ACL Compliance Director Tutorial

Abstract

This is a tutorial on ACL Compliance Director intended to guide new users through the core features of the system.

Table of Contents

Introduction 1
Login to ACL Compliance Director 1
Creating an ACL 2
Editing an ACL 2
Creating a Device 2
Creating a Target 3
Send the ACL to the Target 4
Preview the ACL 4
Synchronizing a Target 4
Viewing the Device Configuration 5
Importing a List 5
Creating a Network Definition 6
Creating a Service Definition 6
History and Rollback 7
Target Status 7
Modify Network and Service 8
Searching 9
Creating and Using a Group 10
Logging and Reporting 10
Summary 11

Introduction

Thanks for using ACL Compliance Director. This tutorial is intended to get new users started quickly with the core features of the product. It will walk you through a series of steps to create, modify, import, and apply an ACL to a dummy networking device. It will also guide your through creating and using network definitions, service definitions, groups, and sublists.

This tutorial does not try to answer device type specific configuration questions. You should see the user manual or contact Cyber Operations at support@cyberoperations.com for questions regarding specific configuration issues. Also, the tutorial assumes that user authorization is already setup on your system, and that you already have an account on your ACL Compliance Director system.

Login to ACL Compliance Director

Enter the URL of your ACL Compliance Director system, for example `https://acl.cyberoperations.com` and you should see the login page. Enter your username and password, then press the `Login` button.
If you are the administrator for your ACL Compliance Director system, and you have not yet configured authorization settings then please see the user manual for instructions on doing so before continuing.

After logging in successfully you will see welcome page with the ACL Compliance Director and Cyber Operations logos.

Creating an ACL

Now we are going to create an ACL.

1. Click the area in the navigation menu titled ACL's. You will then see the "Access Lists" page. This is where you can view all of the access lists in the system, except for the special access lists for targets, devices, and groups which we will talk about later.
2. Click the `Add New ACL` link.
3. On the "Add New ACL" page enter the name "Tutorial List 1" in the Description field. This will be the name of your new access list. Do not worry about the Placement field for now.
4. Click the `Save` button and you will be taken to the "Edit ACL" page.

Editing an ACL

1. From the "Edit ACL" page click the `Edit Entries` link. This will take you to the "List Entries" page for your new access list "Tutorial List 1".
2. Click the `Append New Entry` link which will take you to the `Add New Entry` page.
3. From the drop-down menu for the `Action` field select "Deny".
4. From the drop-down menu for the `Protocol` field select "UDP".
5. In the text box beneath `Source Net/Mask` enter the text "5.4.3.0/24".
6. Last, click the `Save` button. You will be returned to the "Edit Entries" page.

You have just created an ACL entry which will deny all UDP traffic originating on the network 5.4.3.x. The /24 you entered specifies the CIDR mask associated with the address. The value 24 is equivalent to a subnet mask of 255.255.255.0 or a Cisco type wildcard mask of 0.0.0.255.

Creating a Device

Now we are going to create a device to use your new ACL with.

1. Click `Devices` in the navigation menu. On the "Devices" page you can see the devices configured in the system. Each device represents an actual networking device whether it be a firewall, router, or switch.
2. Click the `Add New Device` link which will take you to the "Add New Device" page.
3. Enter "Tutorial Device" in the `Description` field. This will be the name of your device.
4. For the device type, select "Dummy Device" from the `Type` drop-down menu. This is a special type of device which can be used for testing ACL's or trying things out without causing any changes to an actual network device.
5. Click the `Save` button. This will take you to the "Edit Device" page.

Because this is a dummy device, you do not need to worry about the other fields, but we will cover them briefly anyway.

- `Address` - This specifies the DNS name or IP address of the network device to be controlled.
- `Protocol` - This field specifies the communication method or methods that will be used when communicating with the device. The options available depend on the device type. For protocol values that read like First+Second, such as "SSH+TFTP", the first protocol is used for controlling the device while the second is used for sending configuration data back and forth. Please see the user manual for a complete discussion of the available options.
- The `Device Login Name` - This sets the username, if any, used when connecting to the device. This is not required for all combinations of device types and protocols.
- `Device Password` - This sets the password used to authenticate when connecting to the device.
- `Enable Password` - This sets the enable password to be used with the device. This is the password required by some devices, mainly Cisco devices, to elevate the privilege level of the session to the point where configuration changes are permitted. If it is not required by the device in question, then leave it blank.

