

# Automating Cisco ACLs

Application Note

# Introduction

When organizations begin their enterprise network automation journeys, top of mind is enhancing network security, increasing agility, and ensuring business continuity. No matter what path they are on as they move from manual and scripted network management to code-free, error-free automation, they share some common ground on what urgent challenges to tackle first.

This collection of network automation use-cases is designed help customers learn from each other about the common challenges they face, the key learnings they gain along the way, and the benefits they experience as a result of putting intelligent network automation to work on some of their most pressing network challenges.

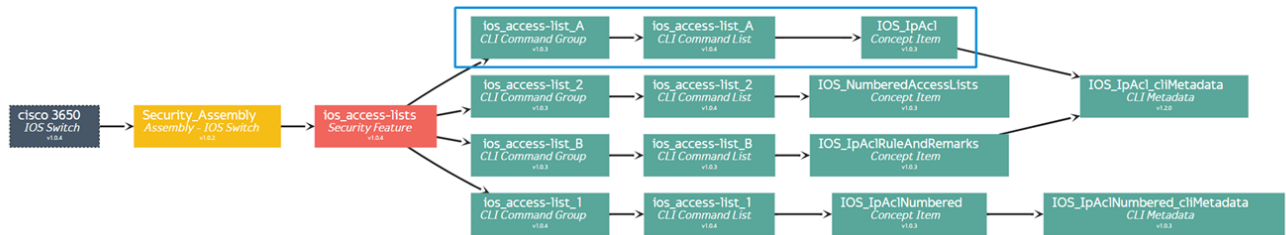
Gluware's off-the-shelf network automation software suite delivers the features, simplicity and reliability organizations seek today to discover, automate and orchestrate their complex, multi-vendor networks. To prevent network outages, manual errors and security issues, a growing number of enterprises look to Gluware for a better approach to automating their mission-critical networks.

This Field Brief describes four methods of automating Cisco ACLs. The brief considers named and numbered ACLs and if the ACL is removed prior to being updated. In each of the below Methods the output and manner of updating the ACL is determined by the specific concept item specified.

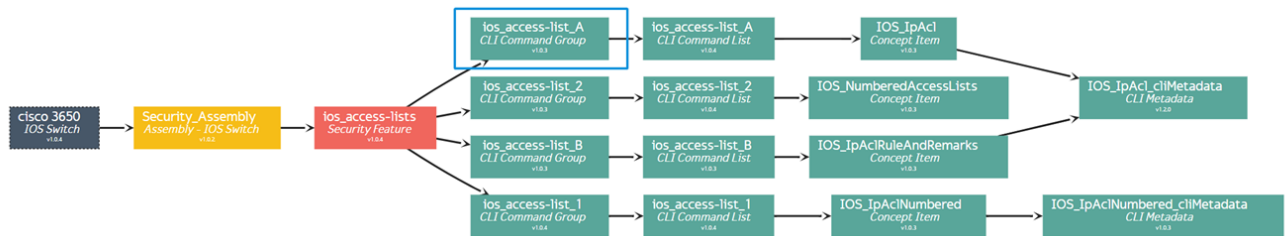
# Contents

<b>Introduction</b>	<b>2</b>
<b>Method 1</b>	<b>4</b>
CLI Command Group	4
CLI Command List	4
Initial Provisioning	5
Running-Config	5
Changes to the Model	6
Provisioning After Changes	6
<b>Method 2</b>	<b>7</b>
CLI Command Group	7
CLI Command List	8
Initial Provisioning	8
Running-Config	9
Changes to the Model	9
Provisioning After Changes	9
<b>Method 3</b>	<b>10</b>
CLI Command List	10
CLI Command Group	11
Initial Provisioning	11
Running-Config	12
Changes to the Model	12
Provisioning After Changes	12
<b>Method 4</b>	<b>13</b>
CLI Command Group	13
CLI Command List	13
Initial Provisioning	14
Running-Config	15
Changes to the Model	15
Provisioning After Changes	15
Gluware Solutions	16

