

CISCO SYSTEMS - CX CENTERS ENTERPRISE NETWORKING

TOTD: New Configuration Archive feature -
Export Device configurations to an
encrypted zip file

Prepared for: Cisco DNA Customer, Solutions Support

Prepared by: Tomas de Leon, Technical Leader

September 21, 2020

Document number: 09212020_v1

CISCO SYSTEMS - CX CENTERS ENTERPRISE NETWORKING

TECHNOTE OF THE DAY (TOTD) -- NEW CONFIGURATION ARCHIVE FEATURE - EXPORT DEVICE CONFIGURATIONS TO AN ENCRYPTED ZIP FILE IN CISCO DNA CENTER VERSION 2.1.2.X

Objective

The objective of this document is to show users the new Configuration Archive feature. A new Rest API was added to export device configurations to an encrypted zip file. The new API was added in Cisco DNA Center version 2.1.2.0.

Goals

Provide an awareness of the new configuration archive feature and to provide an example of using the API with the Postman Rest API Client.

The following technote is written against the Release of Cisco DNA Center version 2.1.2.0.

Reference Information:

- Cisco DNA Center version 2.1.2.x0
- Postman Version 7.32.0 (7.32.0)

CISCO SYSTEMS - CX CENTERS ENTERPRISE NETWORKING

CONFIGURATION ARCHIVE FEATURE

In the Release of Cisco DNA Center version 2.1.2.0, there is only one API URL task provided for the Configuration Archive feature. The current API task is to export device configurations to an encrypted zip file. My understanding is that more API URL task will be coming in future releases but this is always subject to change.

Platform . Developer Toolkit . APIs

Configuration Archive

Name	Description
<i>Export Device configurations</i>	<i>Export Device configurations to an encrypted zip file.</i>
Method	URL
POST	<a href="https://<_dnac.ip.address_>/dna/intent/api/v1/network-device-archive/cleartext">https://<_dnac.ip.address_>/dna/intent/api/v1/network-device-archive/cleartext

Model Schema

payload:

```
{  
  "deviceId": "<List of device uuids to be exported>",  
  "password": "<Password to export the file. Same should be used to view the file>"  
}
```

Note: The schema payload is not listed in the Cisco DNA Center screens or the help. A CDET has been created to add this documentation to the UI in an upcoming release.

Platform . Developer Toolkit . APIs (cont.)

Cisco DNA Center UI Example:

The screenshot shows the Cisco DNA Center Platform . Developer Toolkit interface. The top navigation bar includes the Cisco DNA Center logo, search, help, and cloud icons. Below the navigation, there are tabs for APIs, Integration Flows, Multivendor Support, and Events. The APIs tab is selected. On the left, a sidebar shows Site Management and Site Management. Under Site Management, there is a link to Configuration Archive. The main content area displays the Configuration Archive API details. The API name is "Export Device configurations". It is a POST method with the URL `/network-device-archive/cleartext`. A description states: "Export Device configurations to an encrypted zip file." There is also a "... more" button.

This screenshot provides a detailed view of the "Export Device configurations" API endpoint. At the top, it says "Export Device configurations".

DESCRIPTION

Export Device configurations to an encrypted zip file.

Method	URL
POST	https://172.18.217.184/dna/intent/api/v1/network-device-archive/cleartext

PARAMETERS

Request Headers Parameters

Name	Description	DataType	Default Value	Required
Content-Type		string	application/json	true

RESPONSES

Response Codes

Code	Message
200	

Try It

Method	Public URL :	
POST	https://172.18.217.184/dna/intent/api/v1/network-device-archive/cleartext	
Name	Description	Value
Headers		
Content-Type*		application/json
Body	<pre>1 { 2 3 "deviceId": "<List of device uuids to be exported>", 4 5 "password": "<Password to export the file. Same should be used to view the file>" 6 7 }</pre>	
		<button>Cancel</button> <button>Run</button>

Note: The schema payload is not listed in the Cisco DNA Center screens or the help. A CDET has been created to add this documentation to the UI in an upcoming release.

USING THE POSTMAN REST API CLIENT FOR EXPORTING DEVICE CONFIGURATIONS

Use Case Scenario - Export Device configurations to an encrypted zip file using the Postman Rest API Client.