Creating a Target

A target represents a specific ACL name or filter on a device, and a device can have multiple targets. We need to create a target for our new device so that we can apply our ACL's containing our network policy to the device.

1. Click the `Add New Target` link on the "Edit Device" page for the device you created in the last step. This will take you to the "Add New Target" page.
2. Enter "Tutorial Target" in the `Description` field.
3. Enter "TutorialFilter" in the `Device Filter Name` field.
4. Click the `Save` button. You will be taken to the "Edit Target" page.

For a real device the `Device Filter Name` would be the name the filter or ACL will take in the device's configuration. For example on a Cisco IOS device this would be the actual access-list name or number on the device, and on a Juniper JunOS device this would be the name of the firewall filter. Because this is not a real device the other settings are not required, but we will cover briefly what each setting represents.

- `Device Interface Names` - This setting determines which network interfaces the ACL will be applied to on the device. Be aware however that for many devices this setting is not used and it is left to the user to configure the device itself to apply the list. In the case of Cisco devices, this setting is used when the protocol setting is 'SSH' or 'Telnet' but not otherwise.
- `Traffic Direction` - This setting controls whether the access-list is applied to incoming or outgoing traffic or both. This setting is not supported by all device types and the control is disabled when working with a device that does not support it.
- `Script` - If set this is the full path to a script on the ACL Compliance Director system which will be used to filter the device specific syntax of the ACL before it is sent to the device.
- `IPv6` - For devices which support it this controls whether the IPv6 version of a list is sent to the device. Entries which are IPv6 specific will be stripped out prior to sending the ACL if this is unchecked.

- `Extended` - Some types of devices have both standard and extended types of access lists. This box determines which syntax is used, and is checked by default. Cisco IOS and similiar devices are generally what this is used with, and unless you are using the ACL for a specialized purpose you probably want to use an extended lists because standard Cisco ACL's only allow filtering traffic based on the source address.

Send the ACL to the Target

Now it is time to actually apply our ACL we created earlier to our target. In order to do that we are going to include "Tutorial List 1" as a sublist of the target's ACL.

1. Click on the `Edit ACL` link from the "Edit Target" page.
2. Click the `Edit Entries` link.
3. Click on `Append New Entry`.
4. Near the bottom of the "Add New Entry" there will be a drop-down which initially says "(Select List to insert)". Click the drop-down and find and select "Tutorial List 1".
5. Click the `Save` button.
6. Click `Return to List`.
7. Click `Return to Target`.

You have now included the entries from "Tutorial List 1" into the target ACL. Now whenever you make changes to "Tutorial List 1" those changes will be included in the target ACL the next time the target is synchronized, and the target will also be marked out of sync whenever the list "Tutorial List 1" changes.

Preview the ACL

Now we will use the Preview ACL feature to see the actual device specific syntax of the ACL before sending it to the device.

1. Click `Preview ACL` near the top right of the "Edit Target" page.
2. Examine the text on the "Output Preview" page. This is the device ACL. Since it is a dummy device type the native syntax of Cyber Operations' ACL format is shown.
3. Click `Back to Target` when you are finished with the preview page.

Synchronizing a Target

Now it is time to synchronize our target with our ACL.

1. In the text box to the left of the `Synchronize` button, type the text "This is my comment".
2. Click the `Synchronize` button.
3. When the dialog pops up asking you to confirm synchronization, click `Ok`.

You should now see a line appear towards the bottom of the "Edit Target" page that shows the start time, your username, the comment you entered, the result(either "Success", "Failed", or "In Progress"), finish

time, and message of the synchronization. The message column will show you any error messages or warnings.

If this were a target on a real device, the synchronization would have taken more than a split second and during that time the `Synchronize` button would have been replaced by a barber-pole type progress indicator and a `Cancel` button.

Viewing the Device Configuration

Now that we have applied an ACL to our device, let's look at what the device configuration looks like.

1. From the "Edit Target" page click on `Parent Device`.
2. Click `View Configuration`.

You should now be looking at a page with the heading "Device Configuration for Tutorial Device" which contains a large text box with the text of an ACL in it. The ACL text should be just that of "Tutorial List 1".

Notice that you also have the option to download the device configuration to a file by clicking `Download as Text`.