# Method 1 Standard/Extended Named ACLs without Remarks



## CLI Command Group



ios\_access-list\_A

Add Instance Description

Naming Convention (regex)

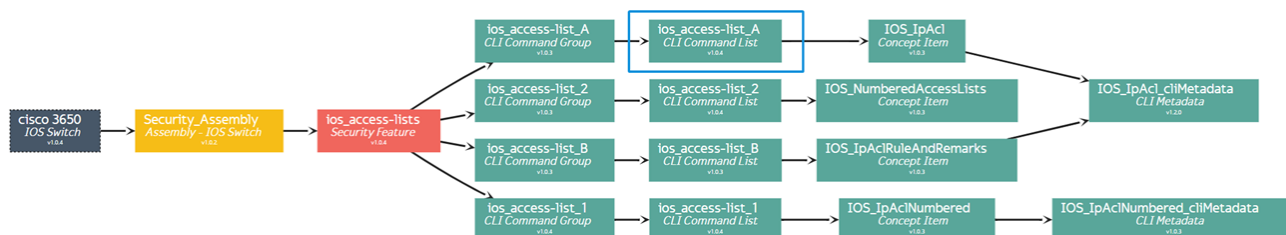
acl-wan-A


Disable Group Removal

**cliBlocks**

Available	Selected
<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input type="text" value="Search"/> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <span style="font-size: 18px; font-weight: bold;">ios_access-list_A</span> </div>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <span style="font-size: 18px; font-weight: bold;">ios_access-list_A</span> </div>

## CLI Command List



 ios\_access-list\_A

Add Instance Description

---

Associated Concept Item \*

IOS\_IpAcl

CLI Commands

```

1 ip access-list extended acl-wan-A
2 remark SSH Traffic
3 permit tcp any any eq 22 log
4 remark HTTP/HTTPS Traffic
5 permit tcp any any eq 80
6 permit tcp any any eq 443
7 remark DNS Traffic
8 permit tcp any any eq 53
9 permit udp any any eq 53
10 permit icmp any any echo-reply log
11 permit udp any any eq isakmp log
12 permit gre any any log
13 permit esp any any log
14 !

```

## Initial Provisioning

```

ip access-list extended acl-wan-A
remark SSH Traffic
10 permit tcp any any eq 22 log
remark HTTP/HTTPS Traffic
20 permit tcp any any eq 80
30 permit tcp any any eq 443
remark DNS Traffic
40 permit tcp any any eq 53
50 permit udp any any eq 53
60 permit icmp any any echo-reply log
70 permit udp any any eq isakmp log
80 permit gre any any log
90 permit esp any any log
exit

```

## Running-Config

```

c3650-podv2-01#sh run | sec ^ip access-list.*-A$
ip access-list extended acl-wan-A
remark SSH Traffic
permit tcp any any eq 22 log
remark HTTP/HTTPS Traffic
permit tcp any any eq www
permit tcp any any eq 443
remark DNS Traffic
permit tcp any any eq domain
permit udp any any eq domain
permit icmp any any echo-reply log
permit udp any any eq isakmp log
permit gre any any log
permit esp any any log

```

## Changes to the Model

```

1 ip access-list extended acl-wan-A
2 remark SSH Traffic
3 permit tcp any any eq 22 log
4 permit tcp any any eq telnet
5 remark HTTP/HTTPS Traffic
6 permit tcp any any eq www
7 permit tcp any any eq 443
8 remark DNS Traffic
9 permit tcp any any eq domain
10 permit udp any any eq domain
11 permit icmp any any echo-reply log
12 permit udp any any eq isakmp log
13 permit gre any any log
14 permit esp any any log
15 remark BGP Traffic
16 permit tcp any any eq bgp
17 !

