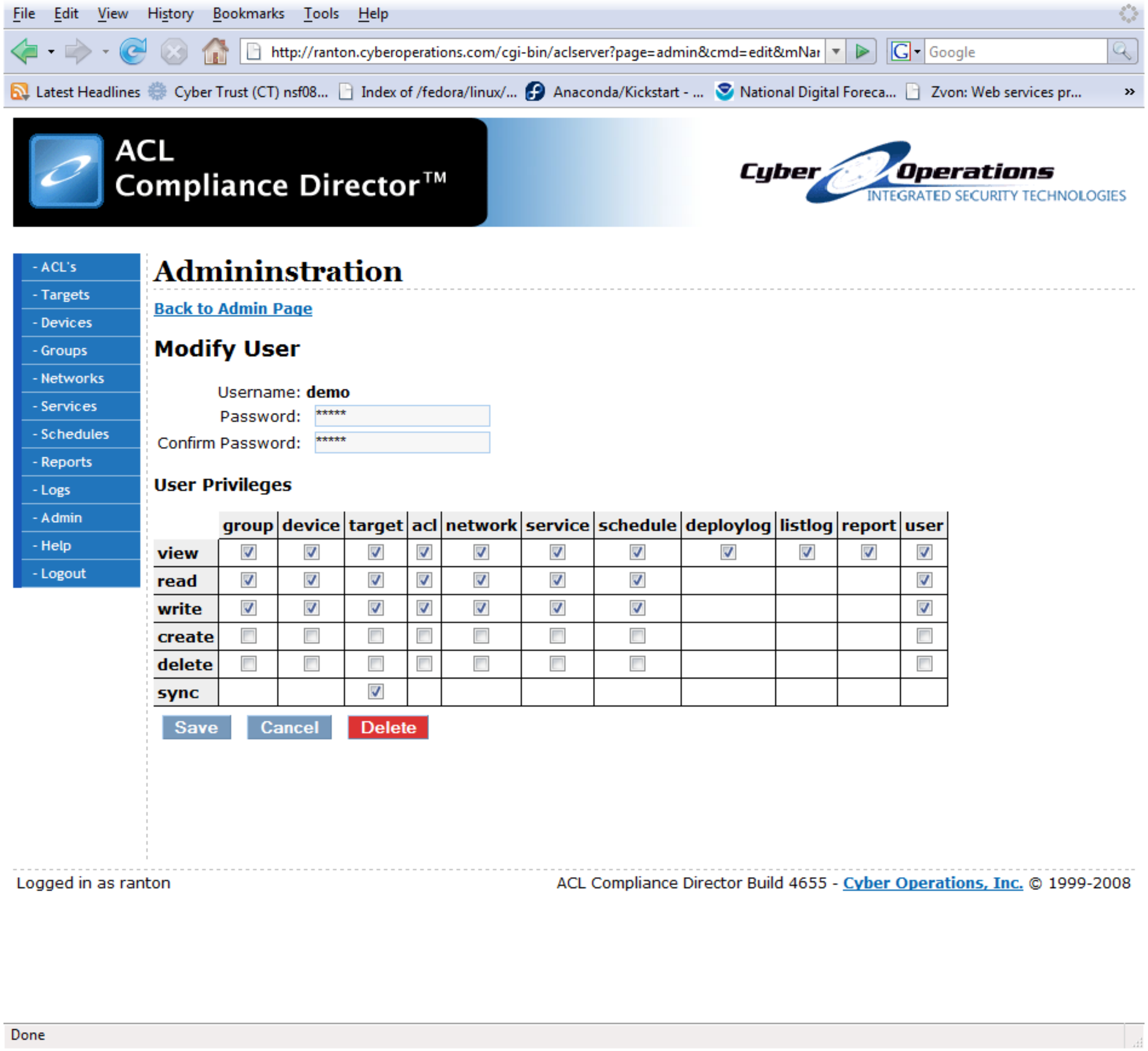
```
AuthType=unix
UnixPasswordFile = /usr/local/acd/passwd
UnixAuthEnabled=1
```

The command line utility **acluser** can be used to create, modify, delete or change the passwords of accounts when using a local password file.

NOTE: Please ensure that you have the file permissions of your password file set appropriately. The **aclserver** CGI must have read access to the file for authorization to work correctly. It is usually best to set the file permissions so that the **httpd** or **apache** user owns the file, but no one else has access to it, and also it is best to ensure it is not in a directory that your web server can view.

Admin Web Interface

When you are using local authentication, meaning that **AuthType** is set to **unix** then you can use the built-in web interface for managing users. Click on 'Admin' in the navigation area on the left side of the web interface. You will see a list of existing users as well as a "Create User" button. When you either click "Create User" or click on an existing user you will see the "Edit User" page which will allow you to set the actions the user is allowed to take by selecting the appropriate checkboxes for each action. See "Limiting User Commands" for more info on user actions.



http://ranton.cyberoperations.com/cgi-bin/aclserver?page=admin&cmd=edit&mNar

Admininstration

Back to Admin Page

Modify User

Username: **demo**
Password: *****
Confirm Password: *****

User Privileges

	group	device	target	acl	network	service	schedule	deploylog	listlog	report	user
view	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
read	☑	☑	☑	☑	☑	☑	☑				☑
write	☑	☑	☑	☑	☑	☑	☑				☑
create	□	□	□	□	□	□	□				□
delete	□	□	□	□	□	□	□				□
sync			☑								

Save Cancel Delete

Logged in as ranton

ACL Compliance Director Build 4655 - Cyber Operations, Inc. © 1999-2008

Figure 1

Limiting User Commands

You can limit the actions individual users are allowed to execute when using TACAS+, Radius, or Unix based authorization schemes. For TACACS+, you configure the commands users have access to in the standard way. For Radius servers, you must set the Cisco-AVPair (which is a Cisco vendor extension to Radius supported by most Radius servers) **allowcmds** to a comma separated list of commands you wish the user to be able to run. For FreeRadius you would have a similar user configuration to this in your **users** file.

```
MyUser  Cleartext-Password := "password"
        Service-Type = Login-User,
        Service-Type = NAS-Prompt-User,
        cisco-avpair = "allowcmds=view, read,create acl,write acl,sync"
```

This user would be allowed to view listings of all types of objects; have read access to all objects; be able to create and write ACL's; and would be able to synchronize(deploy to) devices.

For password file based authorization, the same type of command specification is passed on the command line to **acluser** when creating or modifying a user account, but without the preceding "allowcmds=". For example this command would create an equivalent password file based user to the above example.

```
acluser create MyUser ‘view, read,create acl,write acl,sync’
```

This user created by the command below would be allowed to execute all commands within the system:

```
acluser create AdminUser ‘*’
```

The single quotations keep the shell from trying to do a file expansion of the asterisk.

For more information on **acluser** run the command with no arguments to see its builtin help information.

The command syntax is **<action> <objecttype>** where action is one of **view**, **read**, **write**, **create**, **delete**, or **sync**. The view command gives permission to view the listing of objects of a certain type, where the read command gives permission to examine the actual object values.

The supported object types are **device**, **target**, **group**, **acl**, **network**, **service**, **schedule**, **listlog**, **deploylog**, **report,** and **user**. The **sync** command only applies to objects of type target, and the **create**, **write**, and **delete** commands do not apply to **listlog**, **deploylog**, or **report** object types.

When using local authentication any user with permissions that allow creating or editing users will essentially have all privileges, because they will have the capability of changing user privileges.

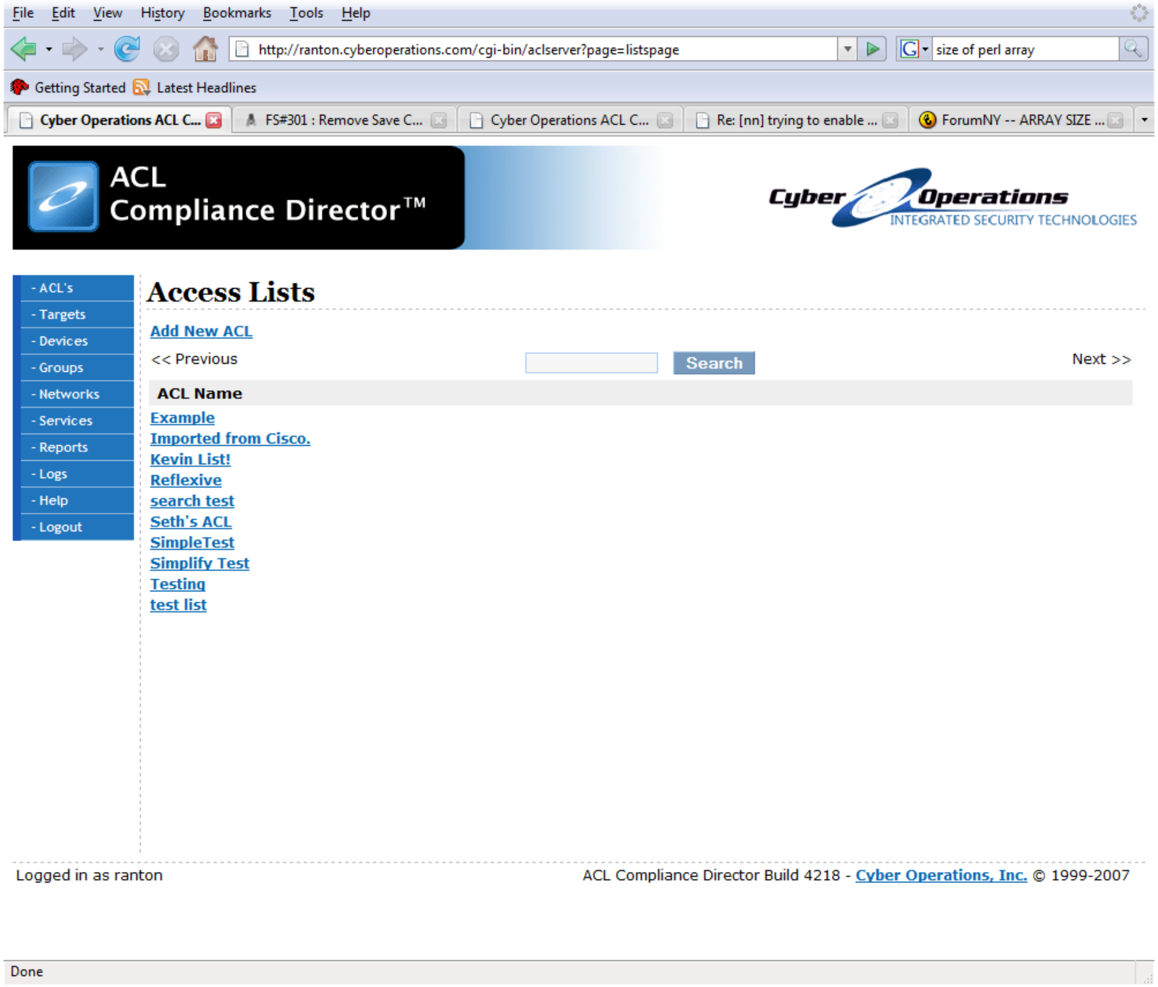
For a command entry if an asterisk (*) is specified instead of the object type then that implies all object types. So "read *" would allow read access on all object types.

Access Lists

List Basics

Access lists, also known as ACL's, consist of a sequence of entries, each of which specifies whether a certain type or group of packets will be permitted or denied through the filter. ACL Compliance Director maintains your access lists in a platform independent format for you so that they can be easily sent to different device types, typically a router or firewall.

Click on the ACL's link in the navigation tab on the left of the web page to view the access lists currently stored in ***ACL Compliance Director***. You should see a page entitled "**Access Lists**". At the top there is a link named "**Add New ACL**", and below that there is a heading "ACL Name" beneath which you can see each existing access list, by name.


File
Edit
View
History
Bookmarks
Tools
Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=listspage
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Search
Done

Access Lists

Add New ACL

<< Previous   Next >>

ACL Name

Example
Imported from Cisco.
Kevin List!
Reflexive
search test
Seth's ACL
SimpleTest
Simplify Test
Testing
test list

Logged in as ranton   ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

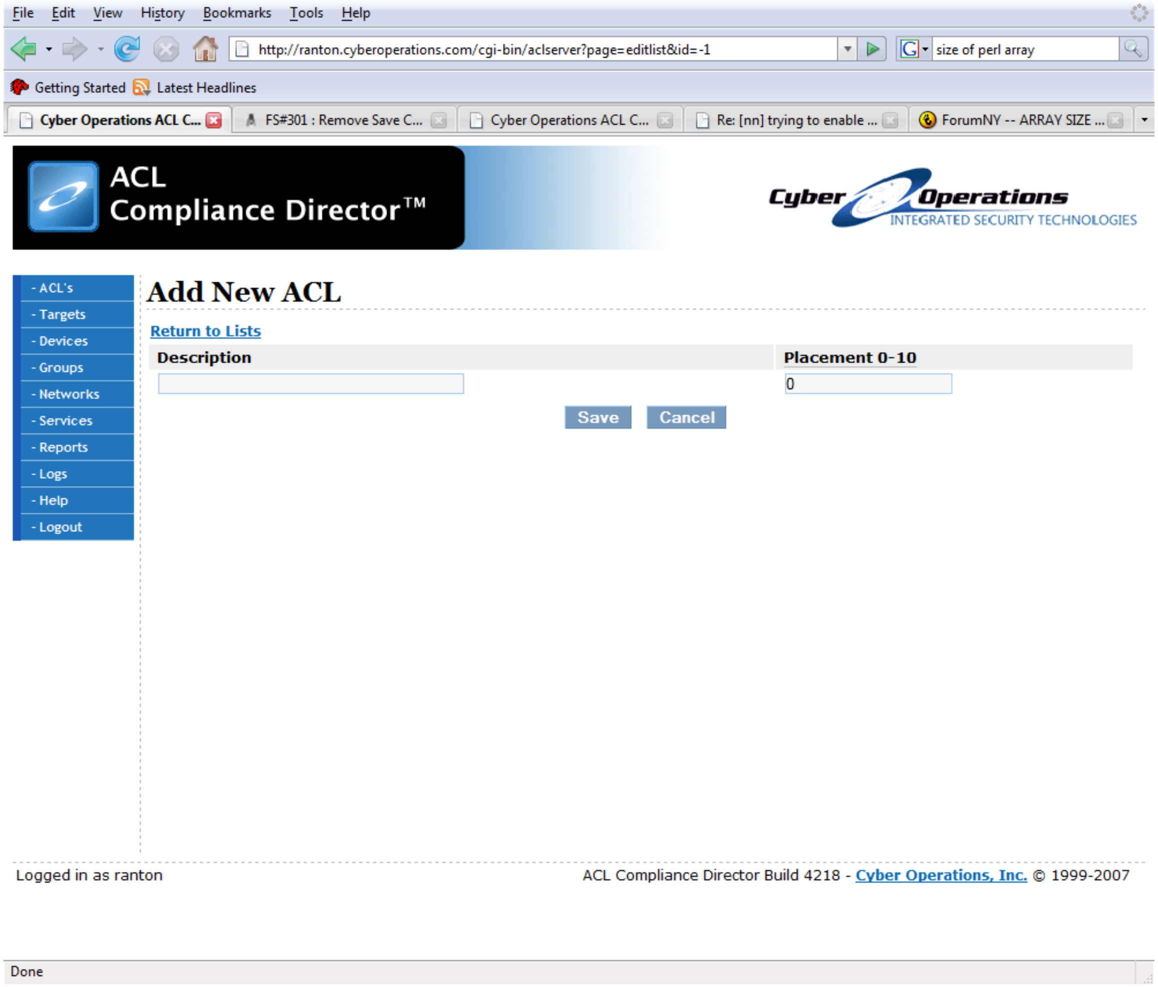
Figure 2 - Access Lists

Creating a New Access List

Follow these steps to create a new access list:

- Log into ***ACL Compliance Director*** if you have not already done so.
- Click the “ACL’s” link in the navigation portion on the left of your browser window.
- Click the link titled “Add New ACL”
- Enter a name for your new ACL, and then click the “Save” button.
- Click the “Edit Entries” link just below the description text box.

You have now created a new access list and you are ready to edit the entries it contains.


File
Edit
View
History
Bookmarks
Tools
Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editlist&id=-1
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Save
Cancel
Done

Add New ACL

Return to Lists

Description	Placement 0-10
	0

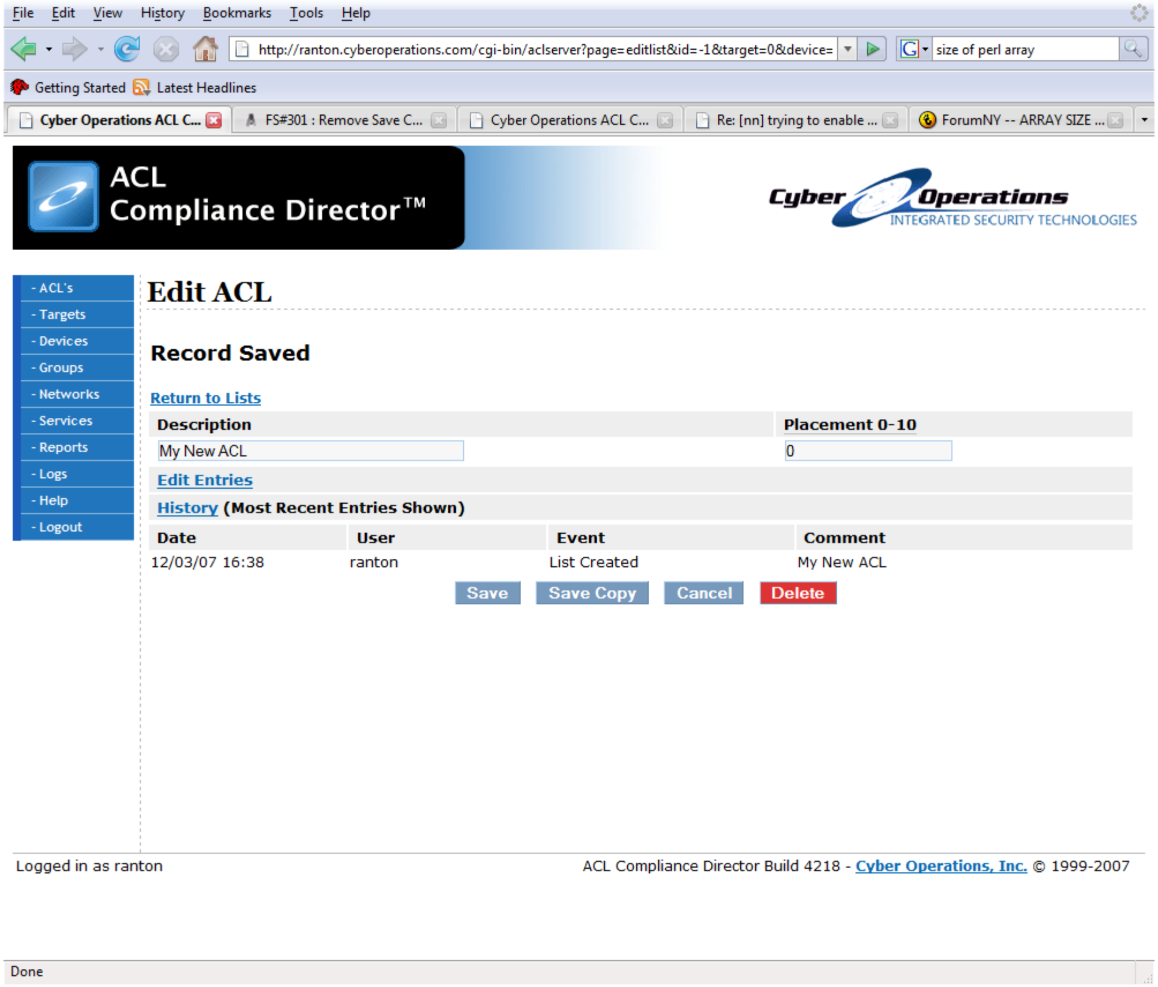
Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 3 - Add New ACL

Adding an entry

Click the “Append New Entry” link near the bottom of the “List Entries” page to append a new entry to the end of the access list, or click the plus shaped icon to the right of an existing access list entry to insert a new entry directly above an existing one.


File
Edit
View
History
Bookmarks
Tools
Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editlist&id=-1&target=0&device=
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Save
Save Copy
Cancel
Delete
Done

Edit ACL

Record Saved

Return to Lists

Description	Placement 0-10
My New ACL	0

Edit Entries

History (Most Recent Entries Shown)

Date	User	Event	Comment
12/03/07 16:38	ranton	List Created	My New ACL

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 4 - My New ACL

Either of these methods will take you to the “Edit Entry” page with the caption “Add New Entry” and all of the fields blank, ready for your entry’s information. This is also the same page you will use to edit existing access list entries.