Importing a List

1. Click the `ACL's` item in the navigation menu on the left
2. Click on "Tutorial List 1"
3. Click on `Edit Entries`
4. Paste the following text into a text file somewhere:

```
ip access-list extended demolist
 remark Allow TCP traffic from our network
 permit tcp 10.3.1.0 0.0.0.255 any
 remark Allow established TCP connections.
 permit tcp any any established
 remark Allow domain queries
 permit udp any any eq 53
 remark Allow domain replies
 permit udp any eq 53 any
 remark Permit ping
 permit icmp any any 8
 remark Ping reply
 permit icmp any any echo-reply
 remark Deny by default
 deny IP any any
```

5. Click `Browse` and select the file where you saved the above text.
6. Click `Import`.

You have now imported the above Cisco access-list into ACL Compliance Director. If there had been more than one ACL in the file you selected, you would have been asked which to import. You will also notice that the original contents of your one entry list have been replaced by the data you imported.

Creating a Network Definition

1. Click `Networks` in the navigation menu.
2. Click `Add New Network`.
3. Type "Tutorial Network" in the `Description` field.
4. Click `Save`.
5. Click `Add Network Address`.
6. Type "10.3.1.0/24" in the `Network and Mask` field.
7. Click `Save`.
8. Click `ACL's` in the navigation menu.
9. Click on "Tutorial List 1".
10. Click `Edit Entries`.
11. Click on the first entry to edit it. Not the comment only entry, but the one after it.
12. On the "Edit Entry" page, delete the text in the `Source Net/Mask` field, and select "Tutorial Network" from the drop-down for that field.
13. Click `Save`.

The source address(es) used by the first entry are now defined by the network definition "Tutorial Network" for the source address of the first entry of "Tutorial List 1". Now if we change the network definition, the rule will automatically be updated.

Creating a Service Definition

Now we are going to replace our entries that allow UDP port 53 access for domain name queries to use a service definition for the port numbers instead of using 53 directly.

1. Click `Services` in the navigation menu.
2. Click `Add New Service`.
3. Type "Tutorial Service" in the `Description` field.
4. Click `Save`.
5. Click `Add Service` on the "Edit Service" page.
6. Enter "53" in the `Service or Port Range` field.
7. Click `Save`.
8. Click `ACL's` in the navigation menu.
9. Click on "Tutorial List 1".
10. Click `Edit Entries`.

11. Click on the entry that says "Permit udp Any to Any port 53(dns)".

12. On the "Edit Entry" page find the "53(dns)" in the `Port/Service` field for the destination and select "Tutorial Service" from the drop-down for that field.

13. Click `Save`.

14. Click on the entry that says "Permit udp Any port 53(dns) to Any".

15. On the "Edit Entry" page find the "53(dns)" in the `Port/Service` field for the source and select "Tutorial Service" from the drop-down for that field.

16. Click `Save`.

Now the entries allowing UDP access to specific ports reference the "Tutorial Service" service definition for the actual list of ports. Now whenever you update "Tutorial Service" this list will reflect your changes.

History and Rollback

Now we are going to show you how to delete an entry in a list, then restore that entry using the history and rollback features of ACL Compliance Director.

1. Click the trash can icon to the right of entry number 5 of "Tutorial List".

2. Now click `Return to List`.

3. Click `History`.

4. It should say "Entry Deleted" in the third column of the top line. Click the date column of the first line.

5. See the difference between the current list and the previous list, then click the back button of your browser.

6. Click `Rollback` in the top line.

7. Click `Return to List`.

8. Click the `Edit Entries` link.

Now you see that you have the entry back that you deleted. You can rollback to any previous point in the revision history of an ACL just by clicking the `Rollback` link on the "History" page across from the oldest change you want to undo.

Target Status

Now that we have modified our target's access list we are going to take a look at how ACL Compliance Director displays target status, and then synchronize our target again.

1. Click the `Targets` button in the navigation menu.

2. Look at the icon in the `Synchronize` column for "Tutorial Device". Notice that it has an icon like two semicircular arrows. This indicates the target is out of sync.

3. In the text box at the bottom of the page (next to the `Synchronize All` button), type "From targets page".

4. Click the circular arrows icon in the `Synchronize` column. Alternately, you can click the `Synchronize All` button which will synchronize all targets marked out of sync.

5. Observe the icon change to a small barber pole type progress indicator. Wait for the icon to change back to a check mark. Your device is now synchronized again.