```

New rule added at sequence 20

New remark and rule added to bottom of ACL

## Provisioning After Changes

This is triggered by the concept item - in this case: IOS\_IpAcl

```

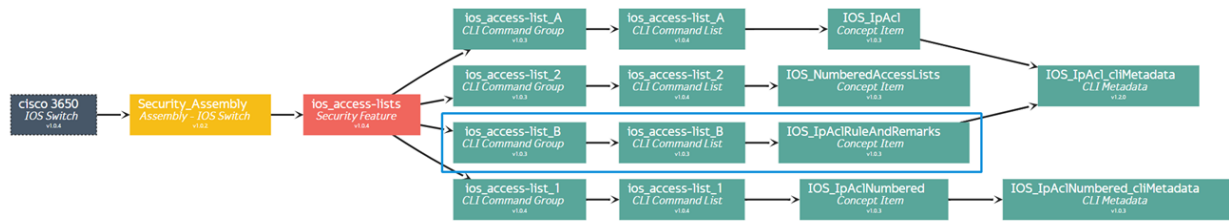
ip access-list extended acl-wan-A
no 20 permit tcp any any eq www
no 30 permit tcp any any eq 443
no 40 permit tcp any any eq domain
no 50 permit udp any any eq domain
no 60 permit icmp any any echo-reply log
no 70 permit udp any any eq isakmp log
no 80 permit gre any any log
no 90 permit esp any any log
20 permit tcp any any eq telnet
30 permit tcp any any eq www
40 permit tcp any any eq 443
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit icmp any any echo-reply log
80 permit udp any any eq isakmp log
90 permit gre any any log
100 permit esp any any log
remark BGP Traffic
110 permit tcp any any eq bgp
exit

```

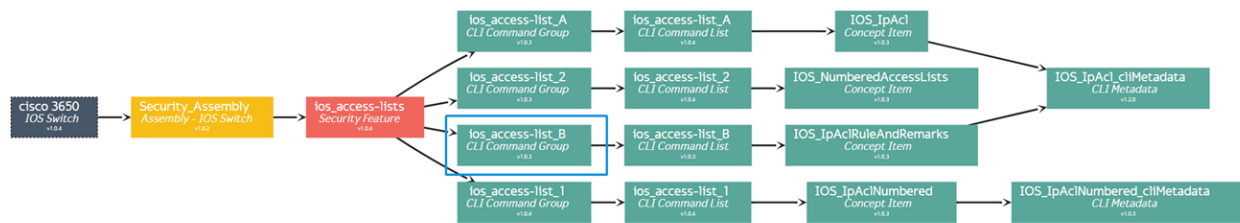
Notice it does not take the original remarks into account (they are not added back)

Also, note that the other ACLs in the model are not changed - only the one we referenced in the *CLI command group*.

# Method 2 Standard/Extended Named ACLs with Remarks



## CLI Command Group



**ios\_access-list\_B**

Add Instance Description

---

Naming Convention (regex)

**acl-wan-B**

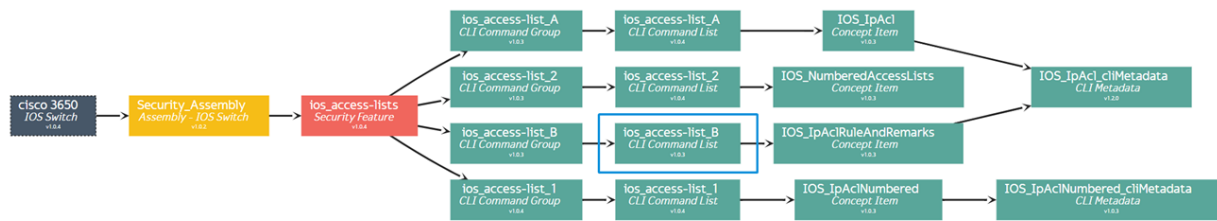
Disable Group Removal

**cliBlocks**

Available	Selected
<input type="text" value="Search"/> <ul style="list-style-type: none"> <li>asa_aaa-auth-cli &gt;&gt;</li> <li>asa_aaa-server-flat_cli &gt;</li> </ul>	<ul style="list-style-type: none"> <li><b>ios_access-list_B</b></li> </ul>