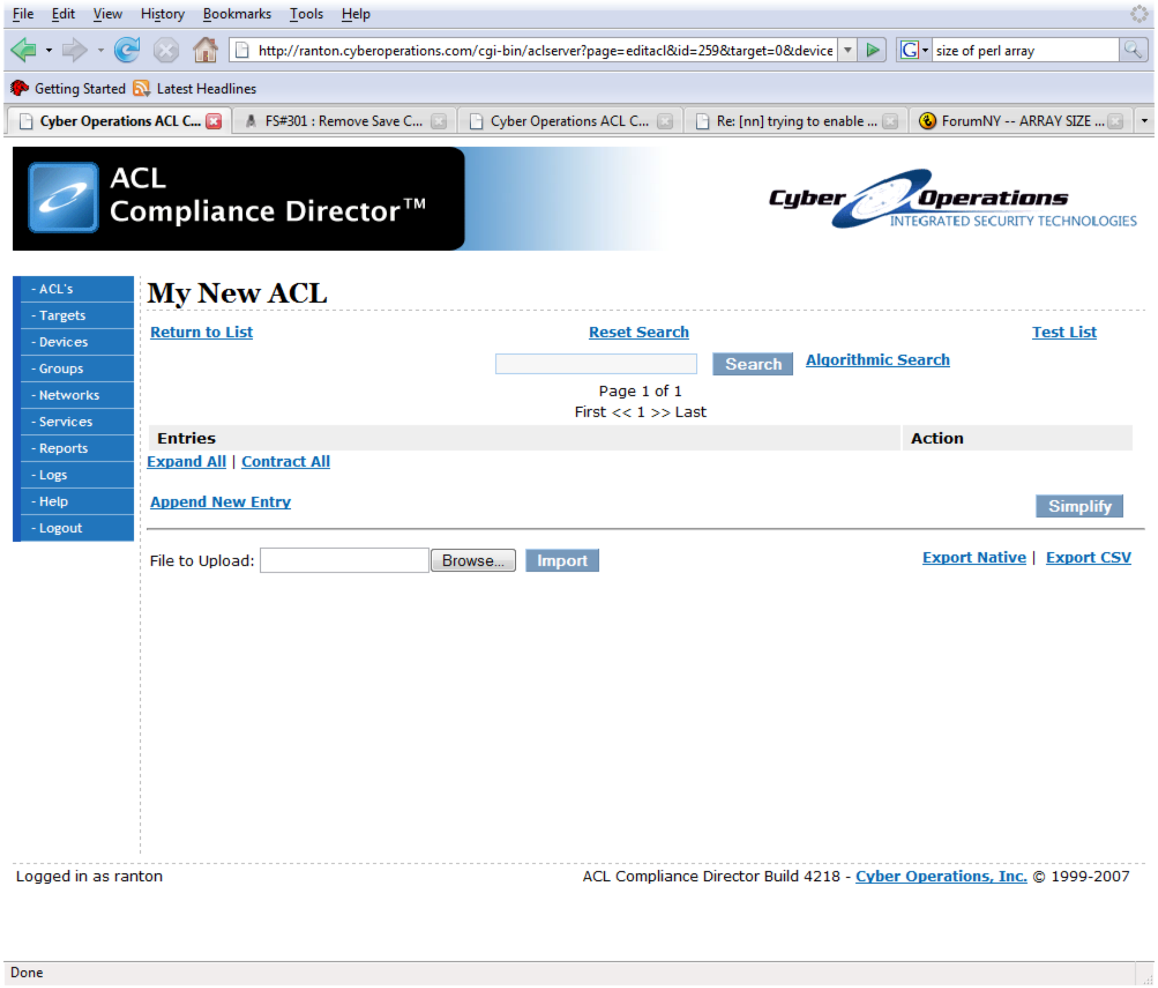

File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editacl&id=259&target=0&device
size of perl array
Getting Started Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
My New ACL
Return to List
Reset Search
Test List
Search
Algorithmic Search
Page 1 of 1
First << 1 >> Last
Entries
Action
Expand All | Contract All
Append New Entry
Simplify
File to Upload:
Browse...
Import
Export Native | Export CSV
Logged in as ranton
ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007
Done

Figure 5 - My New ACL Entries

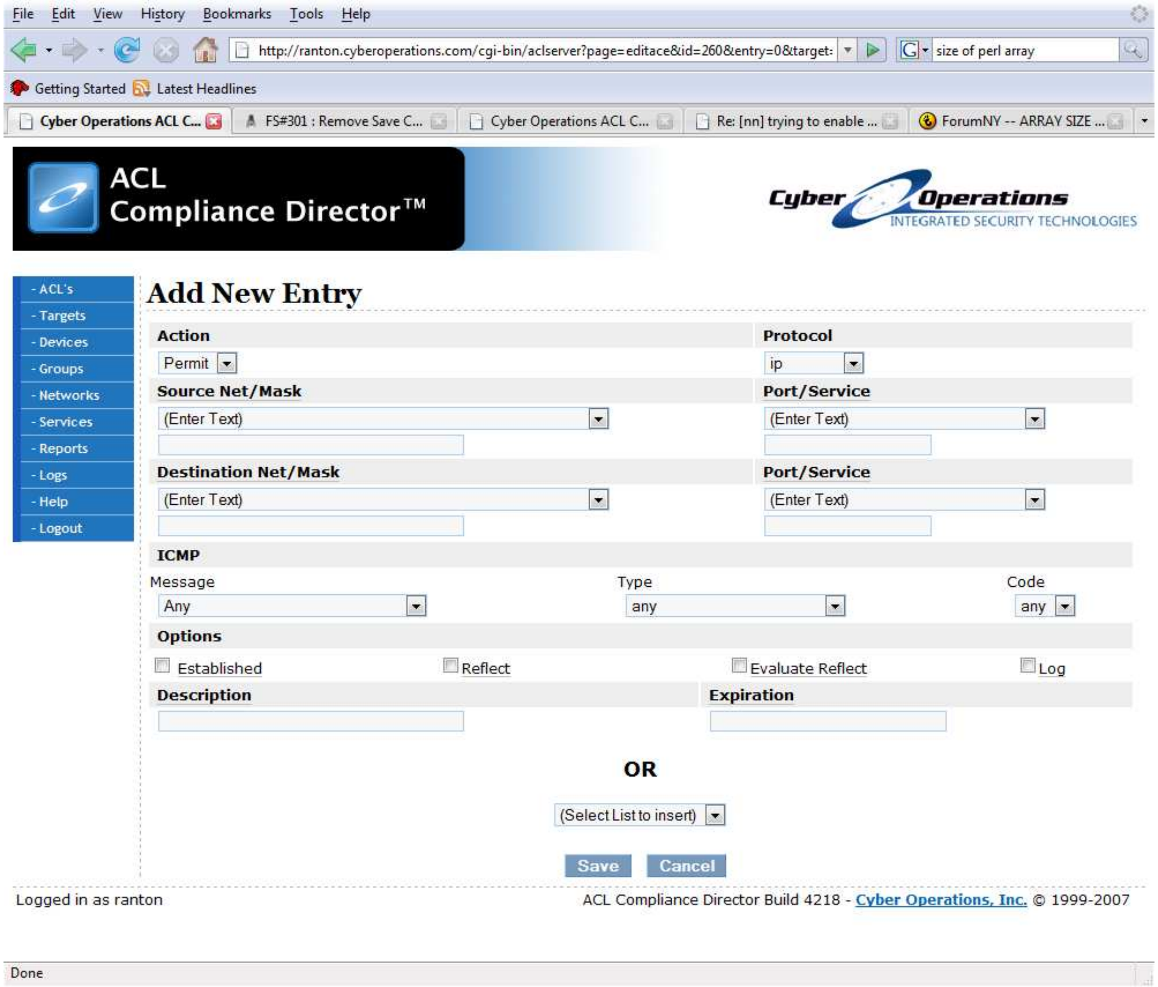
Here is a description of each entry, roughly from left to right and top to bottom as seen:

- **Action** – This is either permit or deny and describes the action that will be taken on packets which match the entry.
- **Protocol** – The protocol a packet must be to match the entry. The value IP means any internet protocol. The most common protocols are TCP, UDP, and ICMP.
- **Source Net/Mask** – This field describes the host or network address and the mask associated with it that the source address of the packet will be checked against when matching this entry. The address can be both an IPv4 or IPv6 internet address, and an optional mask. If the mask is not present for an IPv4 address, it will be assumed to be 32; likewise, if the mask is not present for an IPv6 address it will be assumed to be 128. A mask is specified by a '/' (forward slash) following the address followed by a number. The range for an IPv4 mask is 0 to 32 and the range for an IPv6 mask is 0 to 128. The drop down menu can be used to select a predefined network instead of entering a custom address and mask. See the section "Defining Groups, Networks, and Services" for more information on defining and using Networks.
- **Port/Service** – This field specifies either a port or a predefined Service that the source port of the packet will be checked against for a match. This field is only

enabled when the protocol selected is TCP or UDP. For more information on defining and using Services see the section “Defining Groups, Networks, and Services” of this manual.

- **Destination Net/Mask –** This field describes the host or network address and the mask associated with it that must match the destination of the packet. The format of this field is the same as that of the “Source Net/Mask” field described above.
- **Port/Service –** This field specifies the port or predefined Service that the destination port of the packet will be checked against for a match. This field only applies, and is only enabled if the protocol selected is TCP or UDP.
- **Message** – This menu specified the ICMP message if the protocol is ICMP. Select “Any” to match all messages.
- **Type –** This menu specifies the ICMP type if the protocol is ICMP. Select “Any” to match all types.
- **Code –** This menu specifies the ICMP code if the protocol is ICMP. Select “Any” to match all codes.
- **Established –** This option is only enabled for the TCP protocol. If this is true then the entry will only match packets from established TCP connections.
- **Reflect –** This entry is used to create reflexive access lists.
- **Evaluate Reflect –** This entry is used to evaluate reflexive access lists.
- **Log –** This entry enables logging on the device. This depends on the device type, but typically means that the count of matching packets will be logged for the entry.
- **Description –** This is a descriptive comment for the entry.
- **Expiration –** This entry specifies a date/time for an entry to expire if temporary. For permanent entries leave this field blank.

At the bottom of the “Edit Entry” page you will see a drop down list with the default item “(Select list to insert)”. This item is used to insert sublist references. If you select an access list from this menu, the list will operate as if all the entries from that list were inserted where the sublist entry is located.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editace&id=260&entry=0&target:
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Save
Cancel
Done

Add New Entry

Action: Permit	Protocol: ip
Source Net/Mask: (Enter Text)	Port/Service: (Enter Text)
Destination Net/Mask: (Enter Text)	Port/Service: (Enter Text)

ICMP

Message: Any Type: any Code: any

Options

□ Established □ Reflect □ Evaluate Reflect □ Log

Description Expiration

OR

(Select List to insert)

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 6 - Add New Entry

Delete an Entry

From the "List Entries" page you can click the trash can icon to the right of an entry to delete it from the list.

Move an Entry

You can move entries up and down in order within a list by clicking the up arrow or down arrow icons, respectively, to the right of the entry on the "List Entries" page.

Add an Exception

An exception specifies a case in which the rule(entry) it applies to will be disregarded. To add an exception to an entry, click the exception icon to its right on the "List Entries" page; the icon looks like a right angle shape with a black ball below it. This will take you to a page with the caption "Add Exception". When you click on an existing exception entry you will be taken to an otherwise identical page with the title "Edit Exception".

The fields on the “Add Exception” or “Edit Exception” page are:

- Source Net/Mask – This field describes the host or network address and the mask associated with it that the source address of the packet will be checked against when matching this entry. The address can be both an IPv4 or IPv6 internet address, and an optional mask. If the mask is not present for an IPv4 address, it will be assumed to be 32; likewise, if the mask is not present for an IPv6 address it will be assumed to be 128. A mask is specified by a ‘/’ (forward slash) following the address followed by a number. The range for an IPv4 mask is 0 to 32 and the range for an IPv6 mask is 0 to 128.
- Port/Service – This field specifies a port that the source port of the packet will be checked against for a match. This field will cause the exception to only apply to TCP and UDP packets.
- Destination Net/Mask – This field describes the host or network address and the mask associated with it that must match the destination of the packet. The format of this field is the same as that of the “Source Net/Mask” field described above.
- Port/Service – This field specifies the port that the destination port of the packet will be checked against for a match. This field will cause the exception to only apply to TCP and UDP packets.
- Description – This is a descriptive comment for the entry.
- Expiration – This entry specifies a date/time for an entry to expire if temporary. For permanent entries leave this field blank.

Conflicts and Entries With No Effect

ACL Compliance Director highlights entries which have no effect with a gray background color, and if you let your cursor hover over the entry it will show you the index of the entry which causes the highlighted entry to have no effect.

Likewise, entries which conflict with other entries are highlighted using a darker, nearly black background. An example of a conflicting entry would be trying to permit traffic that was completely blocked by an earlier entry. If you let your cursor hover over the entry it will show you the index of the entry which causes the conflict.

Importing

From the “List Entries” page you can also import entries from existing access lists, or export access lists.

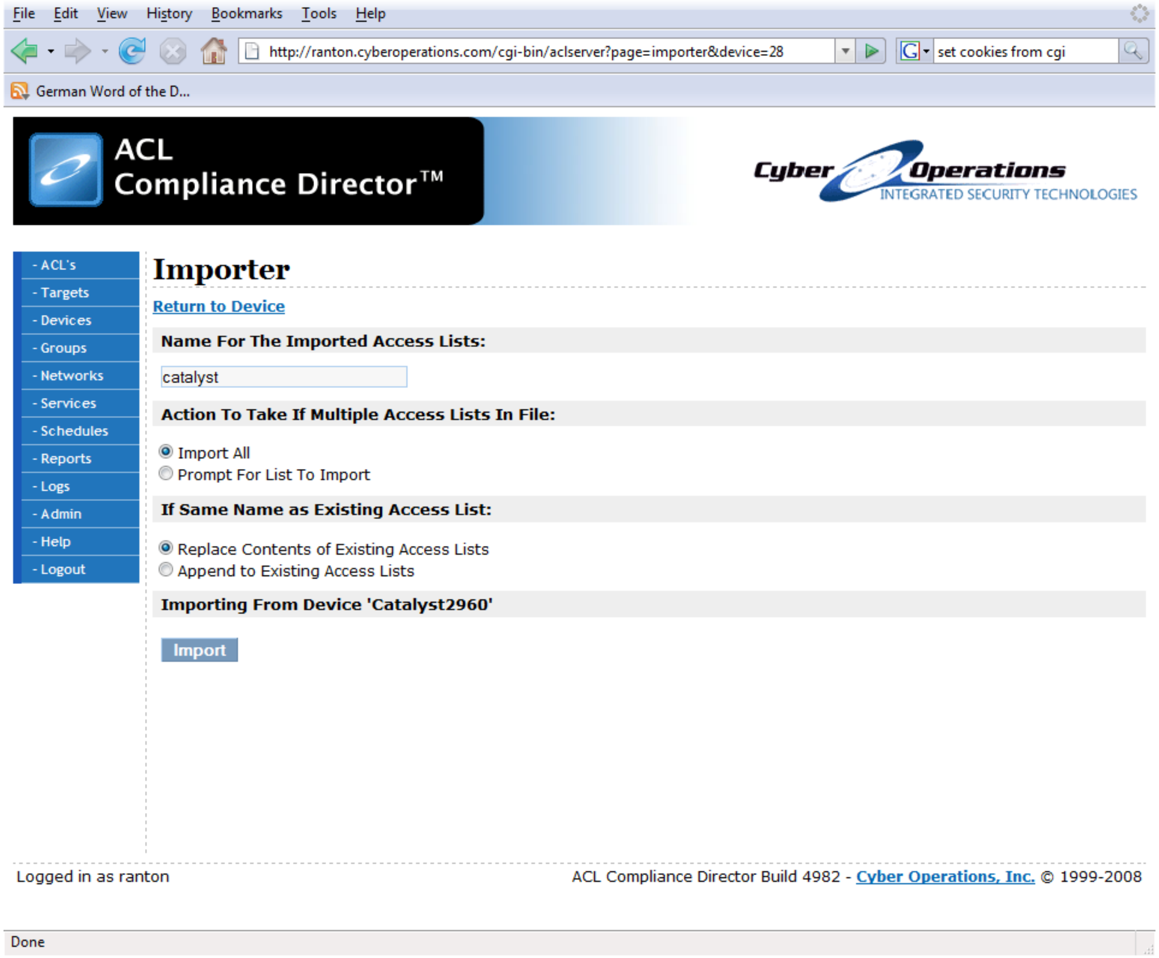
Two formats are supported for importing. The first is the “.ACL” format which is the native format of all of Cyber Operation’s ACL related product line. The second is Cisco configuration files including IOS, PIX, and ASA configuration files. To import either format, simple click the “Browse” button at the bottom of the “List Entries” page to select the file you wish to import, then click on the “Import” button.

You can also click the “Import Access Lists” link from the “Access Lists” page which will give you a larger selection of options when importing, as well as the ability to import all lists from configuration sources containing multiple access lists.

ACL Compliance Director also now supports importing directly from the device. To use this just navigate to the “Edit Device” page for the device in question, and click on the link titled “Import from Device”.

After you have selected “Import Access Lists” or “Import from Device” you will be given the “Importer” page which will let you control whether you want to import all access lists from the selected source or choose a specific access list. You will also have the option to replace or append to existing access lists with the same name(s).

You must also enter a name for your new ACL’s. If you select “Import All” then the name you enter will be used as the prefix of the name of each list in the source.



Importer

Return to Device

Name For The Imported Access Lists:

catalyst

Action To Take If Multiple Access Lists In File:

● Import All
○ Prompt For List To Import

If Same Name as Existing Access List:

● Replace Contents of Existing Access Lists
○ Append to Existing Access Lists

Importing From Device 'Catalyst2960'

Import

Logged in as ranton

ACL Compliance Director Build 4982 - Cyber Operations, Inc. © 1999-2008

Figure 7 - Importer

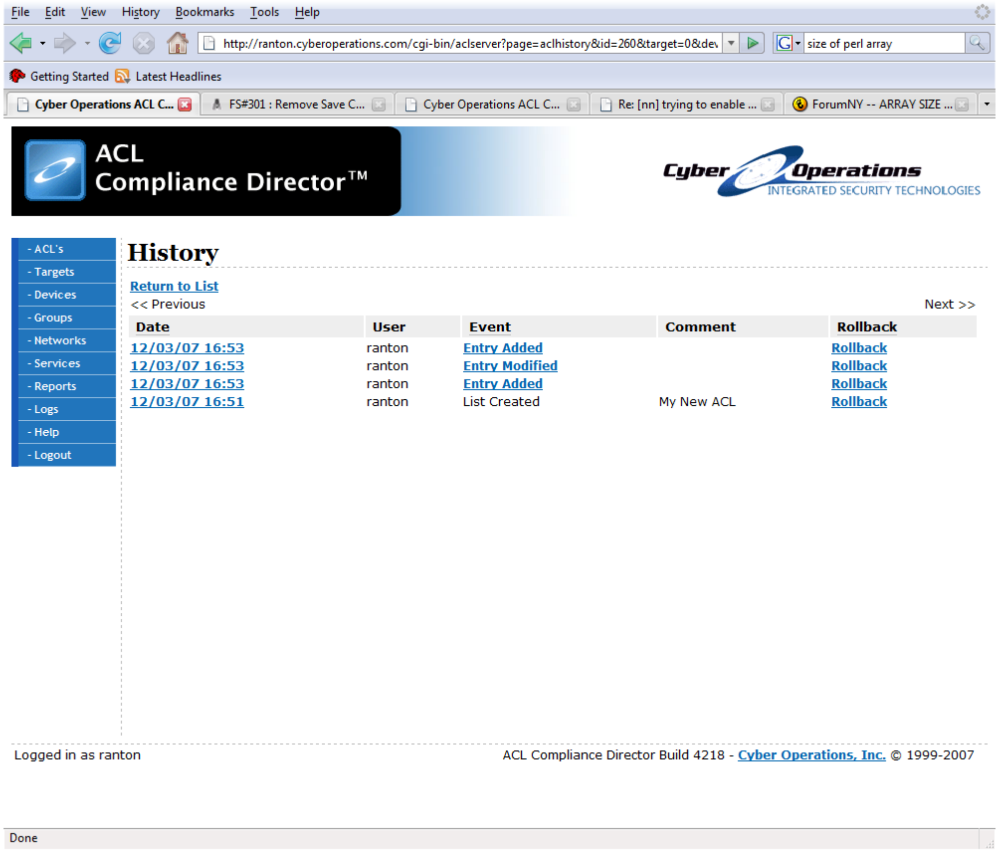
If you are importing from a file that contains more than one access list you will be presented with a menu to select which access list you would like to import.

Exporting

ACL's can be exported to either the ".ACL" format by clicking the "Export Native" link or to a comma delimited text file by clicking the "Export CSV" link. In either case it is recommended that you right-click on the link and select "Save File As" or the equivalent in your browser so that you will have an opportunity to name the downloaded file appropriately.

History and Rollback

There is an automatic history maintained of all changes made to each access list in ***ACL Compliance Director***. In order to access this history, click the link titled "History" from the "Edit List" page (not to be confused with the "List Entries" page).


File
Edit
View
History
Bookmarks
Tools
Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=aclhistory&id=260&target=0&dev
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Done

History

Return to List

<< Previous Next >>

Date	User	Event	Comment	Rollback
12/03/07 16:53	ranton	Entry Added		Rollback
12/03/07 16:53	ranton	Entry Modified		Rollback
12/03/07 16:53	ranton	Entry Added		Rollback
12/03/07 16:51	ranton	List Created	My New ACL	Rollback

Logged in as ranton

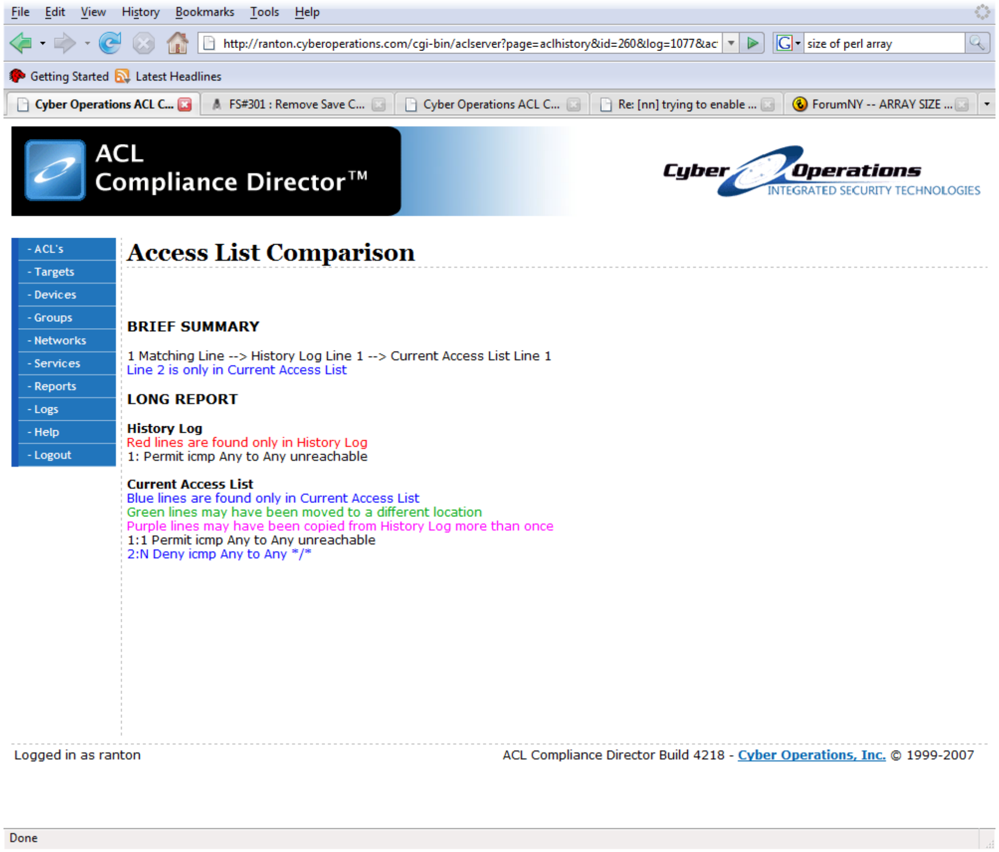
ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 8 – History

Comparing Access Lists

You can compare any two access lists within ACL Compliance Director. Go to the "Edit List" page of the first access list you would like to compare, then select the second access list from the popup menu next to the "Compare ACL to" button, then click the "Compare ACL to" button and you will be presented with a page detailing the differences between the two access lists.