Modify Network and Service

Now we are actually going to modify our network and service definitions to include more than one address block and service definition. We will start with the network definition.

1. Click `Networks` in the navigation menu.

2. Click on "Tutorial Network" to edit the network we created earlier.

3. Click `Add Network Address`.

4. Type "10.4.1.0/24" in the `Network and Mask` field to add an additional class C (netmask of 255.255.255.0 or CIDR of 24) network block.

5. Click `Save`.

6. Click `Add Network Address`.

7. This time, select "Exclude" from the `Action` drop down menu. This will cause the network to exclude the network and mask entered.

8. Enter "10.4.1.15" in the `Network and Mask` field. This host IP which would otherwise be included by the block added ealier will now be excluded.

9. Click `Save`.

Now let's modify the service definition

1. Click `Services` in the navigation menu.

2. Click "Tutorial Service" to edit the service you created earlier.

3. Click `Add Service` on the "Edit Service" page.

4. Enter "60-70" in the `Service or Port Range` field to allow all the ports from 60 through 70 inclusive.

5. Click `Save`.

6. Click `Add Service` on the "Edit Service" page.

7. This time, select "Exclude" from the `Action` drop down menu. This will exclude the specified port or ports from the service definition.

8. Enter "69" in the `Service or Port Range` to exclude 69 (TFTP) from the allowed port range added as the last entry.

9. Click `Save`.

Now we have updated both the network and service definitions used by "Tutorial List" which is in turn included as a sublist of our target list for "Tutorial Target". Now let's take a look at the effect our entries had on the generated syntax by using the preview feature again.

1. Click the `Targets` button in the navigation menu.
2. Click "Tutorial Target". Notice that target is listed as not synchronized again.
3. Click `Preview ACL` near the top right of the "Edit Target" page.
4. Notice that the corresponding entries for the network and services have been generated. You will also notice that adding a network exclude entry can generate some complex syntax, and that adding the excluded port resulted in the 60-70 range generating two entries instead of one.

Searching

Now we are going to go over some of the searching tools that ACL Compliance Director has. These are useful when you are editing or troubleshooting large access-lists. First we are going to use the text based search feature.

1. Click `ACL's` in the navigation menu.
2. Click "Tutorial List".
3. Click `Edit Entries`.
4. In the text box next to the `Search` button, type in "udp".
5. Click the `Search` button.

Now you will see entries the two UDP specific entries highlighted with a yellow background color. The search syntax is that of extended POSIX regular expressions. The '.' matches any character, and you can use parenthesis to group items and the | character as a boolean or operator. For an example of this try searching for the string "udp|icmp". Another example is that you could match all TCP established entries by searching for "tcp.*established" the asterisk signals to match the previous character or expression an unlimited number of times so this would match any string that contained "tcp" and "established" regardless of what is between the two words.

Now we will examing the advanced search feature.

1. Click `Advanced Search`.
2. For `Match Type` select "Subset".
3. For `Protocol` select "UDP".
4. Click the `Search` button.
5. Again the two UDP related entries are hilited.
6. Click `Advanced Search`.
7. Select "Intersect" for `Match Type`.
8. Select "TCP" for `Protocol`.
9. Enter 80 in the destination `Port/Service` text box(the lower one).
10. Click the `Search` button.
11. This time you will see the two TCP entries at the top of the list hilited.

The advanced search feature is very powerful and flexible, but it takes a little more time and thought to use than the text based search.

Creating and Using a Group

ACL Compliance Director has a feature called groups which lets you group together targets, devices, or other groups and apply policy to them as a whole.

You have now created a group. In practice, there is little reason to create a group with only one member. You would normally create a group to apply a policy to multiple devices, targets, or a combination of both. Also, note that adding a device to a group auto-inserts the group list into the device list which is in turn auto-inserted into the ACL of each of the device's targets.