## CLI Command List



ios\_access-list\_B

Add Instance Description

---

Associated Concept Item \*

IOS\_IpAclRuleAndRemarks

CLI Commands

```

1 ip access-list extended acl-wan-B
2 remark SSH Traffic
3 permit tcp any any eq 22 log
4 remark HTTP/HTTPS Traffic
5 permit tcp any any eq 80
6 permit tcp any any eq 443
7 remark DNS Traffic
8 permit tcp any any eq 53
9 permit udp any any eq 53
10 permit icmp any any echo-reply log
11 permit udp any any eq isakmp log
12 permit gre any any log
13 permit esp any any log
14 !

```

## Initial Provisioning

```

ip access-list extended acl-wan-B
remark SSH Traffic
10 permit tcp any any eq 22 log
remark HTTP/HTTPS Traffic
20 permit tcp any any eq 80
30 permit tcp any any eq 443
remark DNS Traffic
40 permit tcp any any eq 53
50 permit udp any any eq 53
60 permit icmp any any echo-reply log
70 permit udp any any eq isakmp log
80 permit gre any any log
90 permit esp any any log
exit

```



## Running-Config

```
c3650-podv2-01#sh run | sec ^ip access-list.*-B$
ip access-list extended acl-wan-B
remark SSH Traffic
permit tcp any any eq 22 log
remark HTTP/HTTPS Traffic
permit tcp any any eq www
permit tcp any any eq 443
remark DNS Traffic
permit tcp any any eq domain
permit udp any any eq domain
permit icmp any any echo-reply log
permit udp any any eq isakmp log
permit gre any any log
permit esp any any log
```

## Changes to the Model

```
2  remark SSH Traffic
3  permit tcp any any eq 22 log
4  permit tcp any any eq telnet
5  remark HTTP/HTTPS Traffic
6  permit tcp any any eq www
7  permit tcp any any eq 443
8  remark DNS Traffic
9  permit tcp any any eq domain
10 permit udp any any eq domain
11 permit icmp any any echo-reply log
12 permit udp any any eq isakmp log
13 permit gre any any log
14 permit esp any any log
15 remark BGP Traffic
16 permit tcp any any eq bgp
17
```

New rule added at sequence 20

New remark and rule added to bottom of ACL

## Provisioning After Changes

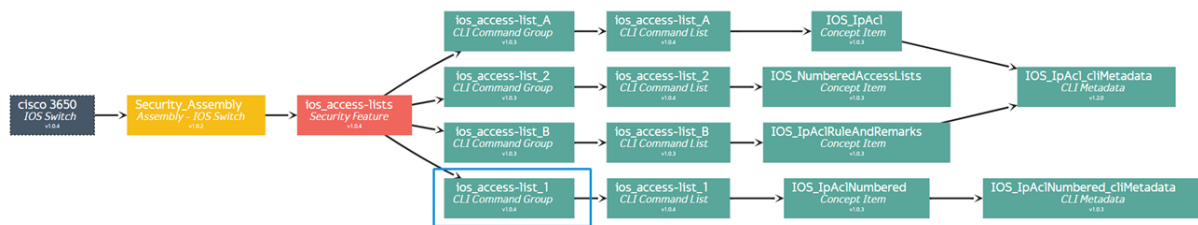
```
ip access-list extended acl-wan-B
no 20 permit tcp any any eq www
no 30 permit tcp any any eq 443
no 40 permit tcp any any eq domain
no 50 permit udp any any eq domain
no 60 permit icmp any any echo-reply log
no 70 permit udp any any eq isakmp log
no 80 permit gre any any log
no 90 permit esp any any log
20 permit tcp any any eq telnet
remark HTTP/HTTPS Traffic
30 permit tcp any any eq www
40 permit tcp any any eq 443
remark DNS Traffic
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit icmp any any echo-reply log
80 permit udp any any eq isakmp log
90 permit gre any any log
100 permit esp any any log
remark BGP Traffic
110 permit tcp any any eq bgp
exit
```

The rules **and remarks** get re-added. (Note: Since the new rule is added at 20, all existing rules from 20 and on are removed and re-add with the new sequence).