The history page will present you with a history of modifications to the list from most recent to least recent. If you click on the date or event columns of a change, you will be taken to a comparison of the list immediately prior and immediately after the change. If you click the "Rollback" link for a change, the list will be rolled back(restored) to its state immediately prior to that change.


File
Edit
View
History
Bookmarks
Tools
Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=aclhistory&id=260&log=1077&ac
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout

Access List Comparison

BRIEF SUMMARY

1 Matching Line --> History Log Line 1 --> Current Access List Line 1
Line 2 is only in Current Access List

LONG REPORT

History Log
Red lines are found only in History Log
1: Permit icmp Any to Any unreachable

Current Access List
Blue lines are found only in Current Access List
Green lines may have been moved to a different location
Purple lines may have been copied from History Log more than once
1:1 Permit icmp Any to Any unreachable
2:N Deny icmp Any to Any */*

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

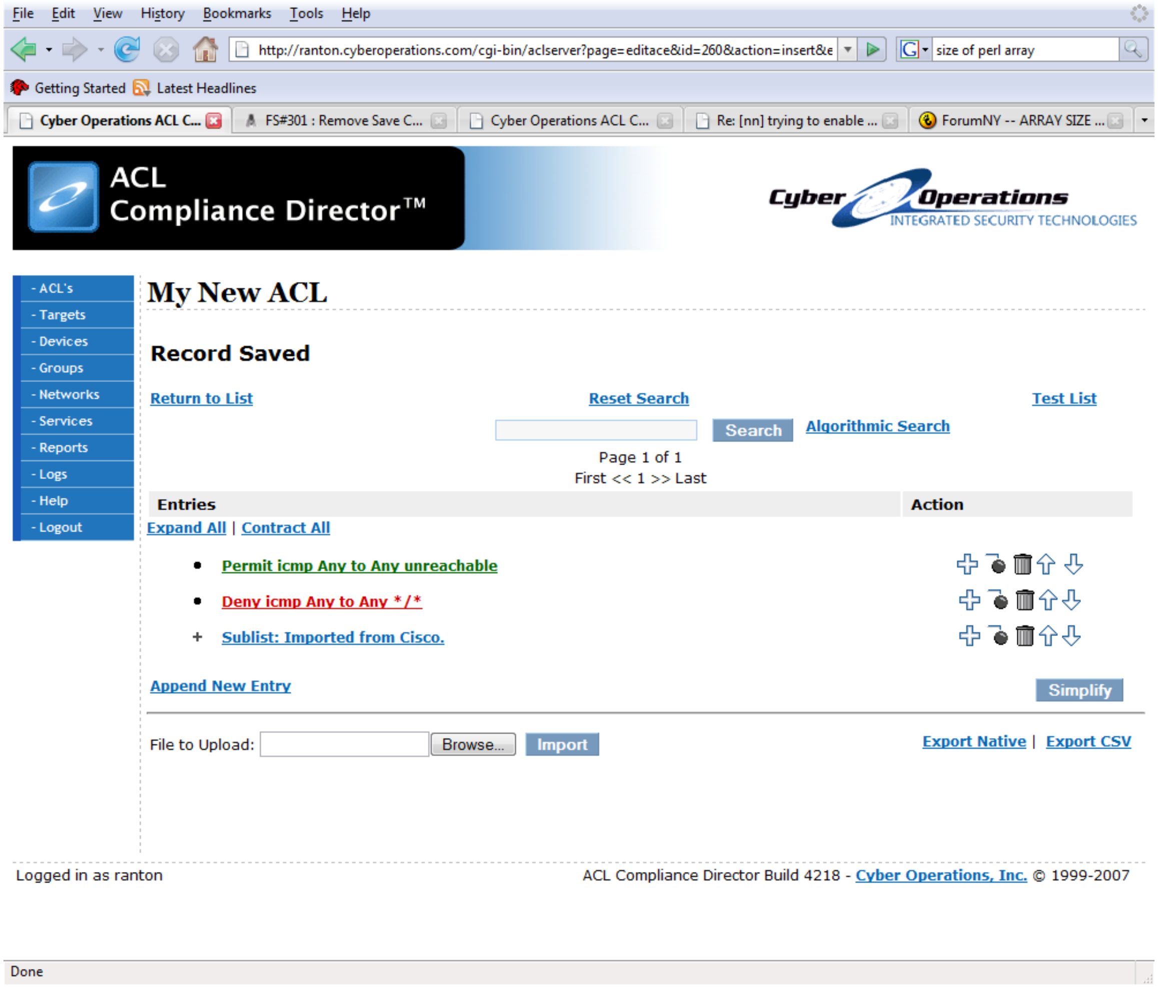
Figure 9 - Modifications

Using Sublists

In addition to regular access list entries, you can also add references to other lists, known as sublists. At the bottom of the "Add New Entry" page, you should see the heading "OR" and below that a drop down menu which allows you to select a list. Selecting a list from this menu and clicking the "Save" button will create a sublist entry in the access list. Whenever the list is sent to a device (synchronized), the actual sublist will be substituted in place of the sublist entry. This works recursively, which means that the sublist may itself have sublists.

This feature is very useful if you have some common rules for multiple devices and targets, but you also have rules which may be common across some are all of your targets. You can simply create a sublist containing the entries which are common across a group of targets, then have each target's list include your common list as a sublist.

Whenever your common list is modified, any target with a list that includes it as a sublist will automatically be marked in need of synchronization.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editace&id=260&action=insert&e
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Return to List
Reset Search
Test List
Search
Algorithmic Search
Expand All | Contract All
Append New Entry
Simplify
Browse...
Import
Export Native | Export CSV
Done

My New ACL

Record Saved

Page 1 of 1
First << 1 >> Last

Entries	Action
• Permit icmp Any to Any unreachable	
• Deny icmp Any to Any */*	
+ Sublist: Imported from Cisco.	

File to Upload:

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 10 - A Sublist

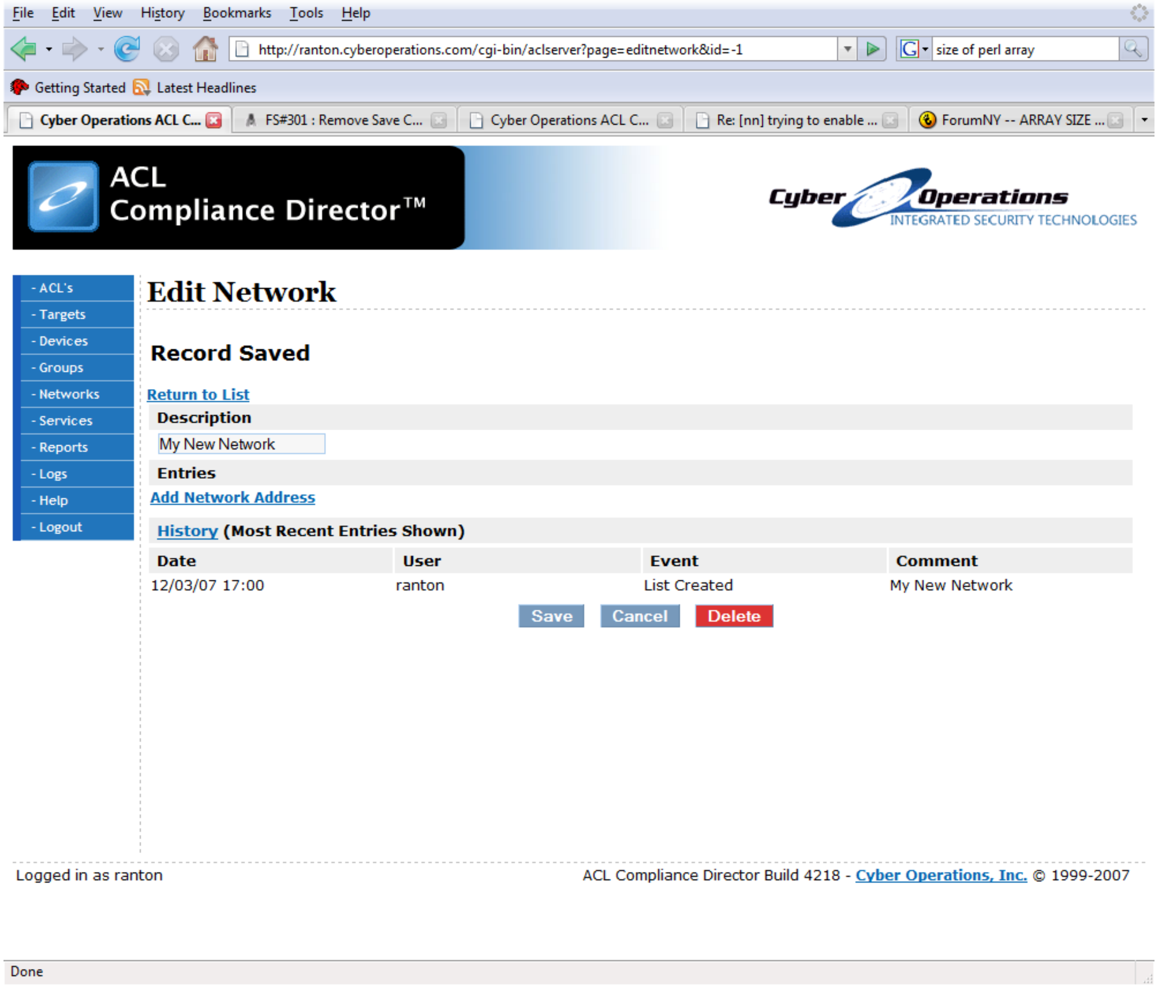
Defining Groups, Networks, and Services

ACL Compliance Director allows you to create custom defined values which can be used from within your access lists to more easily manage your network access policies. These consist of Networks, Services, and Groups. Networks are predefined combinations of network address ranges; services are combinations of ports and port t ranges; and groups are combinations of devices, targets, and other groups which also allow you to define an access list to be included by each group member automatically.

Networks

ACL Compliance Director allows you to create Network definitions which can then be used within access lists. The currently defined networks can be viewed by clicking on the “Networks” navigation link on the left of the web interface.

To create a new network, click the “Add New Network” link from the “Networks” page. You will be prompted to enter a name for your network in the “Description” field. After entering a name, click the “Save” button. After naming your new network you will be taken to the “Edit Network” page where you can define what addresses constitute your network.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editnetwork&id=-1
size of perl array
Getting Started Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Save
Cancel
Delete
Done

Edit Network

Record Saved

Return to List

Description

My New Network

Entries

Add Network Address

History (Most Recent Entries Shown)

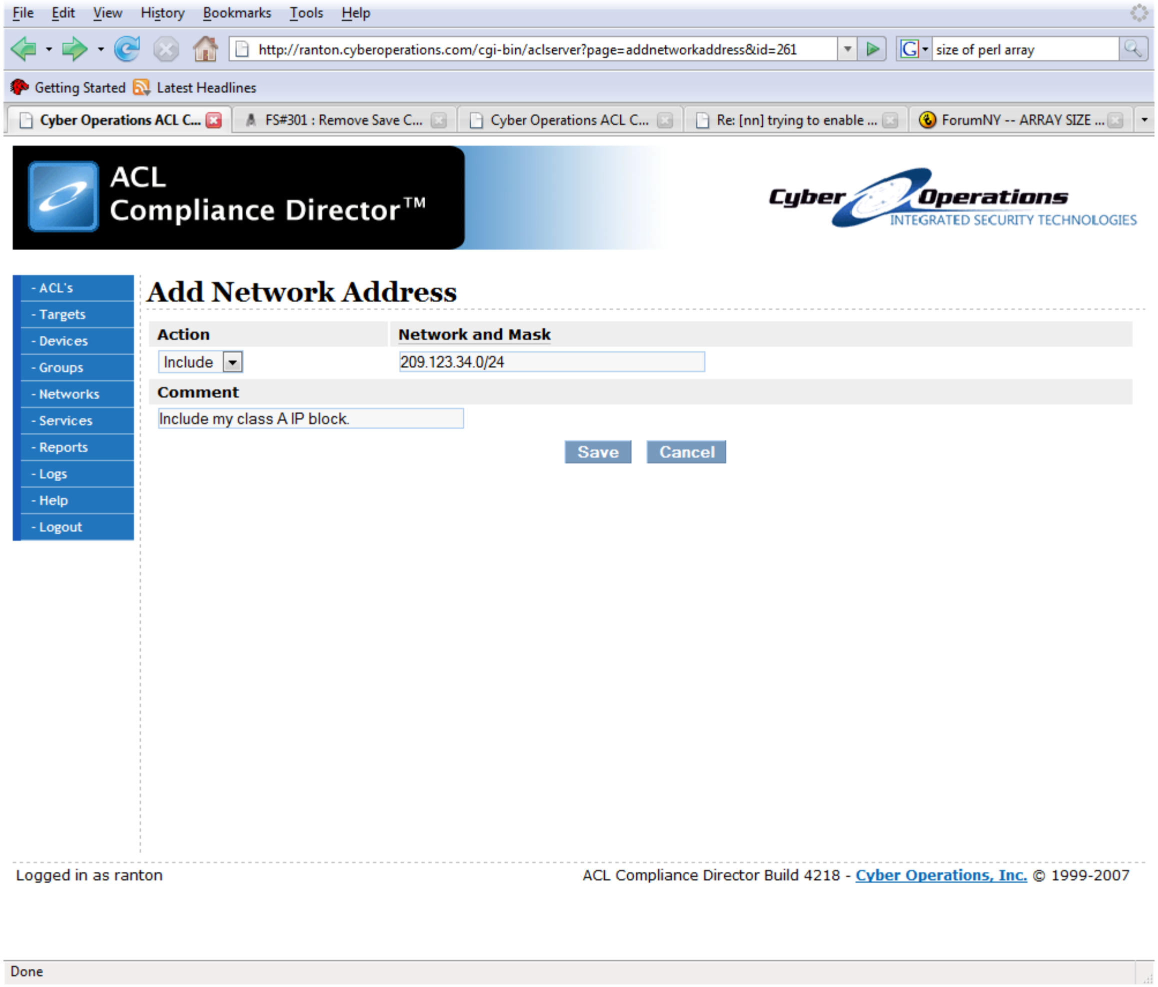
Date	User	Event	Comment
12/03/07 17:00	ranton	List Created	My New Network

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 11 - My New Network

The “Add Network Address” link will take you to a page that asks you for a network and mask as well as a comment for the network address you are adding. Additionally, there will be a menu allowing you to select whether this address will be included in or excluded from your network definition. For example, you could create a network definition that included all of the 10.0.0.0 class A private IP block except for the class C beginning with 10.0.1 by adding the address and mask 10.0.0.0/8 to be included, and adding the network address and mask 10.0.1.0/24 to be excluded.



File Edit View History Bookmarks Tools Help
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
size of perl array
ACL Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Save
Cancel
Done

http://ranton.cyberoperations.com/cgi-bin/aclserver?page=addnetworkaddress&id=261

Add Network Address

Action	Network and Mask
Include	209.123.34.0/24

Comment: Include my class A IP block.

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 12 - Add Network Address

From the “Edit Network” page you can delete network addresses by clicking the trash icon next to the network address you wish to delete.

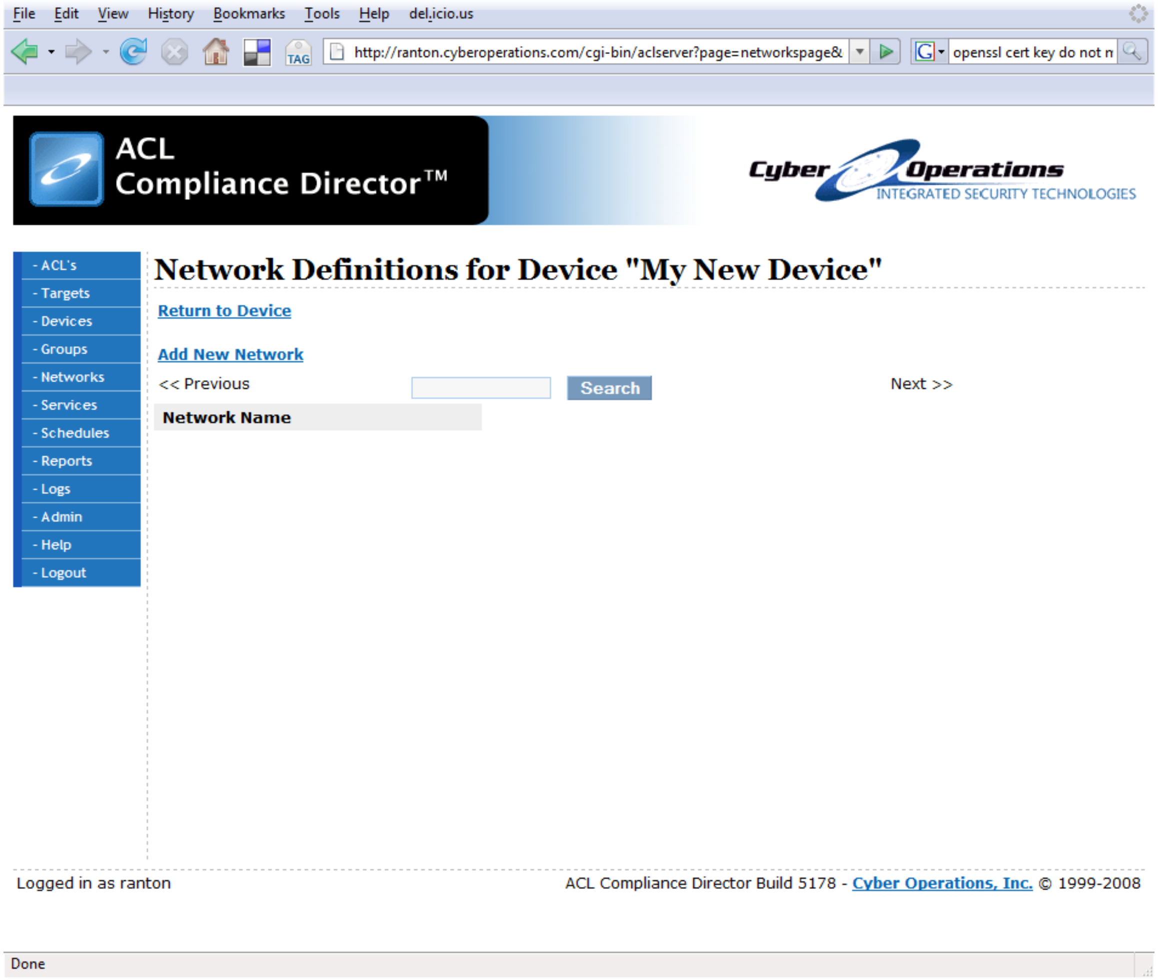
Network Overrides

You can override a network’s definition for a specific device or specific target so that when an ACL is sent to (synchronized with) that target or device, the device or target specific definition is used instead of the global definition.

In order to override a global network definition, simply define one be the same name for the target or device. Also, be aware that you may only override networks for a target or device. When you create access list entries, you may only use networks and devices that are defined globally, so any network you plan to use must have a global definition.

If a device and a target both override a network definition, then the target definition will take precedence.

To view or edit the network definitions for a device or target click the “Network Definitions” link for the “Edit Device” or “Edit Target” page respectively.



File Edit View History Bookmarks Tools Help del.icio.us
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=networkspage&
openssl cert key do not n
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Schedules
- Reports
- Logs
- Admin
- Help
- Logout

Network Definitions for Device "My New Device"

Return to Device

Add New Network

<< Previous Search Next >>

Network Name

Logged in as ranton

ACL Compliance Director Build 5178 - Cyber Operations, Inc. © 1999-2008

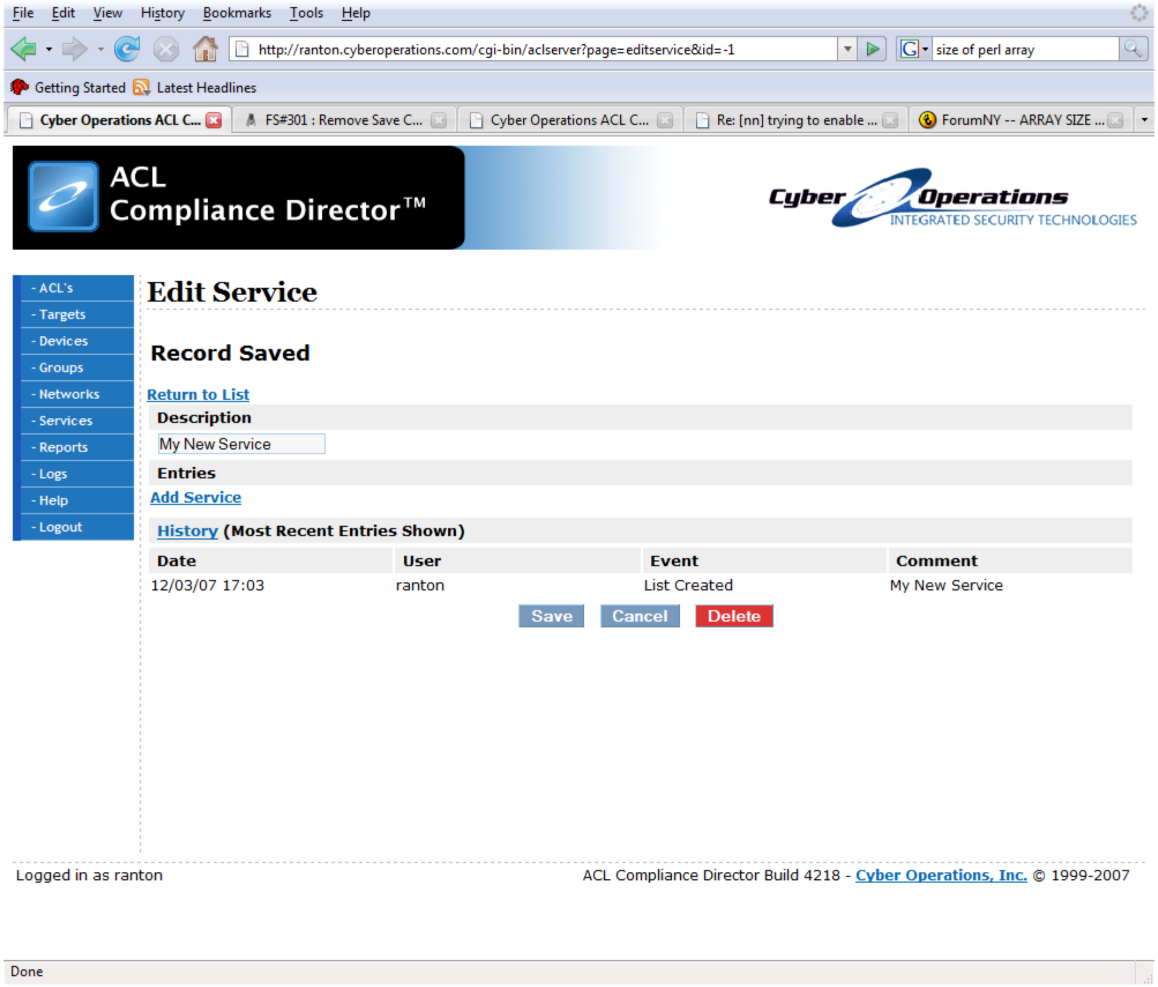
Done

Figure 13 - Network Overrides

Services

The services feature allows you to define groups of ports and port ranges that can be used when defining access list entries. To view defined services click on the “Services” link on the left side of the web interface.