1. Click `Groups` in the navigation menu.
2. Click `Add New Group`.
3. Enter "Tutorial Group" for `Group Name`.
4. Click the `Targets` tab.
5. Click on "Tutorial Target" in the right hand side box under the heading `Non-Members`.
6. Click the `<< Add` button to add the target to the group.
7. Click the `Save` button.
8. Click on `Edit ACL`. This will allow you edit the ACL which will be applied to the entire group.
9. Click `Edit Entries`.
10. Click the `Append New Entry` link which will take you to the `Add New Entry` page.
11. From the drop-down menu for the `Action` field select "Permit".
12. From the drop-down menu for the `Protocol` field select "TCP".
13. Under the destination `Port/Service` enter "80".
14. Click `Save`.
15. Now click `Targets` in the navigation menu.
16. Click "Tutorial Target".
17. Click on `Edit ACL`. You should now see an auto-inserted list entry that reads "Sublist: Group Tutorial Group List". This is to show you that the group's ACL is being included, and at what point in the ACL. You can control the order of the auto-inserted lists by changing the `Placement` setting of the ACL's involved; see the user manual for more info regarding placement. Note that you must remove the sublist entry by removing the target from the group. Trying to remove the auto-inserted sublist via the "Edit Entries" page will have no effect.

Logging and Reporting

Now we are going to take a look at ACL Compliance Director's logging and reporting features.

1. Click `Logs` in the navigation menu. You should see a row for each of the synchronizations for our "Tutorial Target".

The "Logs" page shows each synchronization that has taken place, most recent first along with who performed the synchronization and the start and finish(completion) times. The `Result` column indicates if the synchronization was successful or not; the `Note` column is the comment entered when the synchronization was started; and the `Message` column shows the error message if there was any.

Now let's take a look at the "Reports" page.

1. Click `Reports` in the navigation menu.

2. By default, the `List Reports` option is selected. This is fine for now; we'll deal with the other option later.

3. Click the drop-down labeled `ACL` and select "Tutorial List 1". With this selected you will see all modifications made to the access-list "Tutorial List 1" as opposed to "All Lists". You can also limit the results to a specifc user by clicking on the `Person` drop-down.

4. Click the `Filter` button. This will regenerate the report based on your selections.

5. Now, click the calender icon to the right of the `Start Date` field and click on any day in the past. You can also type date or date and time values into the `Start Date` and `End Date` fields directly. Additionally, you can type things like "-12hours" (or months, weeks, days, or minutes) into a date field to get an effective date and time of 12 hours ago.

6. Click on the `Date` column. Notice that the order of the data is now reversed. You can click on any column heading to sort by that column, and you can click the column again to reverse the order.

7. Now click `Deployment Reports` near the top of the page. Notice that you now see synchronization information very much like the log page.

8. Select "Tutorial Target" from the `Target` drop-down.

You can limit the synchronization(aka Deployment) report results by `Target`, `Device`(meaning all targets of that device), `Person`, or `Group` (meaning all targets in the group whether directly or via their parent device or another group). Also there are `Start Date` and `End Date` fields which work just like they did with list reports. Also, you can sort by any column just as before, or reverse the order by clicking the same column heading again.

Be sure to play around with both types of reports to get a feel for what is possible.

It is also possible to export the data from either type of report to a CSV (comma separated) file by clicking the `Save This Report` link near the bottom of the page.

Summary

Please refer to the user manual for a more complete reference on ACL Compliance Director. The manual is accessible any time by clicking `Help` from the navigation menu or online at http://www.cyberoperations.com/resources/ACLDirector/ACLComplianceDirector_user_manual.pdf.

For the most up to date information on ACL Compliance Director, please visit the Cyber Operations website at http://www.cyberoperations.com.

Here are some topics the tutorial does not cover that you may want to investigate as you become more comfortable with the system. For more information on these please see the user manual.

1. `acltool` - This is the command line tool for accessing ACL Compliance Director functionality. Assuming you have a shell account on the ACL Compliance Director system you are using and everything is installed in the default location, just run "/usr/local/acd/bin/acltool help" to get started.

2. `Schedules` - The schedules feature in conjunction with the acdscheduler daemon allows you to schedule automatic synchronizations of targets as well as the automatic expiration of entries.

3. `Network Overrides` - Network definitions can be overridden per device or target so that the same list when applied to different targets could take on a different actual values. This is to allow configurations such as defining the inside, outside, and DMZ network addresses per firewall device, then using the same ACL policy logic for all of them.

4. `More Importing Options` - There are many more importing options available than discussed in this tutorial. For example you can import directly from a device or configure an autolist which will be periodically re-imported to match the access-list on the device itself.

5. `Administration` - This tutorial does not attempt to address the administration of the ACL Compliance Director server. For more information on administration in general, as well as the "Admin" page within the web interface please see the user manual. Topics of particular interest include configuring your authentication and authorization and using `acdupdate` to update the system whenever a patch is available.