## Method 3 Standard/Extended **Numbered** ACLs (Removes the ACL before Updating)



### CLI Command List



**ios\_access-list\_1**

Add Instance Description

---

Naming Convention (regex)

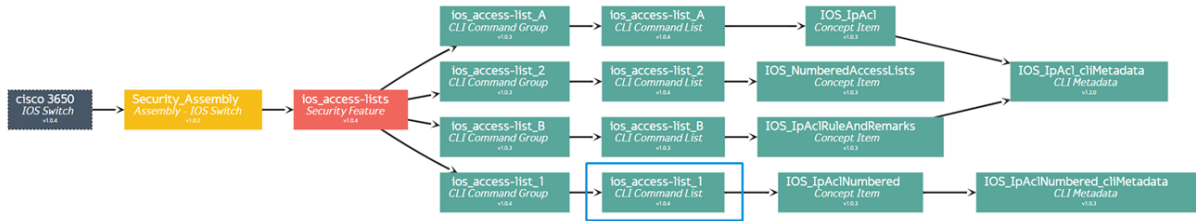
**^1\$**

Disable Group Removal

**cliBlocks**

Available	Selected
<input type="text" value="Search"/> asa_aaa-auth-cli	<b>ios_access-list_1</b>

## CLI Command Group



**ios\_access-list\_1**

Associated Concept Item \*

**IOS\_IpACLNumbered**

CLI Commands

1	access-list 1	remark	SNMP Servers
2	access-list 1	permit	10.111.11.229
3	access-list 1	permit	10.11.175.24
4	access-list 1	permit	10.11.175.25
5	access-list 1	permit	10.111.42.234
6	access-list 1	permit	10.11.175.27
7	access-list 1	permit	10.111.32.245
8	access-list 1	permit	10.111.64.150
9	access-list 1	remark	Syslog Servers
10	access-list 1	permit	10.111.32.246
11	access-list 1	permit	10.11.153.36
12	access-list 1	permit	10.11.43.139
13	access-list 1	permit	10.11.45.139
14	access-list 1	permit	10.111.39.226
15	access-list 1	permit	10.111.11.255
16	access-list 1	permit	10.11.46.180
17	access-list 1	permit	10.111.162.85
18	access-list 1	permit	10.111.42.221

## Initial Provisioning

```

access-list 1 remark SNMP Servers
access-list 1 permit 10.111.11.229
access-list 1 permit 10.11.175.24
access-list 1 permit 10.11.175.25
access-list 1 permit 10.111.42.234
access-list 1 permit 10.11.175.27
access-list 1 permit 10.111.32.245
access-list 1 permit 10.111.64.150
access-list 1 remark Syslog Servers
access-list 1 permit 10.111.32.246
access-list 1 permit 10.11.153.36
access-list 1 permit 10.11.43.139
access-list 1 permit 10.11.45.139
access-list 1 permit 10.111.39.226
access-list 1 permit 10.111.11.255
access-list 1 permit 10.11.46.180
access-list 1 permit 10.111.162.85
access-list 1 permit 10.111.42.221
    
```

## Running-Config

```
c3650-podv2-01#sh run | sec ^access-list 1
access-list 1 remark SNMP Servers
access-list 1 permit 10.111.11.229
access-list 1 permit 10.111.11.255
access-list 1 permit 10.111.162.85
access-list 1 permit 10.111.42.221
access-list 1 permit 10.11.46.180
access-list 1 permit 10.111.39.226
access-list 1 permit 10.11.43.139
access-list 1 permit 10.111.42.234
access-list 1 permit 10.11.45.139
access-list 1 permit 10.111.32.245
access-list 1 permit 10.111.64.150
access-list 1 remark Syslog Servers
access-list 1 permit 10.111.32.246
access-list 1 permit 10.11.175.27
access-list 1 permit 10.11.175.24
access-list 1 permit 10.11.175.25
access-list 1 permit 10.11.153.36
```