Click the “Add New Service” link to create a new service. You will be prompted for a name for your new service. After entering a name in the description field, click save; you will be taken to the “Edit Service” page.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editservice&id=-1
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Save
Cancel
Delete
Done

Edit Service

Record Saved

Return to List

Description

My New Service

Entries

Add Service

History (Most Recent Entries Shown)

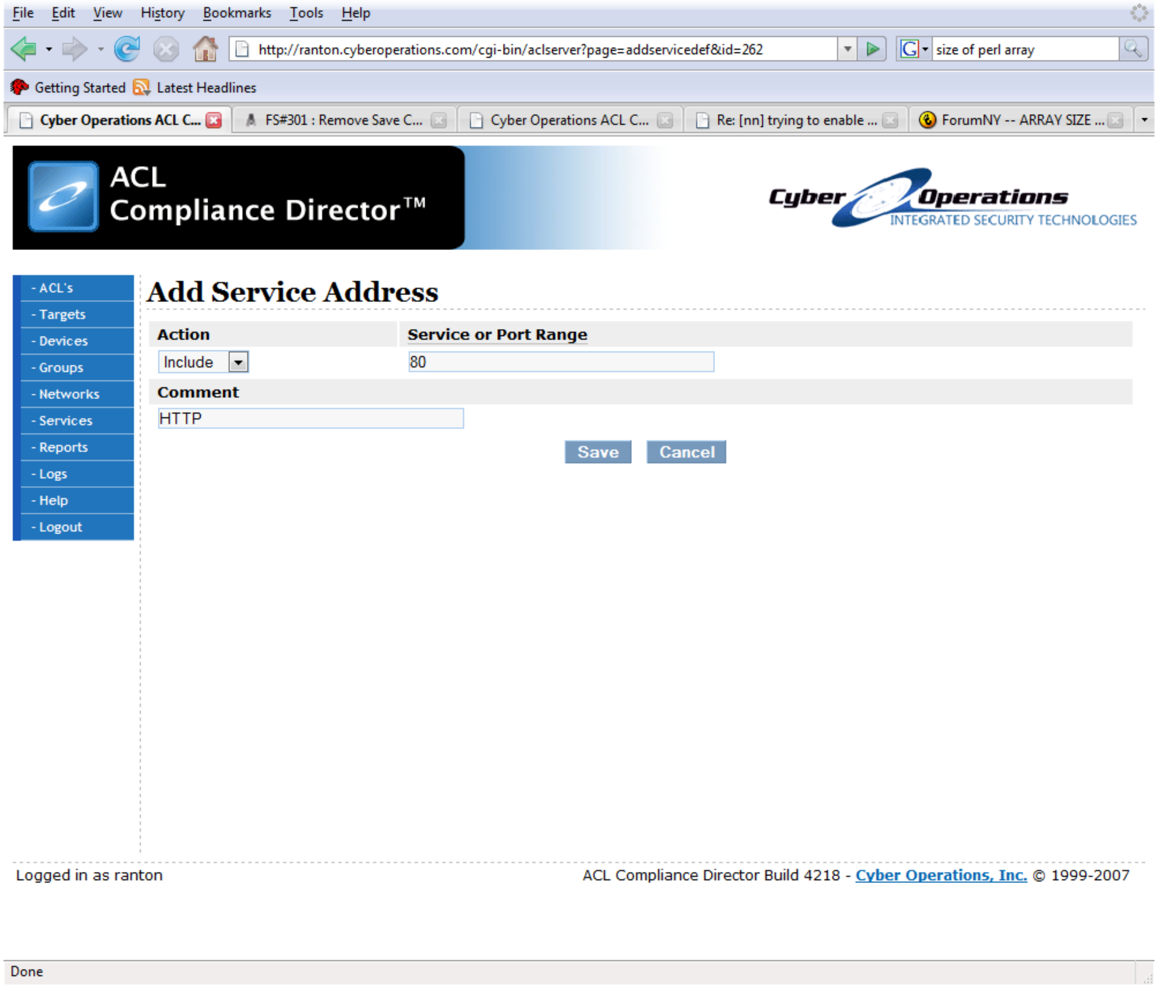
Date	User	Event	Comment
12/03/07 17:03	ranton	List Created	My New Service

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 14 - My New Service

A port or port range can be added to a service definition by clicking the “Add Service” link. You will be asked to select “Include” or “Exclude” from a menu , indicating whether you want this port or port range included or excluded from your service definition. You will also need to enter the port or port range in the “Service or Port Range” field. Port ranges are entered in the format “start-finish”, for example “1-20” would be ports from 1 through 20 inclusive. You can also enter a descriptive comment in the “Comment” field. Click save when you are through entering the fields to return to the “Edit Service” page.



File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=addservicedef&id=262
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Save
Cancel
Done

Add Service Address

Action	Service or Port Range
Include	80

Comment: HTTP

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 15 - Add Service Address

You can also delete ports from the “Edit Service” page by clicking the trash icon next to the port or port range you wish to remove.

Groups

Groups are custom defined combinations of devices, targets, and other groups which also allow you to define an access list to be included by each group member automatically.

You can view your groups by clicking on the “Groups” navigation link at the left of the web interface. Clicking the “Add New Group” link takes you to the edit group page with a new group with a blank name. Enter a name for your group in the “Group Name” field.

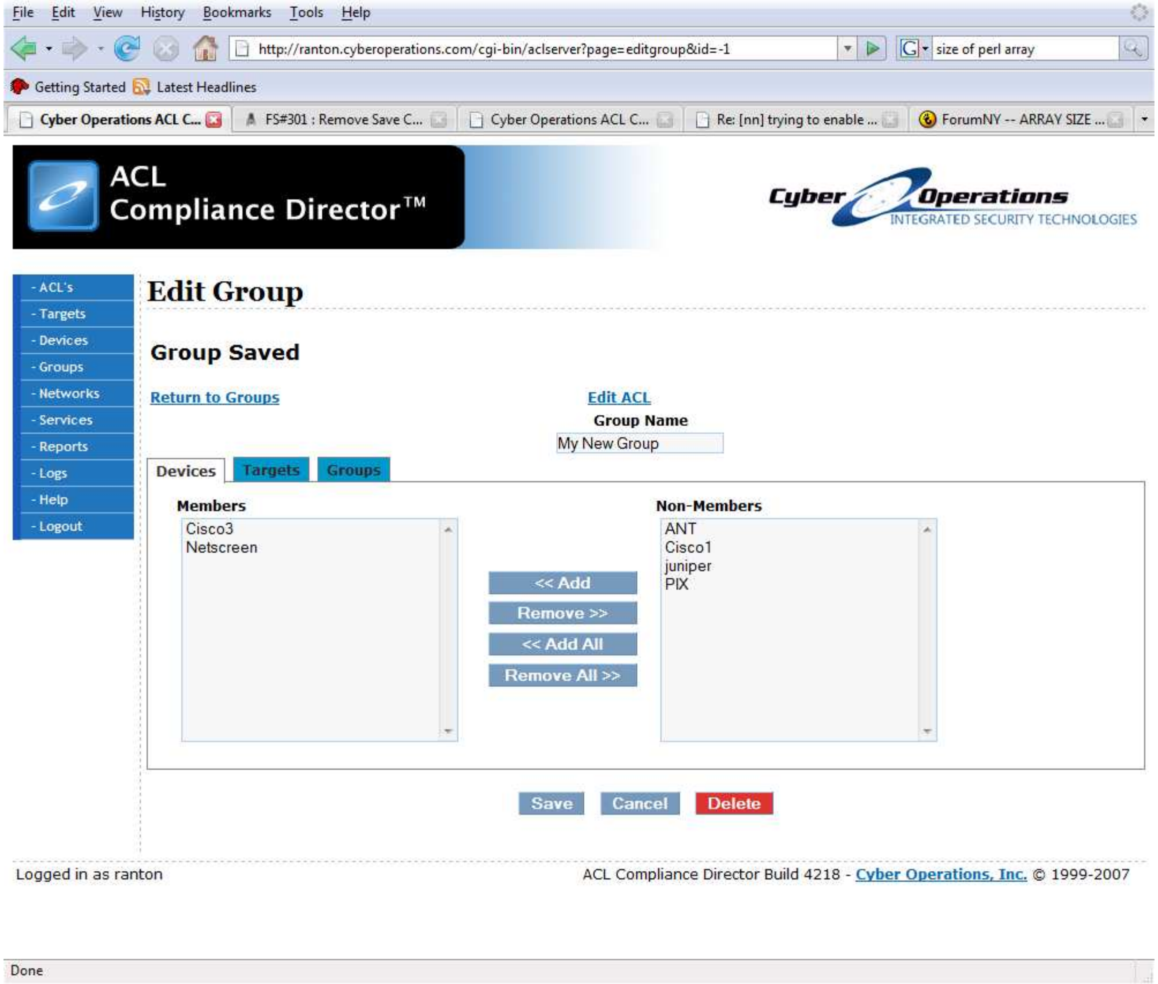
On the “Edit Group” page there are three tabbed areas. The “Devices” area allows you to add or remove devices to your group. The “Targets” area allows you to add or remove targets to your group. Finally, the “Groups” area allows you to add other groups to your group, effectively nesting them within one another.

Within each tabbed area the left area labeled “Members” shows the items that are currently included in the group, and the right area labeled “Non-Members” shows all items that are not included.

To add items select them on the right side under “Non-Members” and click the “Add” button. To remove items select them on the left side under “Members” and click the “Remove” button. You can select multiple items at a time for adding or removing.

You can remove all items from the group or add all items by clicking the “Remove All” or “Add All” buttons respectively.

When you have finished including devices, targets, or other groups in your group click the “Save” button to save your new group.



http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editgroup&id=-1

size of perl array

Edit Group

Group Saved

Group Name: My New Group

Members	Non-Members
Cisco3	ANT
Netscreen	Cisco1
	juniper
	PIX

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 16 - My New Group

Groups each have an associated access list. From the “Edit Group” page this access list can be accessed by clicking the “Edit ACL” link near the top of the page. This will take you to the “Edit ACL” which is discussed in the section “Access Lists” of this manual. The access list for a group is automatically included as a sublist of each member of the group. This means that any access list entry you add to a group's access list is effectively added to the access list of any device or target included in that group, as well as any members of other groups included within that group.

Importing Existing Lists

You can import access lists from Cyber Operations internal format which is used by both ***FLM-ANT*** and ***ACL Manager***, and you can also import lists from Cisco ASA, PIX, and IOS configuration files.

Import from the Edit Entries Page

First you must open the access list you wish to import into. You can create a new list or open an existing list if you wish to append the imported entries to that list.

- Log into ACL Compliance Director if you have not already done so.
- Click the "ACL's" link in the navigation portion on the left of your browser window.
- Either click on one of the links to an existing access list or click "Add New ACL"
- If you are creating a new ACL, enter a name for it and click "Save"
- Click the "Edit Entries" link just below the description text box.
- At the bottom of the "List Entries" page you should see a text box with the caption "File to Upload", a button named "Browse", and an "Import" button.
- Click the browse button, and then select the file you wish to import. This should either be a Cisco configuration file, or an .ACL file from FLM-ANT or ACL Manager.
- Click on the "Import" button once you have chosen the file.
- If you are importing from a Cisco configuration that contains more than one access list you will be given a choice of which ACL to import. Choose the list you wish to import from the drop-down menu when asked.

Using the Importer

If you need to import multiple access lists at a time or need more flexible options then you can use the importer interface by clicking the link "Import Access Lists" from the "Access Lists" page.   See the section "Importing" for more information.

Import Directly from a Device

You can import access lists directly from some types of devices. From the "Edit Device" page of the appropriate device you click the link "Import from Device" and you will be taken to the importer interface, but instead of requesting you to select a file you will be able to import directly from the device.

Dependencies

ACL Compliance Director allows you to view all lists which reference a specific list, service or network.   On the “Access List”, “Edit Network”, and “Edit Service” pages there is a section near the middle of the page title “Referenced By” on the left, with links on the right titled, “Any”, “Lists”, “Targets”, “Devices”, “Groups”. Clicking on any one of these links will take you to the dependency browser page and will show you all lists of the selected type that reference that network, list or service.

For example if you went to the network “My Network” and clicked the “Groups” link across from “Referenced By” you would be shown all group access-lists which contained entries referencing “My Network”. This also includes lists which include sublists that reference “My Network”. Similarly, if you had clicked the “Any” link instead you would see access lists of any type referencing “My Network”

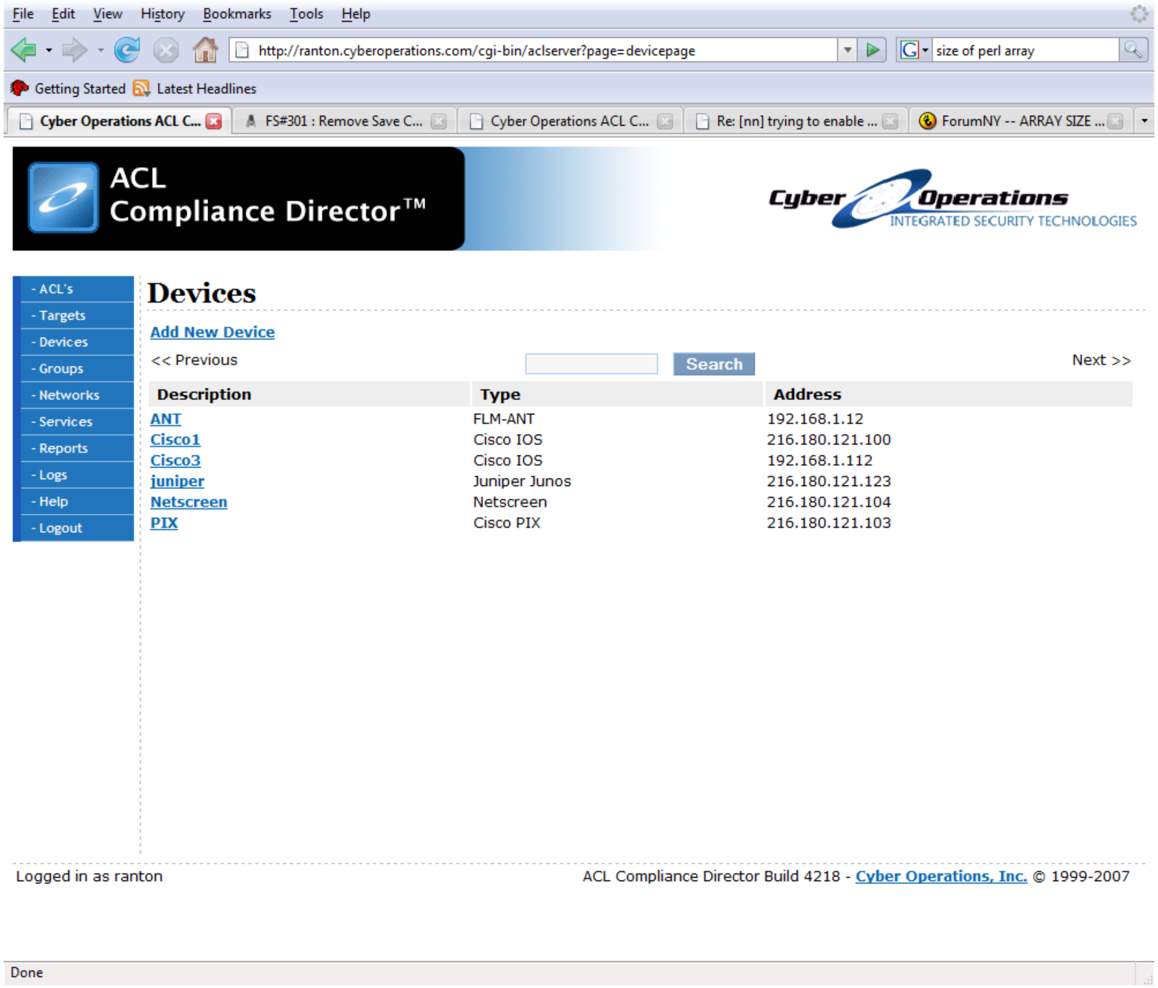
Working with Devices

Devices

Within ***ACL Compliance Director*** a *device* represents a physical networking device such as a router or firewall. For each device a description, internet address, and information required to access the device is maintained in the database.

A device also has an associated ACL which is automatically included as a sublist for each target on the device. You can edit this list to add any entries that you want included for all targets.

The currently configured devices can be viewed by clicking on the “Devices” link in the navigational area on the left of the page. From the “Device” page you can view or edit an existing device by clicking on its name, or you can create a new device by clicking the “Add New Device” link.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=devicepage
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Add New Device
<< Previous
Search
Next >>
Done

Devices

Description	Type	Address
ANT	FLM-ANT	192.168.1.12
Cisco1	Cisco IOS	216.180.121.100
Cisco3	Cisco IOS	192.168.1.112
juniper	Juniper Junos	216.180.121.123
Netscreen	Netscreen	216.180.121.104
PIX	Cisco PIX	216.180.121.103

Logged in as ranton

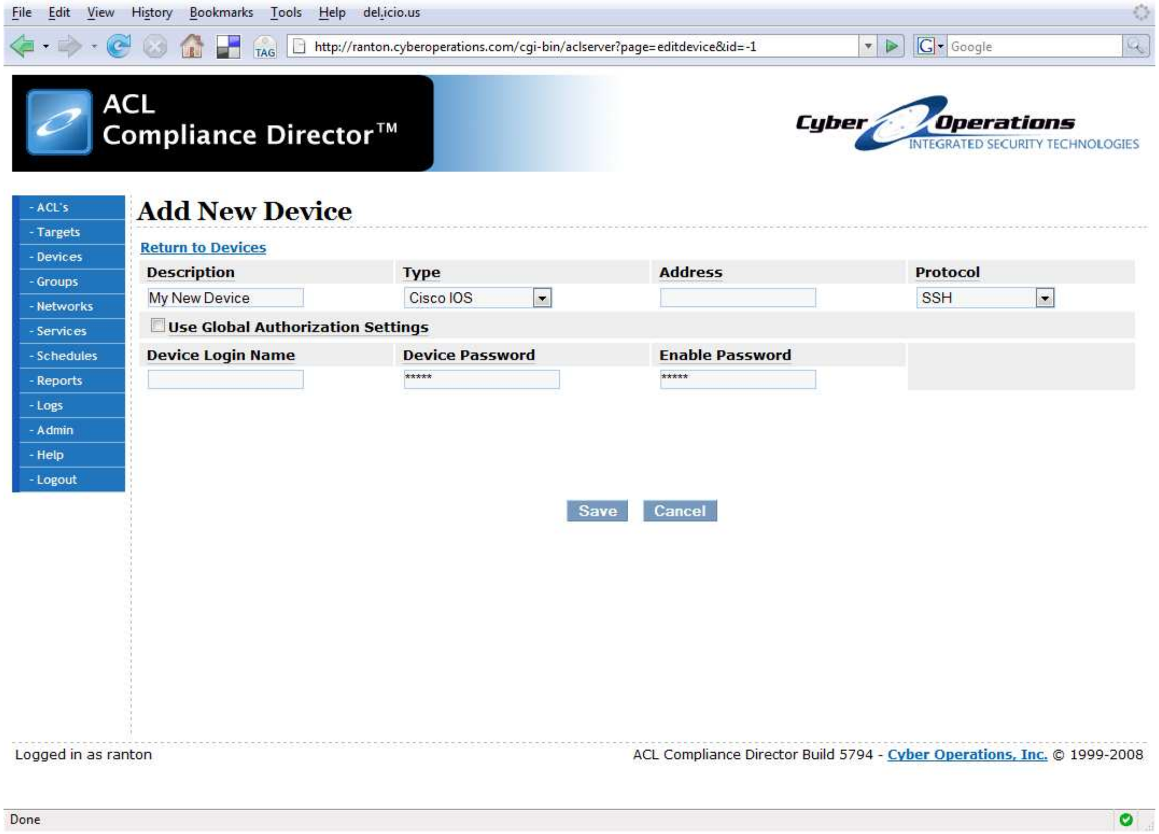
ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 17 - Devices

When you click "Add New Device" you will be taken to a page asking you for the basic configuration values for the device. Below are the fields which you must enter to setup your device.

- **Description** – This will be the name of your device within ***ACL Compliance Director.***
- **Type** – This menu allows you to select one of the supported device types.
- **Address** – This is the network address of the device. Specifically, the address of the interface on the device that ***ACL Compliance Director*** will use to communicate with the device.
- **Protocol** – For some devices, more than one communication protocol for interoperating with the device is supported. Select the protocol that you wish to use to communicate with the device. You must have the device configured to allow this protocol. See the table 'Protocols' for a more complete description of each option.
- **Use Global Authorization Settings** – If this is checked then the global authorization defaults for login name, password, and enable password will be used for this device. The global authorization settings are set on the 'Admin' page of the web interface.