## Changes to the Model

```
1 access-list 1 remark SNMP Servers
2 access-list 1 permit 10.111.11.229
3 access-list 1 permit 10.11.175.24
4 access-list 1 permit 10.11.175.25
5 access-list 1 permit 10.111.42.234
6 access-list 1 permit 10.11.175.27
7 access-list 1 permit 10.111.32.245
8 access-list 1 permit 10.111.64.150
9 access-list 1 remark Syslog Servers
10 access-list 1 permit 10.111.32.246
11 access-list 1 permit 10.11.153.36
12 access-list 1 permit 10.11.43.139
13 access-list 1 permit 10.11.45.139
14 access-list 1 permit 10.111.39.226
15 access-list 1 permit 10.111.11.255
16 access-list 1 permit 10.11.46.180
17 access-list 1 permit 10.111.162.85
18 access-list 1 permit 10.111.42.221
19 access-list 1 remark Remote Access
20 access-list 1 permit 10.1.213.46
21 access-list 1 permit 10.11.23.76
22 access-list 1 permit 10.111.13.99
```

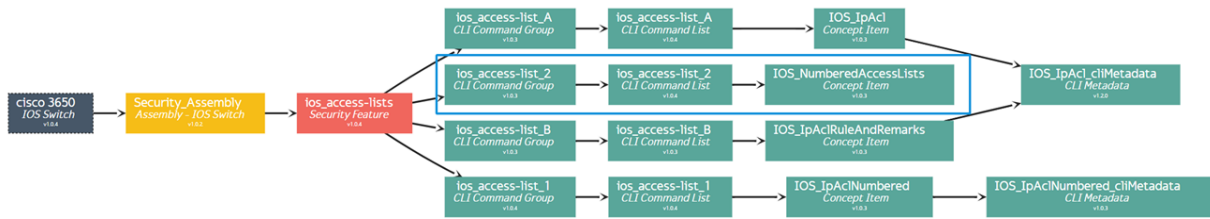
New remark and rules added to the ACL

## Provisioning After Changes

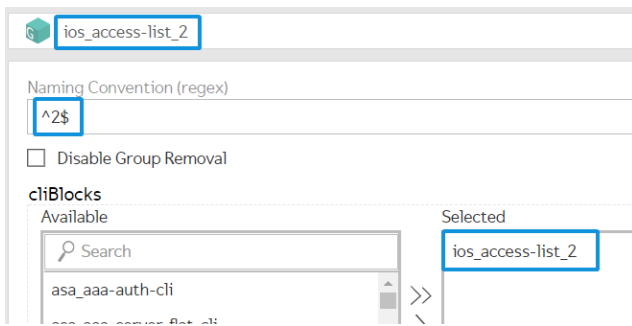
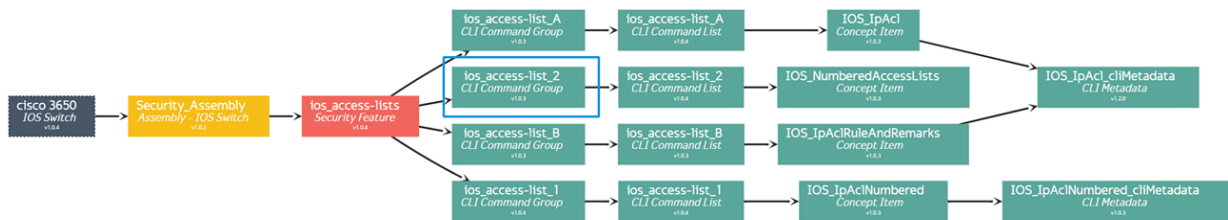
```
no access-list 1
access-list 1 remark SNMP Servers
access-list 1 permit 10.111.11.229
access-list 1 permit 10.11.175.24
access-list 1 permit 10.11.175.25
access-list 1 permit 10.111.42.234
access-list 1 permit 10.11.175.27
access-list 1 permit 10.111.32.245
access-list 1 permit 10.111.64.150
access-list 1 remark Syslog Servers
access-list 1 permit 10.111.32.246
access-list 1 permit 10.11.153.36
access-list 1 permit 10.11.43.139
access-list 1 permit 10.11.45.139
access-list 1 permit 10.111.39.226
access-list 1 permit 10.111.11.255
access-list 1 permit 10.11.46.180
access-list 1 permit 10.111.162.85
access-list 1 permit 10.111.42.221
access-list 1 remark Remote Access
access-list 1 permit 10.1.213.46
access-list 1 permit 10.11.23.76
access-list 1 permit 10.111.13.99
```

The ACL is completely removed before it adds the changes

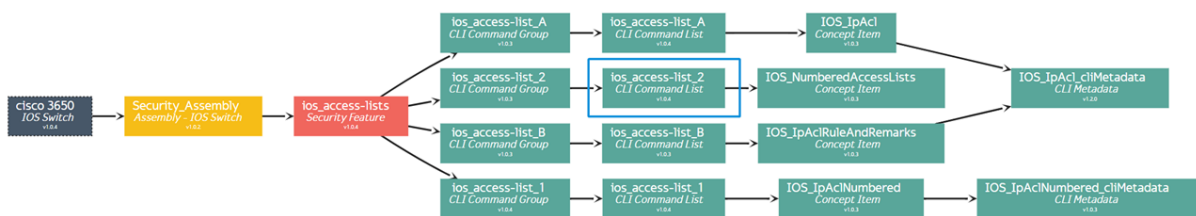
# Method 4 Standard/Extended **Numbered** ACLs (Updates the ACL without removing it)

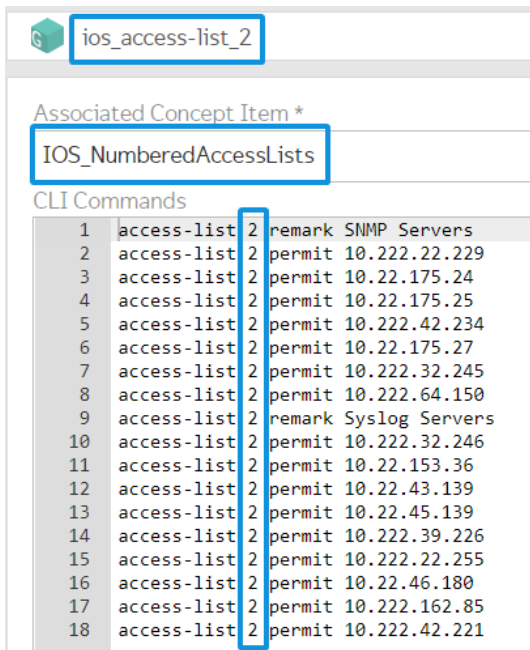


## CLI Command Group



## CLI Command List





The screenshot shows a configuration tool interface. At the top left, there is a Cisco logo and the text 'ios\_access-list\_2'. Below this, there is a section titled 'Associated Concept Item \*' with a box containing 'IOS\_NumberedAccessLists'. Underneath, there is a section titled 'CLI Commands' with a table of 18 numbered rows. Each row contains a command for configuring an access list. The second column of the table is highlighted with a blue box.

Line	Command
1	access-list 2 remark SNMP Servers
2	access-list 2 permit 10.222.22.229
3	access-list 2 permit 10.22.175.24
4	access-list 2 permit 10.22.175.25
5	access-list 2 permit 10.222.42.234
6	access-list 2 permit 10.22.175.27
7	access-list 2 permit 10.222.32.245
8	access-list 2 permit 10.222.64.150
9	access-list 2 remark Syslog Servers
10	access-list 2 permit 10.222.32.246
11	access-list 2 permit 10.22.153.36
12	access-list 2 permit 10.22.43.139
13	access-list 2 permit 10.22.45.139
14	access-list 2 permit 10.222.39.226
15	access-list 2 permit 10.222.22.255
16	access-list 2 permit 10.22.46.180
17	access-list 2 permit 10.222.162.85
18	access-list 2 permit 10.222.42.221