- **Device Login Name –** The login name for the device if not using global authorization settings.
- **Device Password –** Password required when logging into the device if not using global authorization settings.
-
- **Enable Password** – Password to enable management features on the device. This does not apply to all device types. This is only used if not using global authorization settings.
- **Advanced –** This lets you set more advanced configuration options that may also be specific to certain device types.



http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editdevice&id=-1

Add New Device

Return to Devices

Description	Type	Address	Protocol
My New Device	Cisco IOS		SSH

□ Use Global Authorization Settings

Device Login Name	Device Password	Enable Password
	*****	*****

Save Cancel

Logged in as ranton

ACL Compliance Director Build 5794 - Cyber Operations, Inc. © 1999-2008

Done

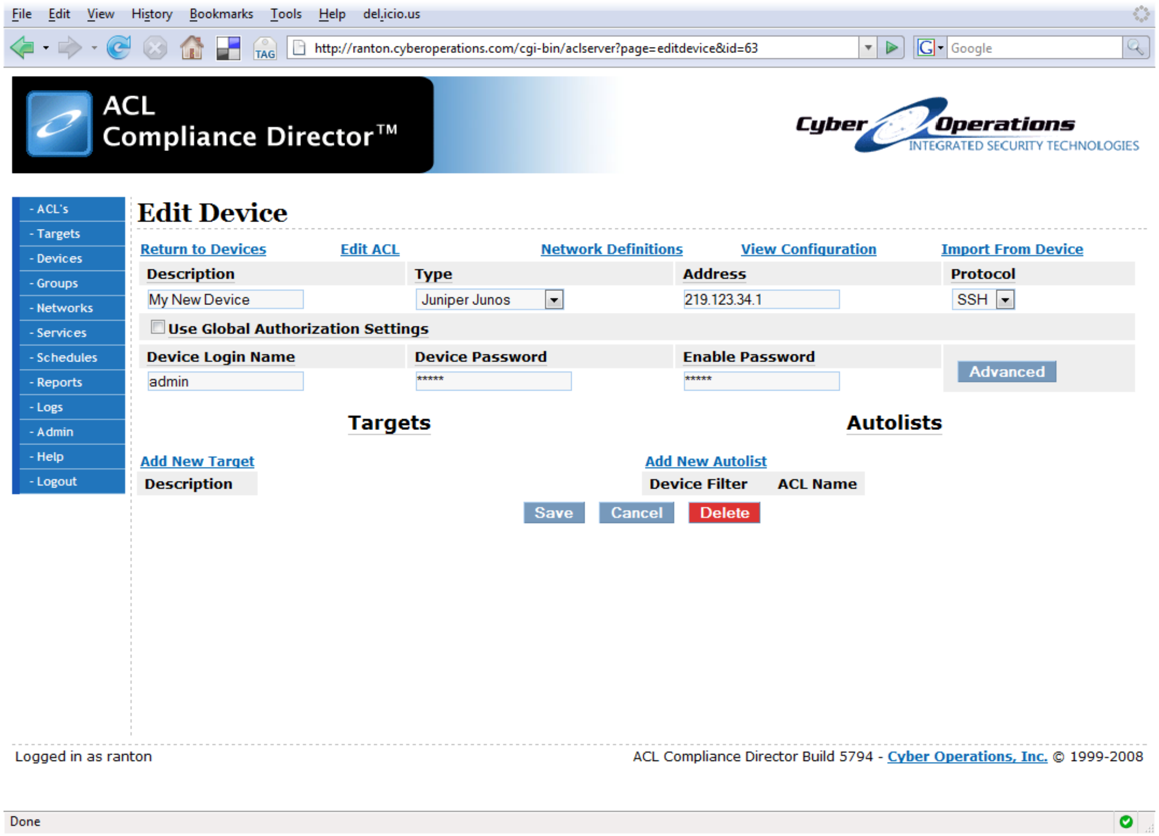
Figure 18 - Add New Device

When you are through entering the values for your device, save it by clicking the "Save" button. In order to send an access list to a device, you must define one or more targets on that device.

Protocols

Protocol	Description
SSH	Communicate with device over SSH terminal connection.
SSH+TFTP	Control device over SSH, but use TFTP for

	transfer of data.
Telnet	Communicate with device over Telnet terminal connection.
Telnet+TFTP	Control device over Telnet, but use TFTP for transfer of data.
SSH+SCP	Control device over SSH, but use SCP(secure copy) for transfer of data. ACL Compliance Director acts as secure copy client, and the device acts as the secure copy server.
SSH+SCP Client	Control device over SSH, but use SCP(secure copy) for transfer of data. ACL Compliance Director acts as secure copy server, and the device acts as the secure copy client.



Description: My New Device
Type: Juniper Junos
Address: 219.123.34.1
Protocol: SSH

☐ Use Global Authorization Settings

Device Login Name: admin
Device Password: *****
Enable Password: *****

Logged in as ranton

ACL Compliance Director Build 5794 - Cyber Operations, Inc. © 1999-2008

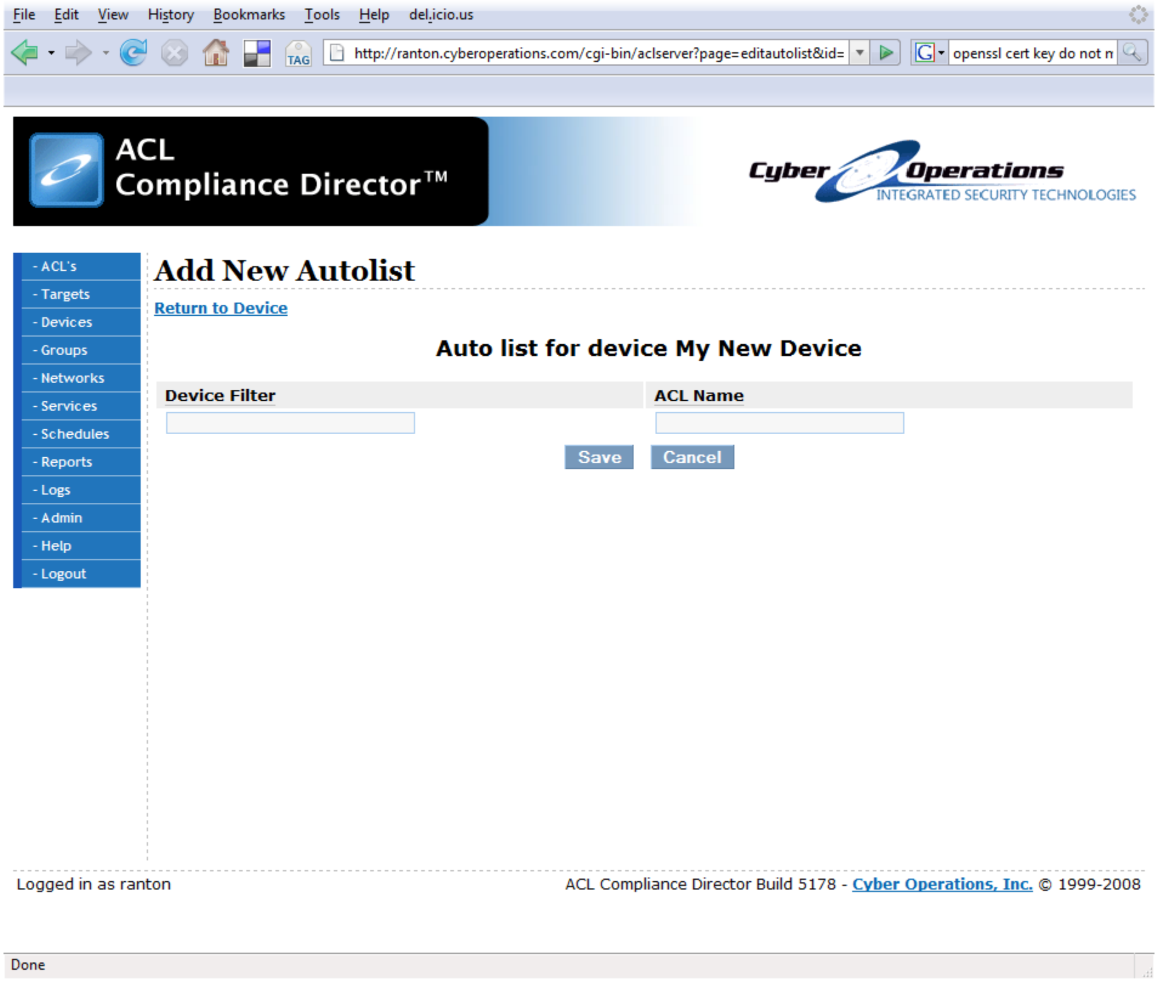
Figure 19 - Edit Device

Autolists

Creating an **Autolist** for a device allows you to have the list automatically imported by the **acdscheduler** daemon whenever it is modified to a list within the system. Autolists

are shown at the lower right hand side of the device page of the device the corresponding device.
In order to create an Autolist, you need only click the “Add New Autolist” link on the device’s page, and then enter the name of the access-list or filter on the device in the “Device Filter” field and the name you want the imported list to have in the “ACL Name” field.

NOTE: Autolists are imported at regular intervals by the **acdscheduler** daemon so you will not see changes take effect immediately. The time between these checks is controlled by the “autoImportInterval” configuration entry and defaults to twenty minutes.



Add New Autolist

Return to Device

Auto list for device My New Device

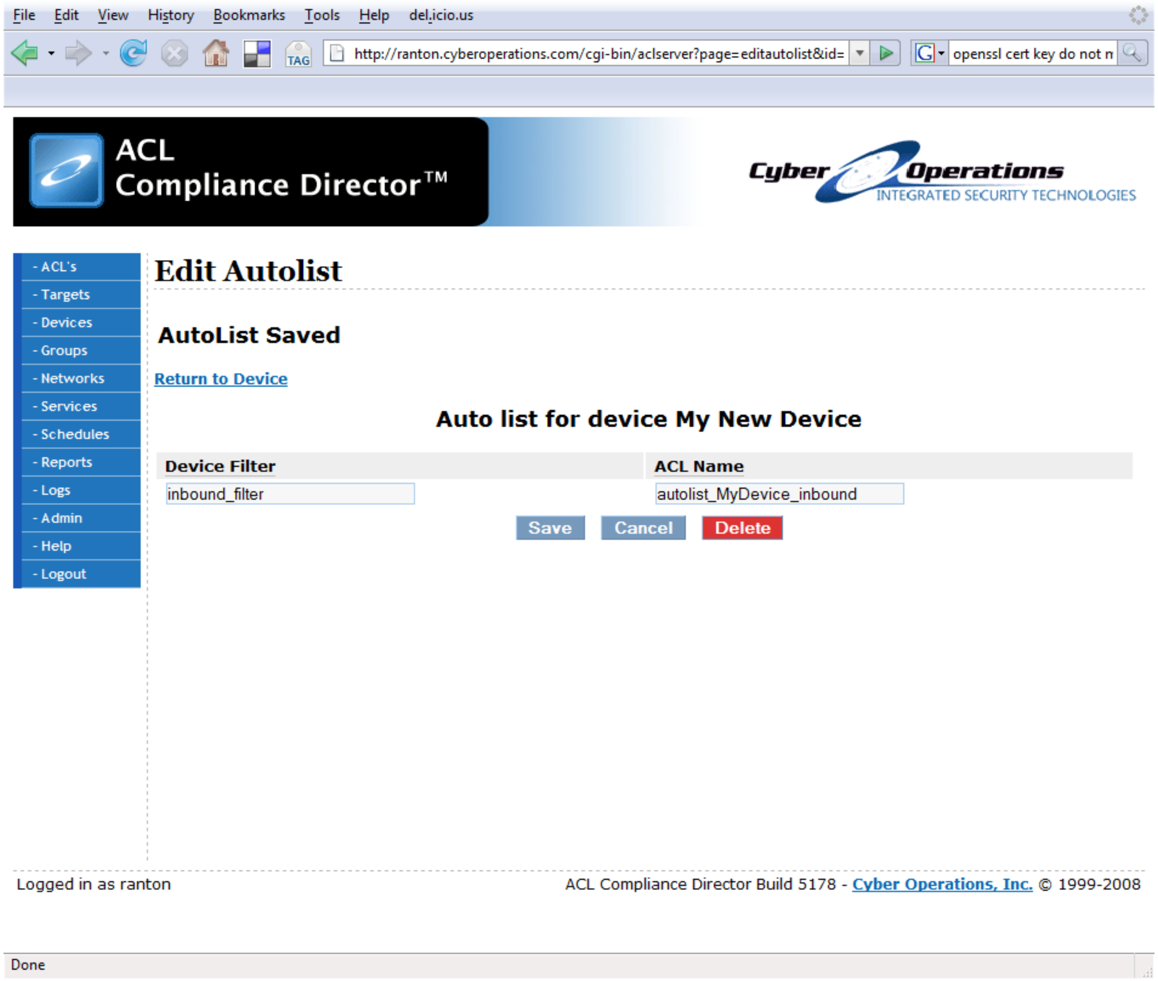
Device Filter	ACL Name

Logged in as ranton

ACL Compliance Director Build 5178 - Cyber Operations, Inc. © 1999-2008

Figure 20 - Add New Autolist

To change the settings for an autolist simply click on its link from the “Edit Device” page. Then make your changes and click the “Save” button.


File Edit View History Bookmarks Tools Help del.icio.us
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=editautolist&id=
openssl cert key do not n
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Schedules
- Reports
- Logs
- Admin
- Help
- Logout
Save
Cancel
Delete
Done

Edit Autolist

AutoList Saved

Return to Device

Auto list for device My New Device

Device Filter	ACL Name
inbound_filter	autolist_MyDevice_inbound

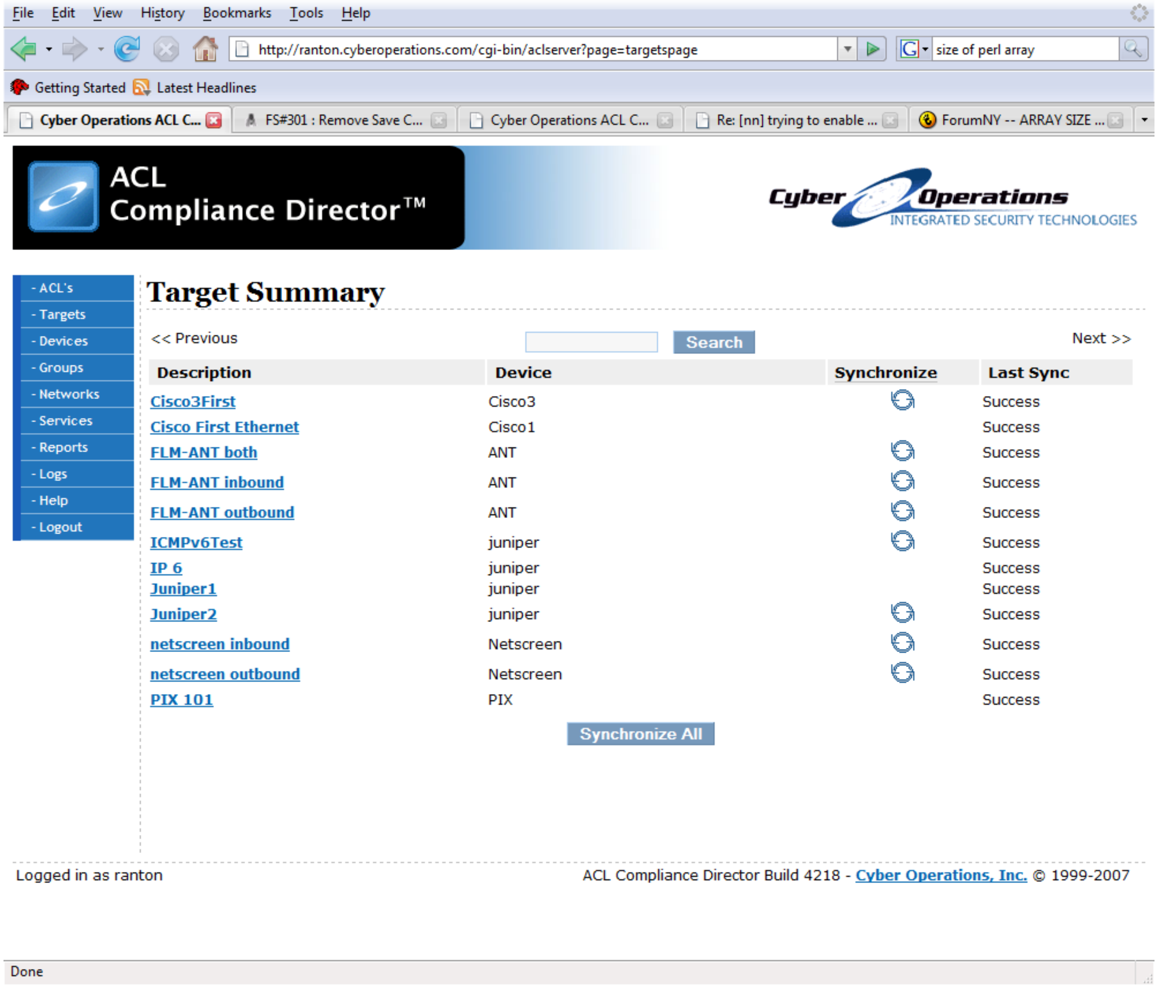
Logged in as ranton

ACL Compliance Director Build 5178 - Cyber Operations, Inc. © 1999-2008

Figure 21 - Edit Autolist

Targets

A target represents an interface and/or named ACL or filter on a device which can be used as a target for synchronization. Whether a specific network interface is specified as part of a target depends on the type of device the target is on.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=targetspage
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
<< Previous
Search
Next >>
Synchronize All
Done

Target Summary

Description	Device	Synchronize	Last Sync
Cisco3First	Cisco3	⟳	Success
Cisco First Ethernet	Cisco1		Success
FLM-ANT both	ANT	⟳	Success
FLM-ANT inbound	ANT	⟳	Success
FLM-ANT outbound	ANT	⟳	Success
ICMPv6Test	juniper	⟳	Success
IP 6	juniper		Success
Juniper1	juniper		Success
Juniper2	juniper	⟳	Success
netscreen inbound	Netscreen	⟳	Success
netscreen outbound	Netscreen	⟳	Success
PIX 101	PIX		Success

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

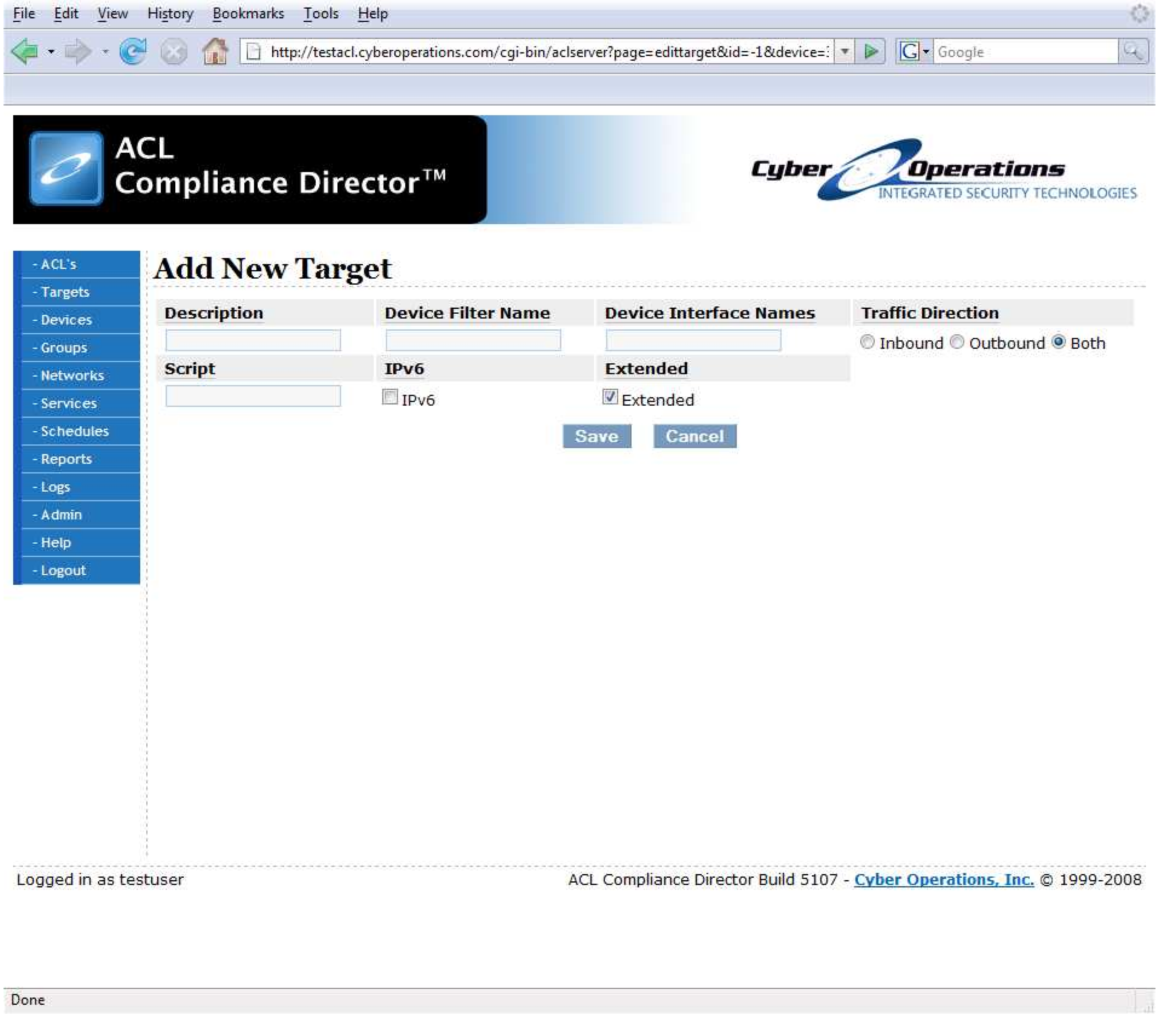
Figure 22 - Targets

A target has an associated ACL which allows you to control the access list entries which are sent to the device each time it is synchronized. The device list of the parent device of the target is automatically included as a sublist in the target list. You can add entries directly to the target list, or you can include other access lists as sublists.

Clicking the "Add New Target" link from the "Edit Device" page will take you to a page asking you for the values for your target. The values needed to define your target are:

- Description – The name of your target in ***ACL Compliance Director.***
- Device Filter Name – This is the name that the deployed access list will have on the device. The list is simply created with this name and you can configure your device to apply it however you choose and use ***ACL Compliance Director*** to maintain the list itself.
- Device Interface Names – On device types where you must deploy the list to a specific network interface this entry is where you specify them.
- Script - The device script for your target. See the section "Device Scripts" for more information on this field.
- IPv6 – If this box is checked lists will be deployed to the device preserving as much IPv6 specific data as possible. If this is not checked then any IPv6

addresses within lists sent to the device will be down converted to IPv4 as accurately as possible. IPv6 is not supported by all device types.



Add New Target

Description	Device Filter Name	Device Interface Names	Traffic Direction
			○ Inbound ○ Outbound ● Both
Script	**IPv6**	**Extended**	
	□ IPv6	☑ Extended	

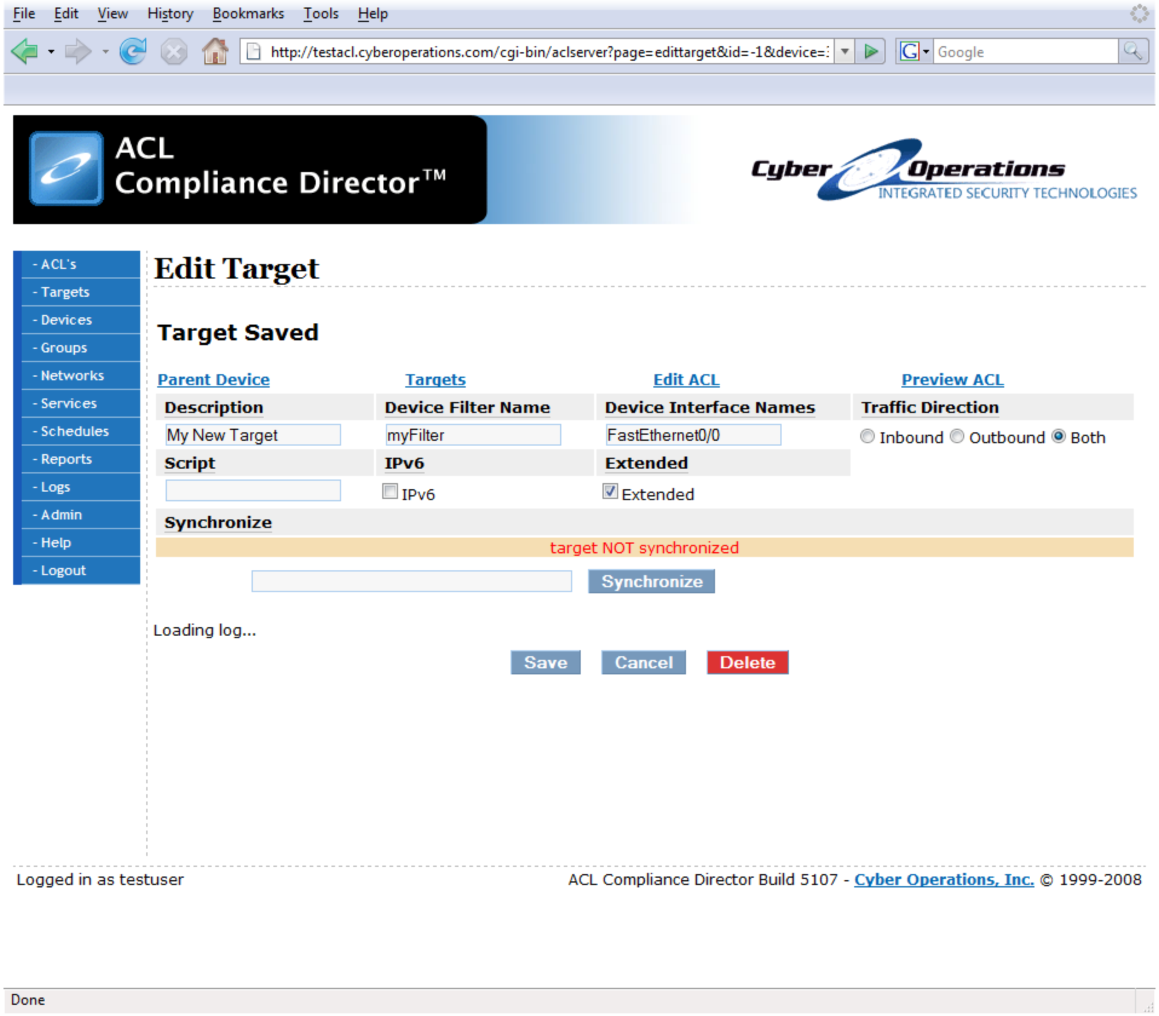
Logged in as testuser

ACL Compliance Director Build 5107 - Cyber Operations, Inc. © 1999-2008

Figure 23 - Add New Target

Targets also support specifying a *device script*. A device script is a command you specify which can modify the access list for the device before it is sent to the device during synchronization. Device scripts are specified per target on the device. The device script must be an executable command on the server running ***ACL Compliance Director***. When the device script is called it will be passed the list, in the native syntax of the device as standard input via a UNIX pipe, and the output of the device script written to standard out will be used by ***ACL Compliance Director*** as the modified version of an access list to be sent to the device.

The directory **/usr/local/acd/sample_dev_scripts** contains some example device scripts for your convenience.



http://testacl.cyberoperations.com/cgi-bin/aclserver?page=edittarget&id=-1&device=

Edit Target

Target Saved

Description	Device Filter Name	Device Interface Names	Traffic Direction
My New Target	myFilter	FastEthernet0/0	○ Inbound ○ Outbound ● Both
Script	**IPv6**	**Extended**	
	□ IPv6	☑ Extended	

Synchronize

target NOT synchronized

Loading log...

Logged in as testuser

ACL Compliance Director Build 5107 - Cyber Operations, Inc. © 1999-2008

Figure 24 - My New Target

Device Type Specifics

The “Device Filter Name” and “Device Interface Names” take on different meanings depending on the type of parent device.

Device Type	Device Filter Name	Device Interface Names
Juniper JunOS	Specifies the firewall filter that will be created or modified in the JunOS configuration.	Not used.
Cisco IOS Cisco PIX Cisco ASA/PIX 7.x Aruba Force10 FTOS	Specifies the name of the access-list that will be created or modified in the IOS configuration.	Only used if device Protocol is “Telnet” or “SSH” and the “Device Interface Names” field is not blank, in which case it

Force10 E-Series Force10 SFTOS		specifies the router interface for a “ip access-group” or “ipv6 traffic-filter” command to be inserted into the interface configuration.
Netscreen	Not used.	Interface must specify the source and destination “zones”f or the access list rules to apply to in the form <srczone>:<dstzone>.

Figure 25 – Device Filter Name Usage

Dummy Devices

The device type ‘Dummy Device’ is a special type of device used for testing and experimenting with access-list policies when you do not want to use an actual network device. The device configuration page of a dummy device returns the last access-list deployed to a target on the device in the native syntax of ***ACL Compliance Director***.

Rotating Device Filter Names

For Cisco IOS, PIX, ASA, Aruba, and all Force 10 device types, it is possible to rotate the access-list used on the device. To take advantage of this feature simply enter the two access-list names you would like to use separated by a colon “:” in the “Device Filter” field.

Additionally, if you enter two numeric values or two names both ending in a number, then ***ACL Compliance Director*** will rotate through all the intermediate numbers as well.

Here are some examples:

firstName:secondName – Synchronizations will alternate between “firstName” and “secondName” as the access-list name on the device.
101:109 – Synchronizations will cycle through 101, 102, etc. all the way through 109 then wrap back around to 109.
basename1:basename100 – Synchronization will start with basename1 then cycle through basename2, basename3, etc. all the way through basename100 before wrapping back to basename1.

IP v6 Access-Lists

For devices which support it, the ‘IPv6’ checkbox selects whether an IPv6 or IPv4 access-list is generated for the target.

Standard versus Extended Access-Lists on IOS Devices

The ‘Extended’ option applies only to Cisco IOS and Aruba devices, and a standard access list is generated if this option is not checked. Also, if you specify a number for the access-list name, and this number falls into the ranges used by Cisco IOS for numbered, standard access-lists, then a standard access-list will be generated instead of an extended list, regardless of the setting of the ‘Extended’ checkbox.

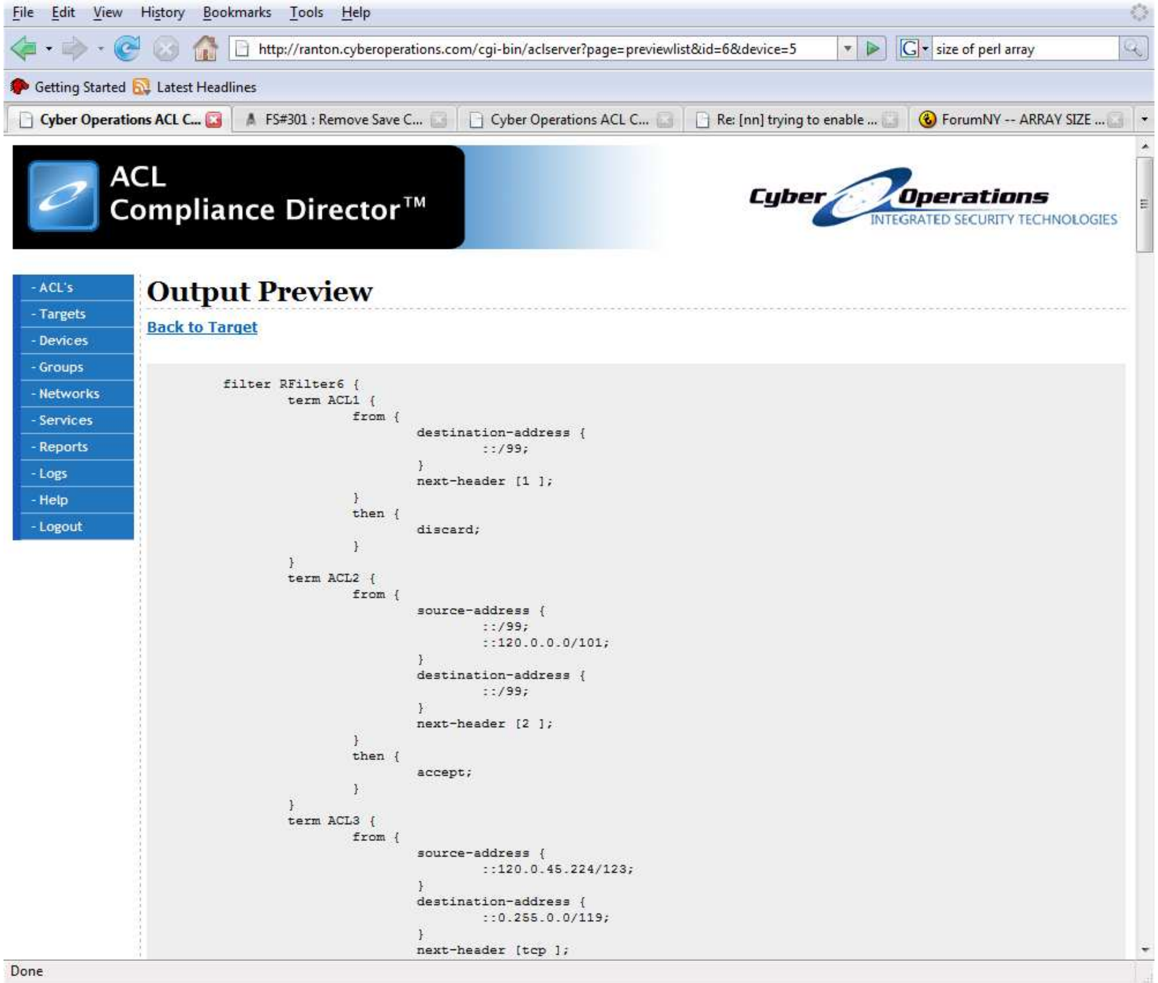
Standard access lists allow limiting traffic only based on the source address.

Traffic Direction

If the device protocol is ‘SSH’ or ‘Telnet’ and the device type is either Cisco IOS, Cisco ASA/PIX 7.x, or Aruba, then the Traffic Direction radio items will control whether the access-list is applied to inbound, outbound, or all (both) traffic.

Previewing Lists

It is possible to preview the device specific syntax generated for a target’s access list without sending it to the device. To do so, you simply click the “Preview ACL” link near the top right of the “Edit Target” page for the appropriate target. This will take you to a page containing the textual list data that would be sent to the target during an actual synchronization so that you can preview any changes you have made.


File
Edit
View
History
Bookmarks
Tools
Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=previewlist&id=6&device=5
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Done

Output Preview

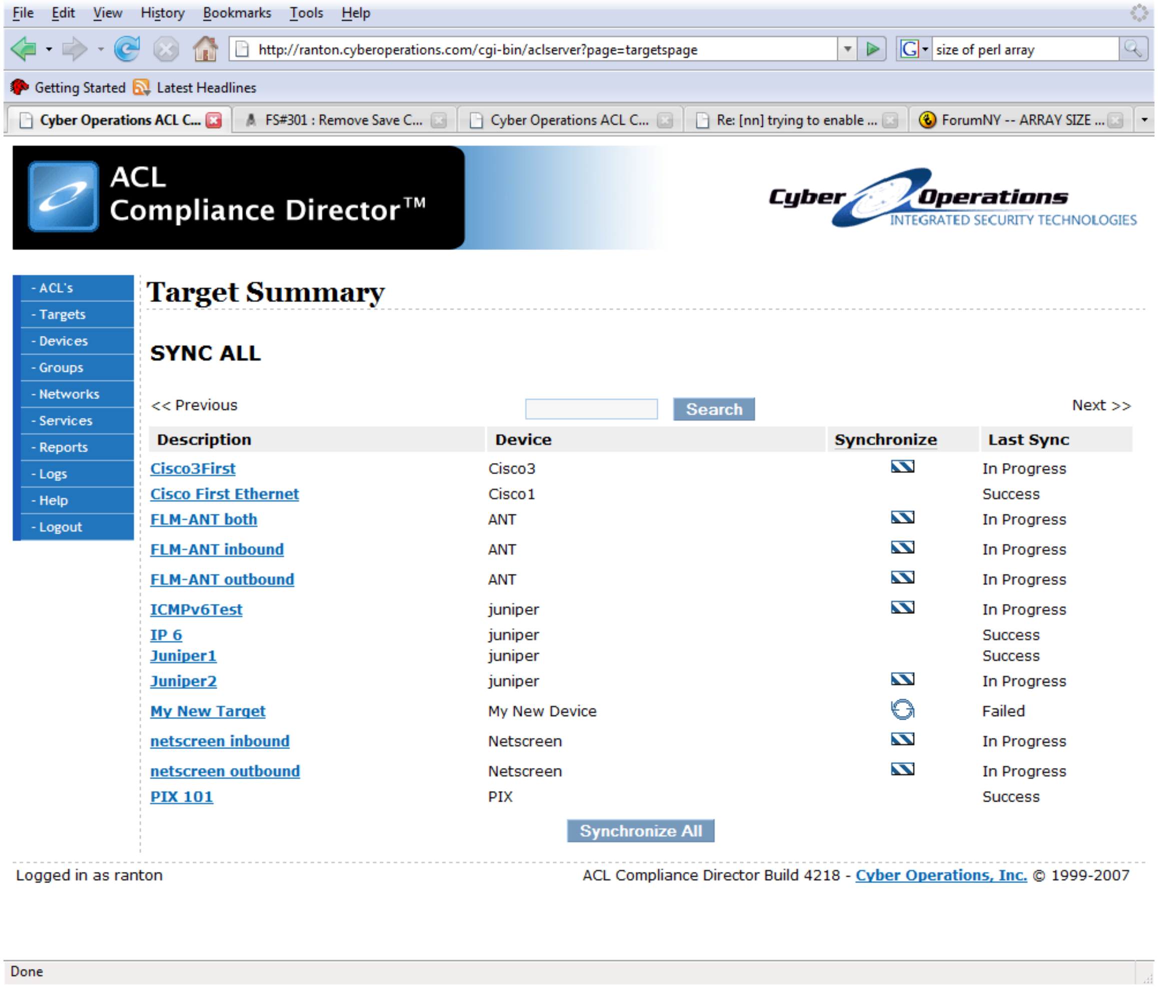
Back to Target

```
filter RFilter6 {
        term ACL1 {
                from {
                        destination-address {
                                ::/99;
                        }
                        next-header [1 ];
                }
                then {
                        discard;
                }
        }
        term ACL2 {
                from {
                        source-address {
                                ::/99;
                                ::120.0.0.0/101;
                        }
                        destination-address {
                                ::/99;
                        }
                        next-header [2 ];
                }
                then {
                        accept;
                }
        }
        term ACL3 {
                from {
                        source-address {
                                ::120.0.45.224/123;
                        }
                        destination-address {
                                ::0.255.0.0/119;
                        }
                        next-header [tcp ];
```

Figure 26 - Preview ACL

Synchronizing

Within ***ACL Compliance Director***, synchronization is the sending of the appropriate access list or lists to a target or targets. For each target and its access list the system maintains synchronization times and modification times so that the system knows if a list or any of its sublists or any networks or services it references have been modified since the last time the target was synchronized. When viewing the “Targets” page, each target that needs to be synchronized will have an icon in the “Synchronize” column that looks like a circle with two arrows. Clicking on the synchronize icon for a target will begin the synchronization process for that target. All synchronizations take place in separate processes from the interface, so you can continue your work within ***ACL Compliance Director*** while targets are being synchronized. Any target that is currently being synchronized will show a barber pole type progress animation in the “Synchronize” column.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=targetspage
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
<< Previous
Search
Next >>
Synchronize All
Done

Target Summary

SYNC ALL

Description	Device	Synchronize	Last Sync
Cisco3First	Cisco3	▨	In Progress
Cisco First Ethernet	Cisco1		Success
FLM-ANT both	ANT	▨	In Progress
FLM-ANT inbound	ANT	▨	In Progress
FLM-ANT outbound	ANT	▨	In Progress
ICMPv6Test	juniper	▨	In Progress
IP 6	juniper		Success
Juniper1	juniper		Success
Juniper2	juniper	▨	In Progress
My New Target	My New Device	⟳	Failed
netscreen inbound	Netscreen	▨	In Progress
netscreen outbound	Netscreen	▨	In Progress
PIX 101	PIX		Success

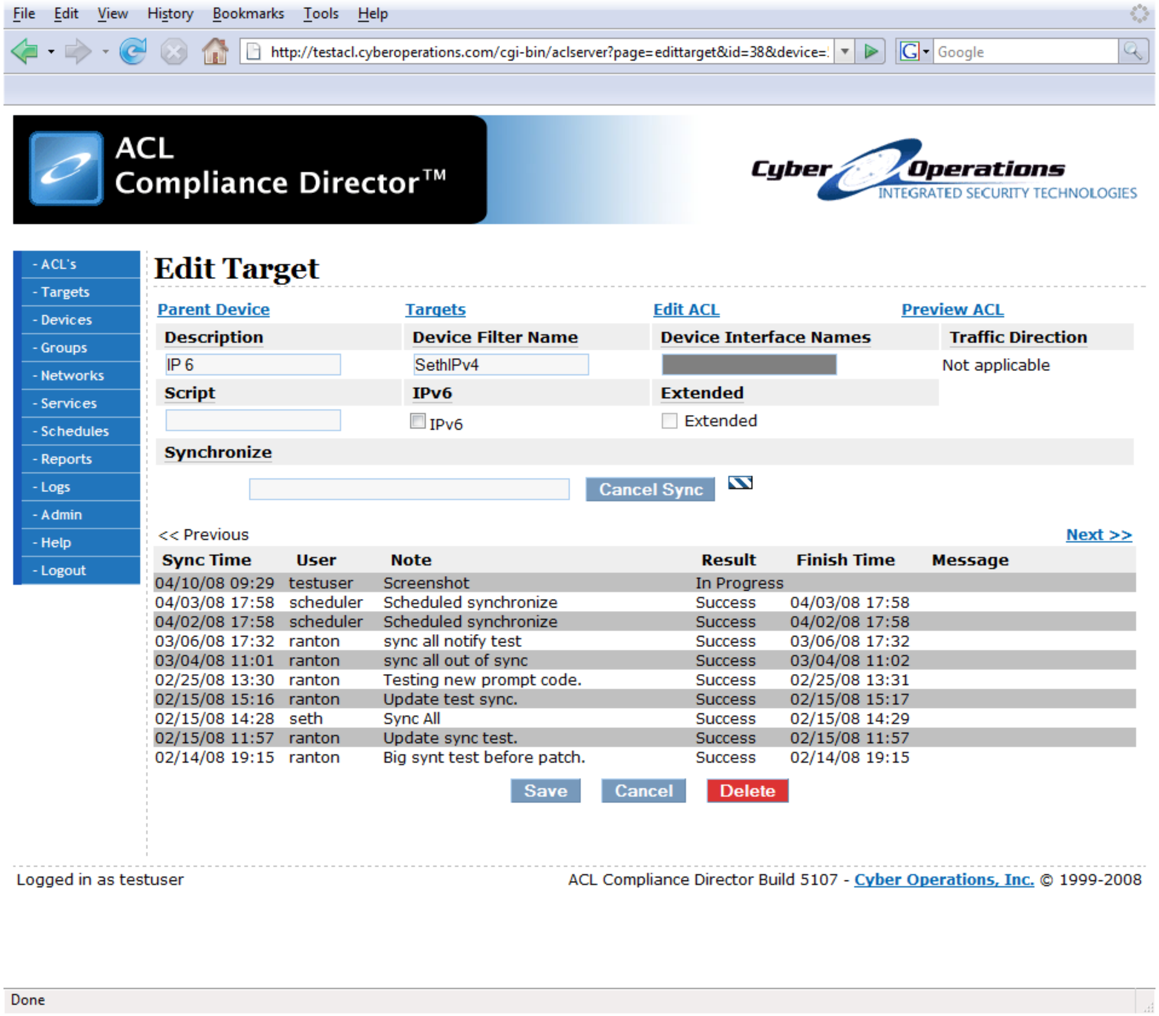
Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 27 - Synchronizing

If you view a target in the "Edit Target" page by clicking its name from the "Target" page or from its parent's "Edit Device" page you will see a horizontal are stating "Target not synchronized" if the target is not up to date with its access list. Below that you will see a text field and a "Synchronize" button. The text field allows you to enter an optional comment for the deploy log when synchronizing, and the "Synchronize" button starts the deployment in the background in the same manner as clicking the sync icon on the "Targets" page would.

When synchronization is in progress the "Synchronize" button on the "Edit Target" page will be replaced by a "Cancel Sync" button with a barber pole type progress indicator next to it.



Edit Target

Parent Device | Targets | Edit ACL | Preview ACL

Description	Device Filter Name	Device Interface Names	Traffic Direction
IP 6	SethIPv4		Not applicable
Script	**IPv6**	**Extended**	
	□ IPv6	□ Extended	

Synchronize

Sync Time	User	Note	Result	Finish Time	Message
04/10/08 09:29	testuser	Screenshot	In Progress		
04/03/08 17:58	scheduler	Scheduled synchronize	Success	04/03/08 17:58	
04/02/08 17:58	scheduler	Scheduled synchronize	Success	04/02/08 17:58	
03/06/08 17:32	ranton	sync all notify test	Success	03/06/08 17:32	
03/04/08 11:01	ranton	sync all out of sync	Success	03/04/08 11:02	
02/25/08 13:30	ranton	Testing new prompt code.	Success	02/25/08 13:31	
02/15/08 15:16	ranton	Update test sync.	Success	02/15/08 15:17	
02/15/08 14:28	seth	Sync All	Success	02/15/08 14:29	
02/15/08 11:57	ranton	Update sync test.	Success	02/15/08 11:57	
02/14/08 19:15	ranton	Big synt test before patch.	Success	02/14/08 19:15	

Logged in as testuser

ACL Compliance Director Build 5107 - Cyber Operations, Inc. © 1999-2008

Figure 28 - Synchronize from Edit Target

When synchronization begins a deployment log entry will be added for the target indicating that it has a deployment in progress showing the user initiating the action and any comment they entered. Upon completion, cancellation, or failure of synchronization to a target the deployment log entry will updated to indicate the result and the message. The result will either be "Success" or "Failed". Cancelled synchronizations are marked failed. The "Message" field contains the text "Cancelled" for cancellations, and for errors it will contain the text of any error messages indicating what problems occurred.