## Initial Provisioning

```
ip access-list standard 2
remark SNMP Servers
permit 10.222.22.229
permit 10.22.175.24
permit 10.22.175.25
permit 10.222.42.234
permit 10.22.175.27
permit 10.222.32.245
permit 10.222.64.150
remark Syslog Servers
permit 10.222.32.246
permit 10.22.153.36
permit 10.22.43.139
permit 10.22.45.139
permit 10.222.39.226
permit 10.222.22.255
permit 10.22.46.180
permit 10.222.162.85
permit 10.222.42.221
exit
```

## Running-Config

```
c3650-podv2-01#sh run | sec ^access-list 2
access-list 2 permit 10.222.32.245
access-list 2 permit 10.222.64.150
access-list 2 remark Syslog Servers
access-list 2 permit 10.222.32.246
access-list 2 permit 10.222.39.226
access-list 2 permit 10.222.42.234
access-list 2 permit 10.222.162.85
access-list 2 permit 10.222.42.221
access-list 2 remark SNMP Servers
access-list 2 permit 10.222.22.229
access-list 2 permit 10.222.22.255
access-list 2 permit 10.22.46.180
access-list 2 permit 10.22.153.36
access-list 2 permit 10.22.175.27
access-list 2 permit 10.22.175.25
access-list 2 permit 10.22.175.24
access-list 2 permit 10.22.45.139
access-list 2 permit 10.22.43.139
```

## Changes to the Model

```
1 access-list 2 remark SNMP Servers
2 access-list 2 permit 10.222.22.229
3 access-list 2 permit 10.22.175.24
4 access-list 2 permit 10.22.175.25
5 access-list 2 permit 10.222.42.234
6 access-list 2 permit 10.22.175.27
7 access-list 2 permit 10.222.32.245
8 access-list 2 permit 10.222.64.150
9 access-list 2 remark Syslog Servers
10 access-list 2 permit 10.222.32.246
11 access-list 2 permit 10.22.153.36
12 access-list 2 permit 10.22.43.139
13 access-list 2 permit 10.22.45.139
14 access-list 2 permit 10.222.39.226
15 access-list 2 permit 10.222.22.255
16 access-list 2 permit 10.22.46.180
17 access-list 2 permit 10.222.162.85
18 access-list 2 permit 10.222.42.221
19 access-list 2 remark Remote Access
20 access-list 2 permit 10.2.213.46
21 access-list 2 permit 10.22.23.76
22 access-list 2 permit 10.222.13.99
```

New remark and rules added to the ACL

## Provisioning After Changes

```
ip access-list standard 2
remark Remote Access
170 permit 10.2.213.46
180 permit 10.22.23.76
190 permit 10.222.13.99
exit
```

The ACL is updated with only the differences

Note: Both the “access-list 2 permit” lines and “ip access-list standard 2” reference the same ACL however the Cisco IOS displays the ACL structure differently so our engine internally transforms the modeled structure to hierarchical to manage the ACL without removing it.



# Gluware Solutions

## Starting the Journey

When your team is ready to begin their enterprise network automation journey toward code-free, error-free security and agility, Gluware Intelligent Network Automation delivers the capability many of our customers require:

- **Flexible Automation** On-prem or cloud-delivered; One app or more
- **Expanded Vendor Support** Growing list of platforms
- **Inclusive Environments** Multi-vendor | Multi-domain | Multi-cloud
- **Quality User Experience** Enterprise-class features and dashboards
- **Multiple Payment Offerings** Get started your way

When you are ready to get started, our team of automation experts are ready to help.

[sales@gluware.com](mailto:sales@gluware.com)



2020 L Street, Suite 130  
Sacramento, CA 95811

[www.gluware.com](http://www.gluware.com)