Management Features

Schedules

You can schedule synchronizations to take place at a later date or time or on a recurring schedule. To view the scheduled synchronizations click on the "Schedules" link in the navigation al area on the left of the page.

Simply click “Add New Schedule” to create a new scheduled synchronization. You will be prompted to enter a name for the Schedule, select the target(or all targets) that the schedule applies to, and a date for the schedule to begin. If you click the “Recurring Schedule” checkbox then you will also need to set the interval which can be either hourly, daily, weekly, monthly, or other which allows you to specify a number of minutes between synchronizations.

When entering the “Date/Time” value you can enter relative amounts of time from the present. For example you could enter “+1day” to schedule a synchronization 24 hours away. Or you could enter “+30mins” or “+2hours”.

If you click on the name of a Schedule on the “Schedules” page then you will be able to change any of the values for an existing schedule or delete that schedule.

NOTE: You should be aware that scheduled synchronization depends on the **acdscheduler** daemon running.

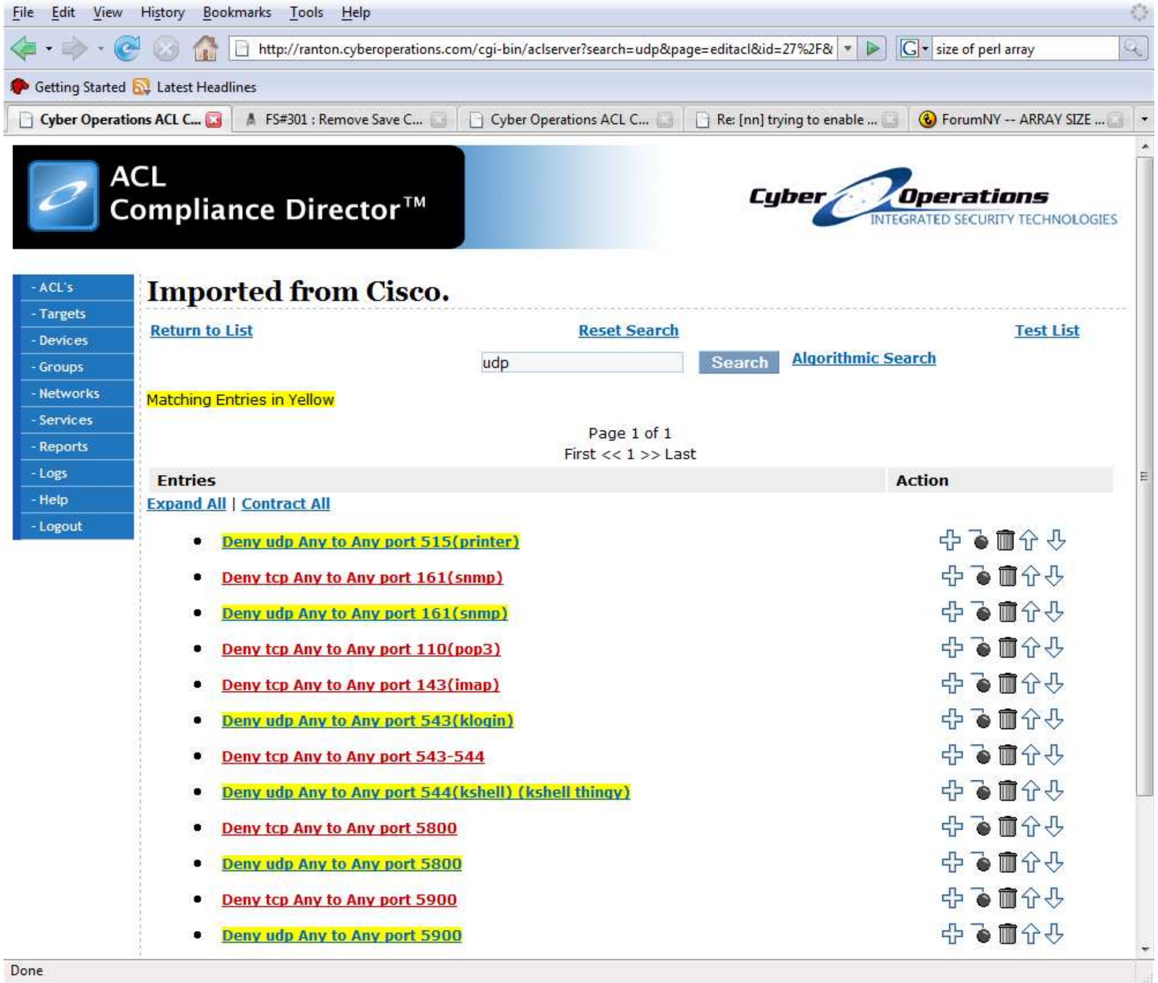
Searching

There are two different types of searches supported by the system. Textual searches allow you to search the textual representation of a list, and advanced searches allow you to search list entries based on specific parameters for entry fields.

Textual Searches

The textual search feature allows you to regular expressions to search the textual representation of the list entries. The regular expressions syntax used is that of POSIX 1003.2, and all expression matching is case insensitive. To search within a list, you must be on the “List Entries” page of the appropriate list. Enter the string or regular expression you wish to search for in the text field to the left of the “Search” button; then click “Search”. All matching entries will be hilited with a yellow background. Below are some examples of regular expression for searching:

- **permit.*udp** – This would match any entry containing the text “udp” somewhere after the text “permit”. The ‘.’ Represents a wildcard matching any character, and the ‘*’ indicates match zero or more of the preceding value.
- **port** – This would simply match any entry containing the port keyword.
- **(tcp)|(udp)** – This would match all entries containing the word “tcp” or the word “udp”


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?search=udp&page=editacl&id=27%2F&
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL
Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Return to List
Reset Search
Test List
Search
Algorithmic Search
Expand All | Contract All
Done

Imported from Cisco.

udp

Matching Entries in Yellow

Page 1 of 1
First << 1 >> Last

Entries	Action
Deny udp Any to Any port 515(printer)	
Deny tcp Any to Any port 161(snmp)	
Deny udp Any to Any port 161(snmp)	
Deny tcp Any to Any port 110(pop3)	
Deny tcp Any to Any port 143(imap)	
Deny udp Any to Any port 543(klogin)	
Deny tcp Any to Any port 543-544	
Deny udp Any to Any port 544(kshell) (kshell thingy)	
Deny tcp Any to Any port 5800	
Deny udp Any to Any port 5800	
Deny tcp Any to Any port 5900	
Deny udp Any to Any port 5900	

Figure 29 - Textual Search

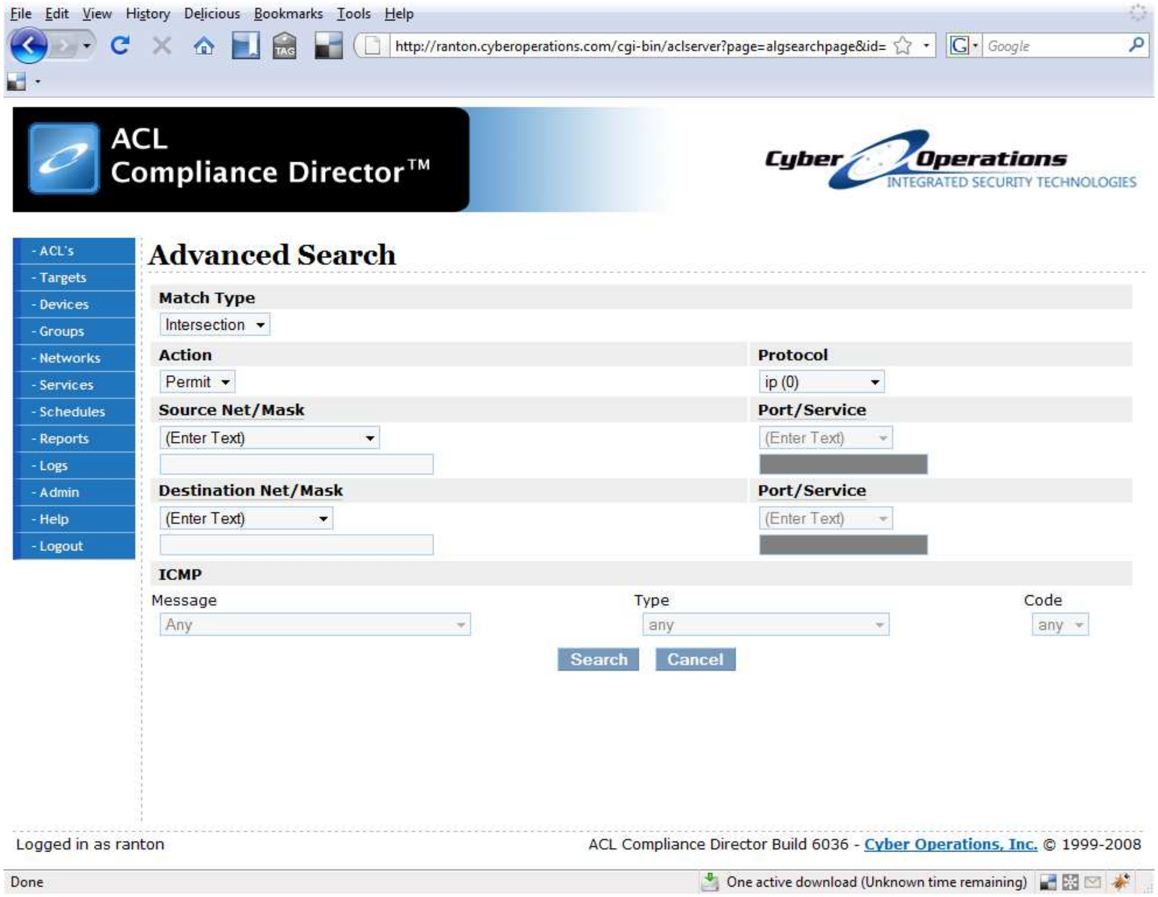
Advanced Search

From the “List Entries” page the “Advanced Search” link near the top takes you to the “Advanced Search” page where you can specify ACL entry values to match against entries in the list while searching. All fields are the same as the fields from the “Edit Entry” page where you define access list entry values with the exceptions that there are no search fields for “Log”, “Reflect”, “Evaluate Reflect”, or “Established”, and at the top there is an additional field named “Match Type” where you specify the relationship the entry must have to the search values to be considered a match. The choices are:

- **Intersection** – If there is any overlap between the entry and the search settings the entry will be considered a match. For example, TCP and UDP do not intersection, but IP and TCP do, and 192.168.1.0 and 10.0.0.0 do not intersect, but 192.168.0.0/16 and 192.168.1.0/24 do intersect.
- **Superset** – The list entry must be a superset of the search values to match. This means that each value must be the same or less restrictive in the list entry. For example, IP is a superset of TCP as a protocol, and 192.168.0.0/16 is a superset of 192.168.1.0/24 as a Source Net/Mask.

- **Subset –** This is the opposite of superset, meaning that the search values must be a superset of the list entry values.
- **Exact –** Only match entries that match each field in the search parameters exactly.

Any field not specified on the “Advanced Search” page defaults to include any value, meaning that leaving “Source Net/Mask” or “Destination Net/Mask” blank defaults to any source or destination address, and that leaving “Port/Service” blank defaults to any port.


File Edit View History Delicious Bookmarks Tools Help
Google
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Schedules
- Reports
- Logs
- Admin
- Help
- Logout
Search
Cancel
Done
One active download (Unknown time remaining)

http://ranton.cyberoperations.com/cgi-bin/aclserver?page=algsearchpage&id=

Advanced Search

Match Type: Intersection

Action: Permit

Protocol: ip (0)

Source Net/Mask: (Enter Text)

Port/Service: (Enter Text)

Destination Net/Mask: (Enter Text)

Port/Service: (Enter Text)

ICMP

Message: Any

Type: any

Code: any

Logged in as ranton

ACL Compliance Director Build 6036 - Cyber Operations, Inc. © 1999-2008

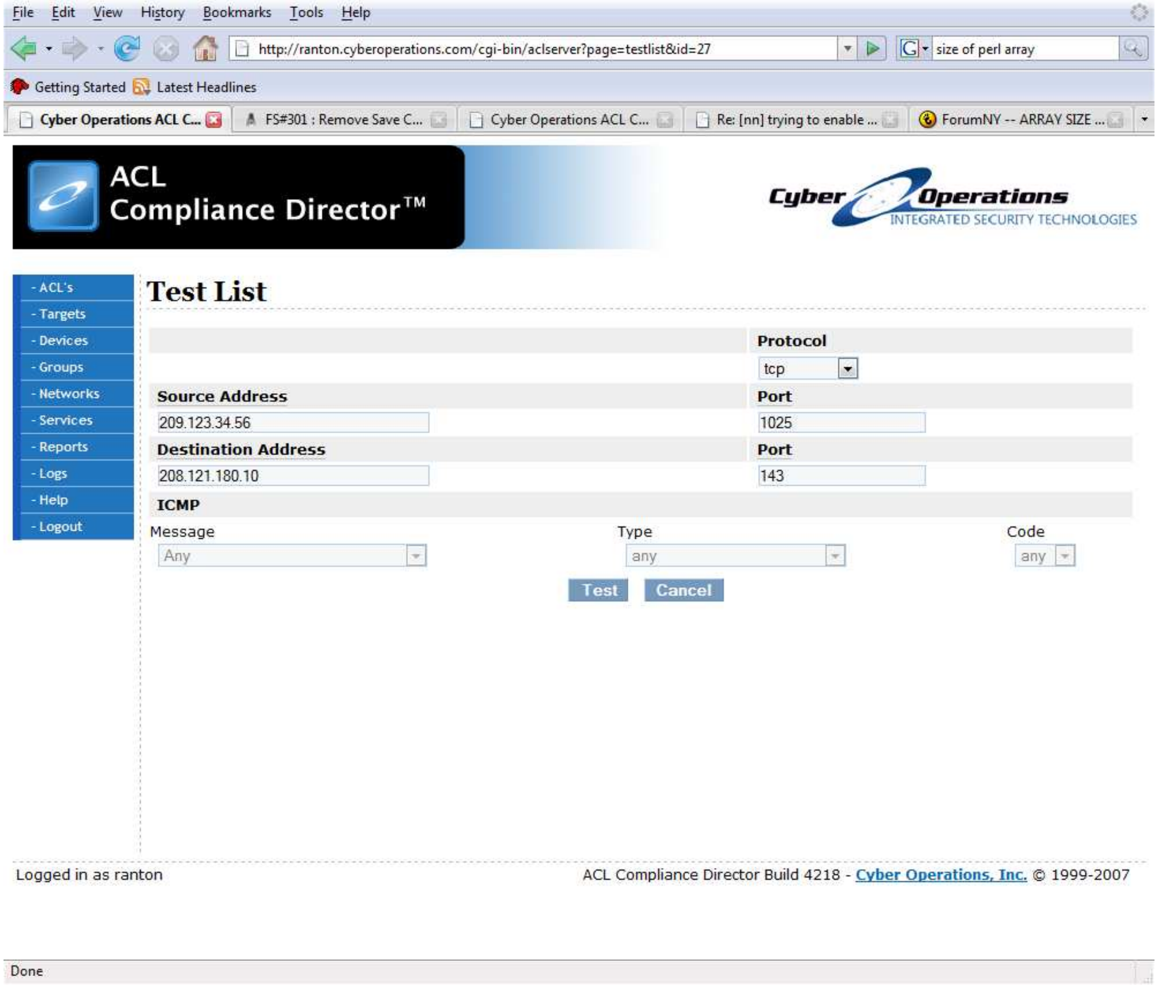
Figure 30 - Advanced Search

Once you have entered all of your search parameters click the “Search” button and you will be returned to the “List Entries” page with all matching entries highlighted in yellow.

Testing

ACL Compliance Director includes a feature which allows you to test what would happen to a theoretical packet as it is processed by an access list. Clicking the “Test List” link from the top right of the “List Entries” page of an access list will take you to the “Test List” page where you will be asked to enter some basic information for you test case.

Select the protocol and enter the source and destination internet addresses. If the protocol you selected was TCP or UDP you must enter source and destination ports for your test case as well. If you selected ICMP as the protocol you must select the ICMP message, type, and code values from the menus.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=testlist&id=27
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Test
Cancel
Done

Test List

Protocol: tcp

Source Address: 209.123.34.56 Port: 1025

Destination Address: 208.121.180.10 Port: 143

ICMP

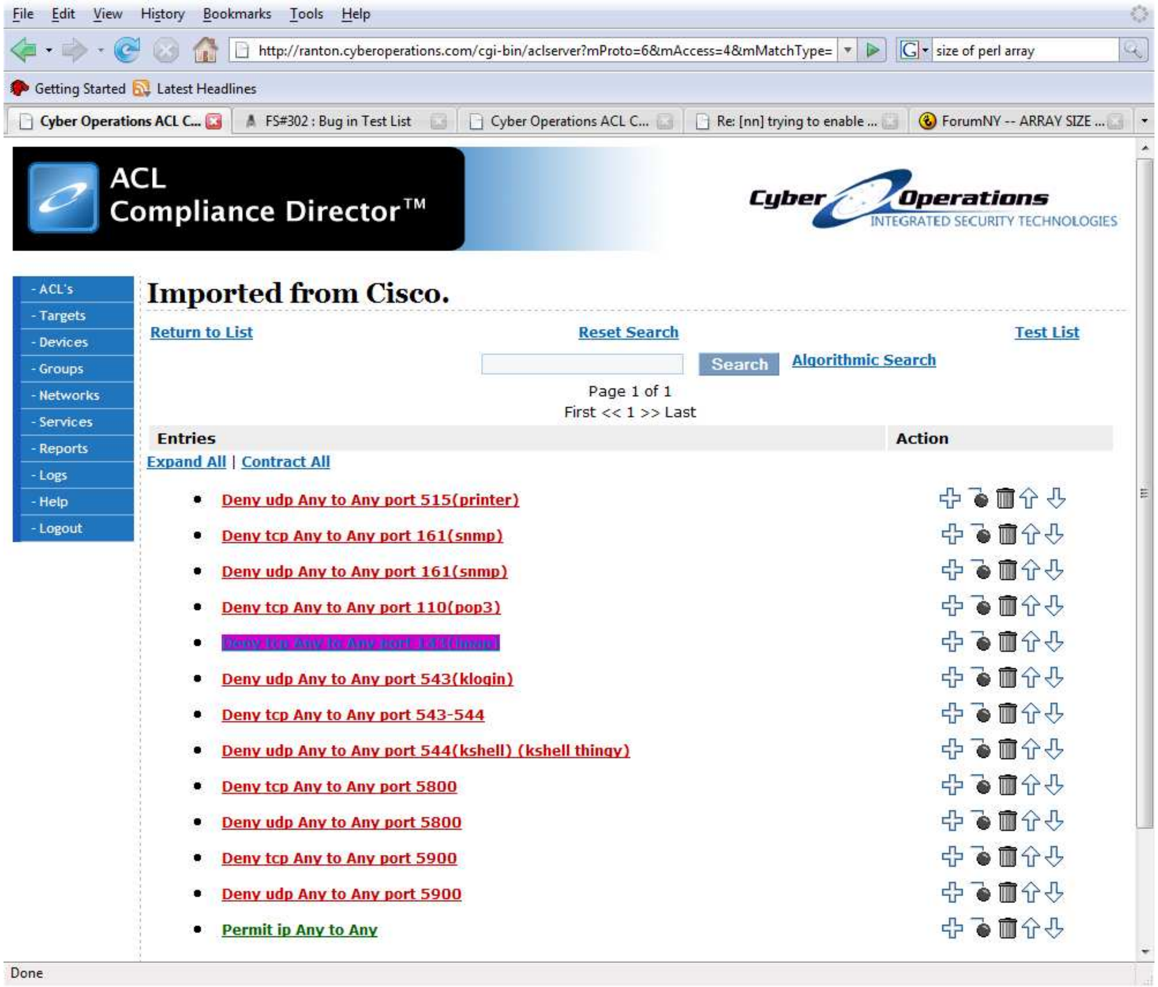
Message: Any Type: any Code: any

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 31 - Test List

When you have entered your parameters, click the “Test” button. You will be taken to the “List Entries” page with the entry which matched your sample values highlighted. This is the terminal entry for those values in the list, meaning that it is the entry which finally permitted or denied the packet.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?mProto=6&mAccess=4&mMatchType=
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#302 : Bug in Test List
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Done

Imported from Cisco.

Return to List | Reset Search | Test List

Search | Algorithmic Search

Page 1 of 1

First << 1 >> Last

Entries | Action

Expand All | Contract All

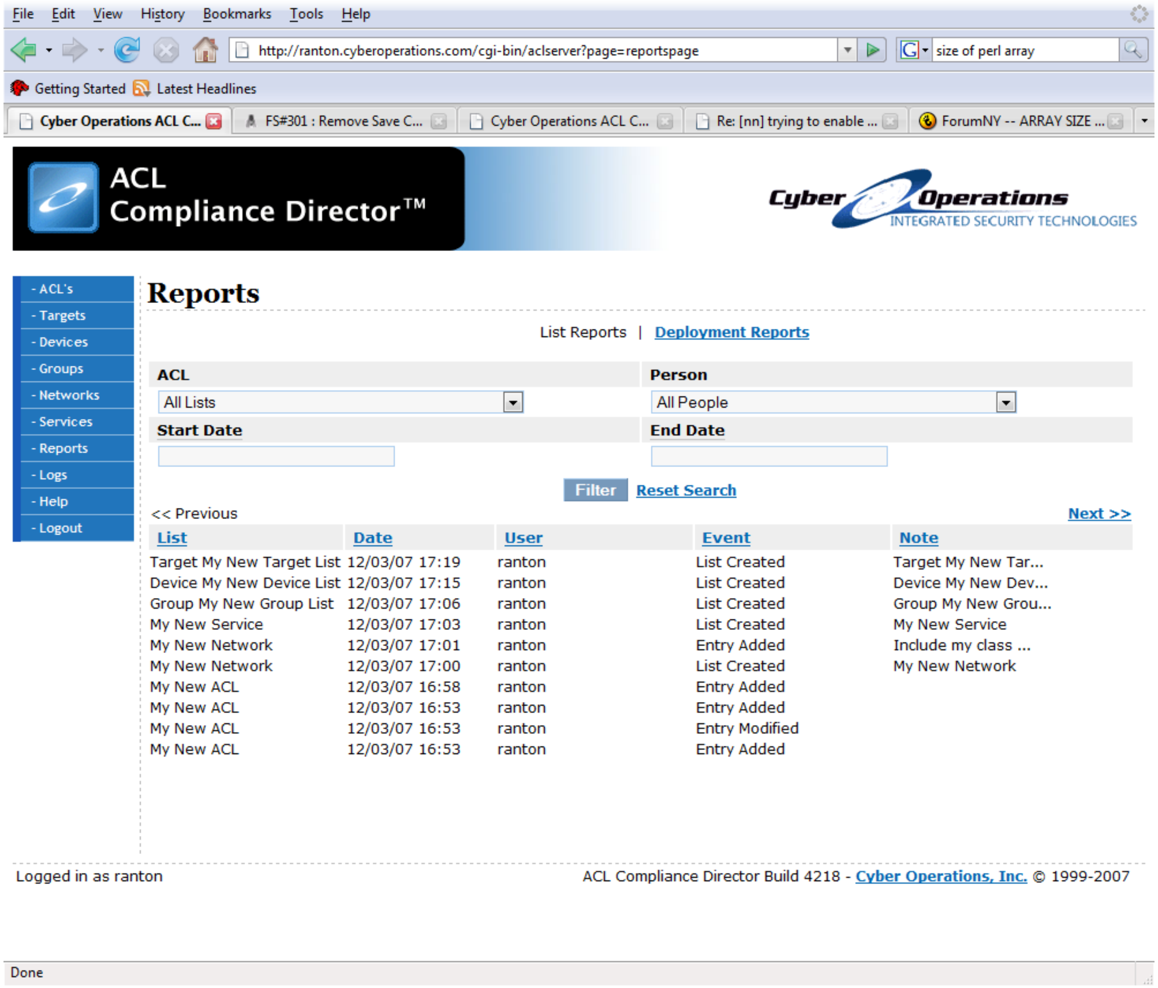
- Deny udp Any to Any port 515(printer)
- Deny tcp Any to Any port 161(snmp)
- Deny udp Any to Any port 161(snmp)
- Deny tcp Any to Any port 110(pop3)
- Deny tcp Any to Any port 143(imap)
- Deny udp Any to Any port 543(klogin)
- Deny tcp Any to Any port 543-544
- Deny udp Any to Any port 544(kshell) (kshell thingy)
- Deny tcp Any to Any port 5800
- Deny udp Any to Any port 5800
- Deny tcp Any to Any port 5900
- Deny udp Any to Any port 5900
- Permit ip Any to Any

Figure 32 - Matching Entry

Reports

ACL Compliance Director supports two types of reports, deployment reports cover all synchronizations which have taken place and list reports which cover all changes made to access lists.

Both types of reports are viewed by clicking the "Reports" tab from the navigational area on the left of the page. Near the top there are two links, one titled "List Reports" and one titled "Deployment Reports", which will take you to the respective type of report.


File Edit View History Bookmarks Tools Help
Getting Started Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Filter
Reset Search
Done

http://ranton.cyberoperations.com/cgi-bin/aclserver?page=reportspage

size of perl array

Reports

List Reports | Deployment Reports

ACL	Person
All Lists	All People
Start Date	**End Date**

<< Previous   Next >>

List	Date	User	Event	Note
Target My New Target List	12/03/07 17:19	ranton	List Created	Target My New Tar...
Device My New Device List	12/03/07 17:15	ranton	List Created	Device My New Dev...
Group My New Group List	12/03/07 17:06	ranton	List Created	Group My New Grou...
My New Service	12/03/07 17:03	ranton	List Created	My New Service
My New Network	12/03/07 17:01	ranton	Entry Added	Include my class ...
My New Network	12/03/07 17:00	ranton	List Created	My New Network
My New ACL	12/03/07 16:58	ranton	Entry Added	
My New ACL	12/03/07 16:53	ranton	Entry Added	
My New ACL	12/03/07 16:53	ranton	Entry Modified	
My New ACL	12/03/07 16:53	ranton	Entry Added	

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 33 - List Reports

Each type of report can be narrowed by various criteria such as user or a date range for example. For list reports, you can select a specific access list, a specific user, a start date, and end date, or any combination of these. Any parameter you do not specify will default to allow any value. For deployment reports you can specify a particular target, device, user, or group as well as specify a date range. Any combination of these values is also possible.

For date ranges with any type of report if only a start date is specified the date range will be the start date until the current time, and if only an end date is specified the date range will be the earliest entry until the end date.

Dates are specified in the form **MM/DD/YYYY** or **MM/DD/YYYY HH:MM** and can also be specified as offsets backwards such as **-30days** or **-1hrs** or **-30mins**.

After you have selected parameters for your report click the “Filter” button to refresh the data.

Logging

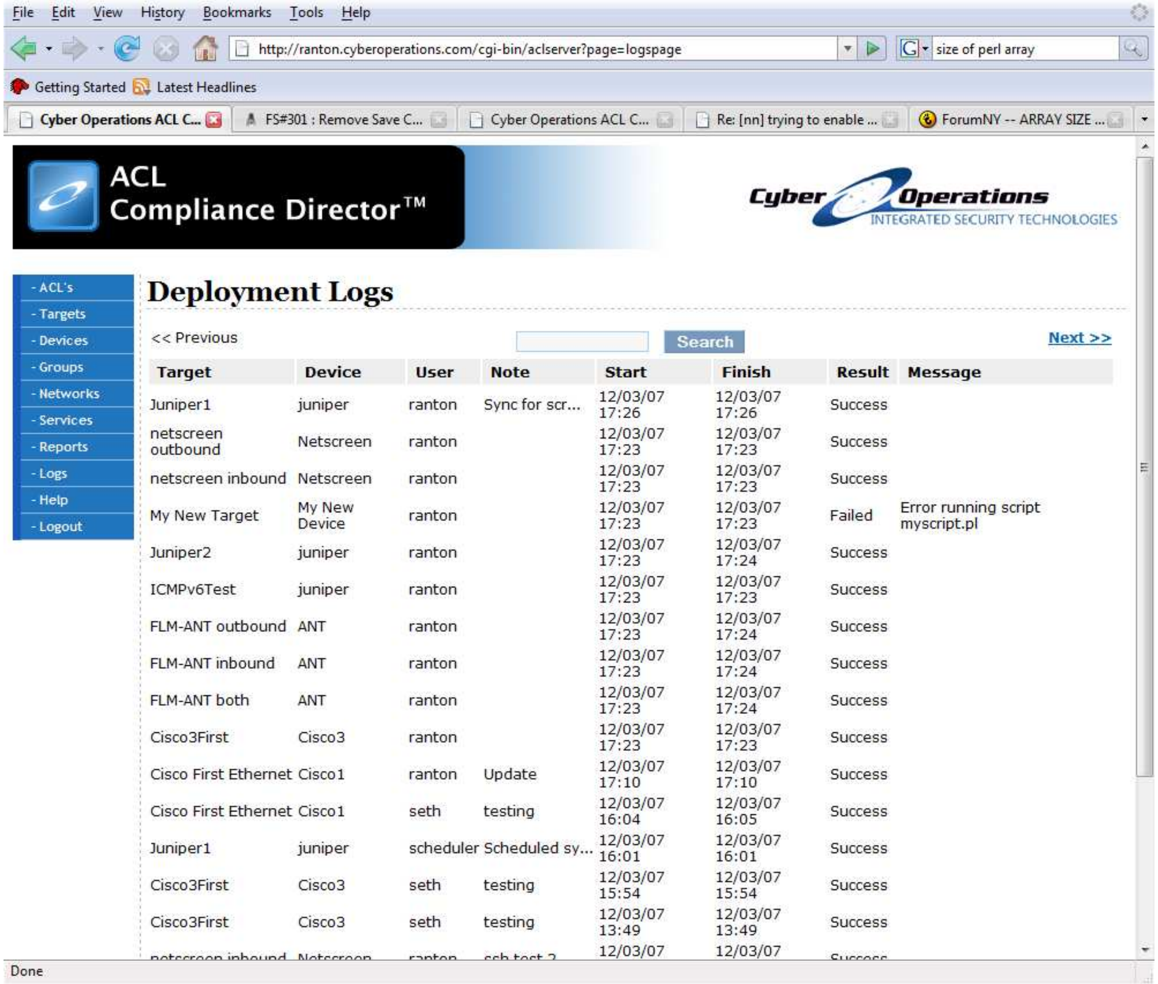
ACL Compliance Director maintains two types of logs. The first type of log saves a history of all synchronizations performed by any user to any target. The second type of log saves a history of all modifications made to the database by users. These logging features allow you to better track user actions, and troubleshoot any problems with your lists or devices.

Deployment Logs

On the “Edit Target” page the deployment log is shown for that particular target with the time, user, note, result, finish time, and any message for each synchronization.

A separate page showing all deployment logs can be viewed by clicking the “Logs” link in the navigational area on the left of the interface. This page shows the target, device, user, note, start time, finish time, result, and any message for each deployment.

Deployment logs also provide the data used for generating deployment reports as discussed in the “Reports” section of this manual.



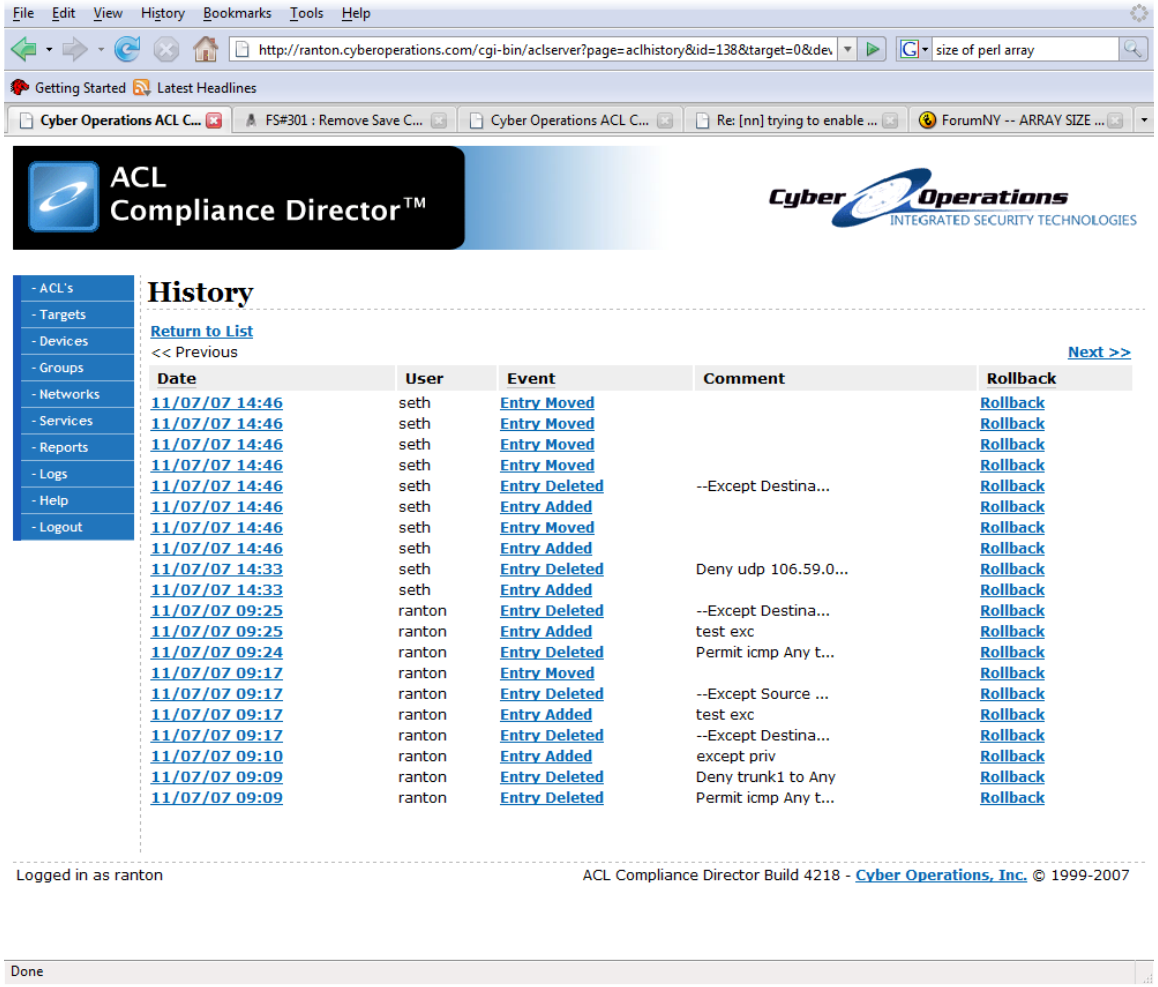
Deployment Logs

Target	Device	User	Note	Start	Finish	Result	Message
Juniper1	juniper	ranton	Sync for scr...	12/03/07 17:26	12/03/07 17:26	Success	
netscreen outbound	Netscreen	ranton		12/03/07 17:23	12/03/07 17:23	Success	
netscreen inbound	Netscreen	ranton		12/03/07 17:23	12/03/07 17:23	Success	
My New Target	My New Device	ranton		12/03/07 17:23	12/03/07 17:23	Failed	Error running script myscript.pl
Juniper2	juniper	ranton		12/03/07 17:23	12/03/07 17:24	Success	
ICMPv6Test	juniper	ranton		12/03/07 17:23	12/03/07 17:23	Success	
FLM-ANT outbound	ANT	ranton		12/03/07 17:23	12/03/07 17:24	Success	
FLM-ANT inbound	ANT	ranton		12/03/07 17:23	12/03/07 17:24	Success	
FLM-ANT both	ANT	ranton		12/03/07 17:23	12/03/07 17:24	Success	
Cisco3First	Cisco3	ranton		12/03/07 17:23	12/03/07 17:23	Success	
Cisco First Ethernet	Cisco1	ranton	Update	12/03/07 17:10	12/03/07 17:10	Success	
Cisco First Ethernet	Cisco1	seth	testing	12/03/07 16:04	12/03/07 16:05	Success	
Juniper1	juniper	scheduler	Scheduled sy...	12/03/07 16:01	12/03/07 16:01	Success	
Cisco3First	Cisco3	seth	testing	12/03/07 15:54	12/03/07 15:54	Success	
Cisco3First	Cisco3	seth	testing	12/03/07 13:49	12/03/07 13:49	Success	
netscreen inbound	Netscreen	ranton	ssh test 2	12/03/07	12/03/07	Success	

Figure 34 - Deployment Logs

Modification Logs

Modification logs, also referred to as list logs, document all the changes made to access lists by the users of the system. The most recent modification log entries for an access list are displayed at the bottom of the "Edit ACL" page for that list. For each log entry the date, user, event (action taken), and comment entered are shown. The complete modification history of an ACL can be viewed by clicking the "History" link. The "History" page is discussed in the section "History and Rollback" in this manual.


File Edit View History Bookmarks Tools Help
http://ranton.cyberoperations.com/cgi-bin/aclserver?page=aclhistory&id=138&target=0&dev
size of perl array
Getting Started
Latest Headlines
Cyber Operations ACL C...
FS#301 : Remove Save C...
Cyber Operations ACL C...
Re: [nn] trying to enable ...
ForumNY -- ARRAY SIZE ...
ACL Compliance Director™
Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES
- ACL's
- Targets
- Devices
- Groups
- Networks
- Services
- Reports
- Logs
- Help
- Logout
Done

History

Return to List

<< Previous Next >>

Date	User	Event	Comment	Rollback
11/07/07 14:46	seth	Entry Moved		Rollback
11/07/07 14:46	seth	Entry Moved		Rollback
11/07/07 14:46	seth	Entry Moved		Rollback
11/07/07 14:46	seth	Entry Moved		Rollback
11/07/07 14:46	seth	Entry Deleted	--Except Destina...	Rollback
11/07/07 14:46	seth	Entry Added		Rollback
11/07/07 14:46	seth	Entry Moved		Rollback
11/07/07 14:46	seth	Entry Added		Rollback
11/07/07 14:33	seth	Entry Deleted	Deny udp 106.59.0...	Rollback
11/07/07 14:33	seth	Entry Added		Rollback
11/07/07 09:25	ranton	Entry Deleted	--Except Destina...	Rollback
11/07/07 09:25	ranton	Entry Added	test exc	Rollback
11/07/07 09:24	ranton	Entry Deleted	Permit icmp Any t...	Rollback
11/07/07 09:17	ranton	Entry Moved		Rollback
11/07/07 09:17	ranton	Entry Deleted	--Except Source ...	Rollback
11/07/07 09:17	ranton	Entry Added	test exc	Rollback
11/07/07 09:17	ranton	Entry Deleted	--Except Destina...	Rollback
11/07/07 09:10	ranton	Entry Added	except priv	Rollback
11/07/07 09:09	ranton	Entry Deleted	Deny trunk1 to Any	Rollback
11/07/07 09:09	ranton	Entry Deleted	Permit icmp Any t...	Rollback

Logged in as ranton

ACL Compliance Director Build 4218 - Cyber Operations, Inc. © 1999-2007

Figure 35 – History

Logging via Syslog

ACL Compliance Director supports logging via the syslog facility. In order to enable this feature, you must configure syslog to direct the **local1** to the appropriate destination.

For example, adding this line to your /etc/syslog.conf would direct log entries to the **/var/log/aclcd** file:

```
local1.*                                                /var/log/aclcd
```

Notification

ACL Compliance Director supports email notification when certain types of events take place. This feature is controlled via the “Administration” page. In order to setup email notification follows these steps:

- Login if you have not already.
- Click the “Admin” link on the left side of the page.
- Under the heading ‘Email Notification’ type the email address you wish to receive notifications in the text box and click on the “Add Email Address” button.
- Repeat the last step for any additional email addresses.
- Uncheck any events for which you do not wish to receive notifications.
- Click ‘Update Notification Settings’ if you changed any of the checkboxes.

System Updates

ACL Compliance Director includes an update mechanism which allows you to receive notifications of available updates over the web. Whenever a new update is available, you will see a notification on the “Administration” page of the web interface. In order to install an available update, run the command line tool “**acdupdate”** from a root shell on the system.

Command Line Tools

ACL Compliance Director also includes **acltool** which is an extensive command line tool that allows the user access to much of the features available via the web interface from the command line, as well as some things not available from the web interface. Please see the extensive built-in help available for using **acltool** by running the command “**acltool help**”.

One thing of interest is the “trusted” configuration entry which will be of interest to anyone wanting to fully automate tasks with **acltool** because it will allow you to grant trusted access to local shell users on the server, whereas acltool normally requires the entry of a username and password on the command line.

Appendix A - Configuration Entries

Below is a table of all configuration values used by ACL Compliance Director. The configuration file is always located at **/etc/aclserver.conf**. Each line of the configuration file is of the form NAME=VALUE where NAME is the name of the configuration entry and everything after the equals sign is the value you are assigning to that entry. Anything after a pound sign # is considered to be a comment and is ignored. Blank lines are also ignored.

Name	**Default**	**Description**
autoImportInterval	20	Interval in minutes at which acdscheduler daemon will check devices for changes to lists being imported by Autolists feature.
BasePath	"/usr/local/acd"	Base directory of installation.
DatabaseAddress	"127.0.0.1"	Address or domain name of database server.
DatabaseName	"acl"	Name of database on database server.
DatabaseUser	"acl"	Username to access database.
DatabasePassword	"acl"	Password to access database.
SyncRefresh	15	Time in seconds between refreshes of synchronization status within web interface.
Devlockbase	"/usr/local/acd/lock/acd_"	Base name for creating per device lock files used to prevent multiple synchronizations to same device at once.
scpRoot	"/usr/local/acd/acdfile"	Home directory and temp directory of the user account used for "SSH + SCP Client" protocol secure copy transfers to and from devices.
scpUser	acdfile	The system account used for "SSH + SCP Client" protocol secure copy transfers.
tftpAccess	Timed	One of open, timed, or restricted. If

		access is open there are no restrictions by time, path or address for TFTP server access. If access is timed, then access is restricted by pathname and time window. If access is restricted, then access is restricted to specific combination of client address, time window, and pathname. Access is always limited to tftpRoot directory regardless of this setting.
tftpPid	“/var/run/acdtftpd.pid”	Path for process ID (PID) file of built in TFTP server.
tftpRoot	“/usr/local/acd/tftp”	Directory built in TFTP server will run from; it will chroot to this path for security reasons.
tftpUser	“httpd”	Username TFTP daemon process will run as. Must have write access to path configured in tftp Root. Defaults to httpd to allow simple interaction between web interface and TFTP server control system without insecure permissions.
schedulerPid	“/var/run/acdscheduler.pid”	Path for process ID (PID) file of scheduler daemon.
schedulerUser	“httpd”	Username that **acdscheduler**, the scheduler daemon will run as. This should generally be the same as that used for tftpUser.
sendmail	“/usr/sbin/sendmail”	Path to sendmail program for sending email notifications.
LDAPServer	No default	Address or hostname of LDAP server for authentication services.
LDAPBaseDN	No Default	Base ‘**dn**’ value of LDAP directory used for authentication.
LDAPInfoUser	“”	LDAP username used when querying user information(not authenticating). Default is blank which will cause anonymous access to be used.
LDAPInfoPass	“”	LDAP password used when querying user information. This is only required if LDAPInfoUser is set.
RadServer1	No default	Address or hostname and server secret of Radius server that will

		provide authentication services.
RadServer2	No default	Address or hostname and server secret of secondary Radius server that will provide authentication services.
TacServer1	No default	Address or hostname and server secret of TACACS+ server that will provide authentication services.
TacServer2	No default	Address or hostname and server secret of secondary TACACS+ server that will provide authentication services.
trusted	root	Comma separated list of trusted local users. These users are implicitly given full authorization when running acltool, where other users are required to authenticate. This is intended to allow full automation for scripting.
UnixPasswordFile	The system password file.	Path to the passwd file used for Unix password authentication.
UnixAuthEnable	0	Set to 1 to enable authorization of specific commands when using the Unix authentication method.
AuthType	“tacacs”	One of “tacacs”, “radius”, “ldap”, or “unix”. See **Authorization** section for more information.
AuthIdleTimeout	3600	Time in seconds that authentication credentials can be cached before querying authentication server.

Support

Please contact us if this manual does not answer your questions, or if you experience any problems while using ***ACL Compliance Director.***

Technical Support

Monday - Friday, 8am - 5pm CST
Phone: 205-403-2923
Email: support@CyberOperations.com
Website: www.CyberOperations.com

Cyber Operations
INTEGRATED SECURITY TECHNOLOGIES