- Cisco DNA Center version 2.1.2.0
- Postman Version 7.32.0 (7.32.0)

STEP 1 - GET TOKEN - Authentication/Authorization

<u>Method</u>	<u>URL</u>
POST	<a href="https://<_dnac.ip.address_>/dna/system/api/v1/auth/token">https://<_dnac.ip.address_>/dna/system/api/v1/auth/token

Response:

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpxVCJ9.eyJzdWIiOiIzjU30WQwNWQxZDZkNTAwOGJlOTdhNWYiLCJhdXRoU291cmNlIjoizXh0ZXJuYWwiLCJ0ZW5hbnROYW1lIjoive5UMCISinJvbGVzIjpBIjVLNDc00DJhN2E4MDQ3MDBiZjhizTBLzjJdLCJ0ZW5hbnRJZCI6IjVlNDc00DJhN2E4MDQ3MDBiZjhizTBLZCISimV4cCI6MTYwMDYxNTI2MywiaWF0IjoxNjAwNjExNjYzLCJqdGki0ijYjA0NDQzM1jYjRiLTQ4ZjQtOTE2YS1iMGY4YmQzM5NmIiLCJ1c2VybmxFtZSI6InYxYWRTaw4ifQ.hEKDnflrGfxf10-H9HOHLJIGSs000BgpCp_C8a7R8Llk_gjMmuXwxQxomLQmwsG6j3v9xe6Xje9Sh3-_pPv0RjQxteUhsZunGFhhCx bPgSlhpLhedAjeXAofif0kD1jgGgioRRufbtQMqr4VdoMAHSGh8xHH7RgCPn8r19eFzmS327tIkLRQFfb_yIURp3awpWtCsStPCyzt mNxogkjtQALImzJstoKELW_W-FvqDGphDldQ86x6Z0Xt_Z_IAwAm7reLxe40rxZeP3DGqnxceD_Hr50Vzq2xY_lWd2knH71ZGjLIYM FvqDGphDldQ86x6Z0Xt_Z_IAwAm7reLxe40rxZeP3DGqnxceD_Hr50Vzq2xY_lWd2knH71ZGjLIYMKiNBAMpppFbfpsvVLAsxgY4WzDIkq5ibg
```

The screenshot shows the Postman interface with the following details:

- Request URL:** https://172.18.217.184/dna/system/api/v1/auth/token
- Method:** POST
- Authorization:** Basic Auth (Username: v1admin, Password: [redacted])
- Body:** JSON response containing the token.
- Response Headers:** 200 OK, 900 ms, 1.18 KB
- Response Body (Pretty Print):**

```

1 "Token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpxVCJ9.
2   eyJzdWIiOiIzjU30WQwNWQxZDZkNTAwOGJlOTdhNWYiLCJhdXRoU291cmNlIjoizXh0ZXJuYWwiLCJ0ZW5hbnROYW1lIjoive5UMCISinJvbGVzIjpBIjVLNDc00DJhN2E4MDQ3MDBiZjhizTBLzjJdLCJ0ZW5hbnRJZCI6IjVlNDc00DJhN2E4MDQ3MDBiZjhizTBLZCISimV4cCI6MTYwMDYxNTI2MywiaWF0IjoxNjAwNjExNjYzLCJqdGki0ijYjA0NDQzM1jYjRiLTQ4ZjQtOTE2YS1iMGY4YmQzM5NmIiLCJ1c2VybmxFtZSI6InYxYWRTaw4ifQ.hEKDnflrGfxf10-H9HOHLJIGSs000BgpCp_C8a7R8Llk_gjMmuXwxQxomLQmwsG6j3v9xe6Xje9Sh3-_pPv0RjQxteUhsZunGFhhCx bPgSlhpLhedAjeXAofif0kD1jgGgioRRufbtQMqr4VdoMAHSGh8xHH7RgCPn8r19eFzmS327tIkLRQFfb_yIURp3awpWtCsStPCyzt mNxogkjtQALImzJstoKELW_W-FvqDGphDldQ86x6Z0Xt_Z_IAwAm7reLxe40rxZeP3DGqnxceD_Hr50Vzq2xY_lWd2knH71ZGjLIYM FvqDGphDldQ86x6Z0Xt_Z_IAwAm7reLxe40rxZeP3DGqnxceD_Hr50Vzq2xY_lWd2knH71ZGjLIYMKiNBAMpppFbfpsvVLAsxgY4WzDIkq5ibg"
3
  
```

STEP 2 - GET DEVICE INFO using managementIpAddressMethod

GET

URLhttps://<_dnac.ip.address_>/dna/intent/api/v1/network-device?managementIpAddress=<_device.mgmt.ip.address_>

- Test Case Parameters

NETWORK DEVICE INFORMATION

NAME	MGMT_IP	PLATFORM	SERIAL_NUM
deadbeef-1.dna.local	192.168.0.101	C9200L-48T-4G	JAE22490HPJ
deadbeef-2.dna.local	192.168.0.102	C9200L-48T-4G	JAE22490HGT

Response: (abbreviated)

```
{  
  "response": [  
    {  
      "family": "Switches and Hubs",  
      "collectionStatus": "Managed",  
      "serialNumber": "JAE22490HPJ",  
      "macAddress": "08:ec:f5:88:0d:80",  
      "hostname": "deadbeef-1.dna.local",  
      "managementState": "Managed",  
      "managementIpAddress": "192.168.0.101",  
      "platformId": "C9200L-48T-4G",  
      "reachabilityStatus": "Reachable",  
      "series": "Cisco Catalyst 9200 Series Switches",  
      "snmpContact": "Tomas de Leon - CX 919.867.5309",  
      "snmpLocation": "Cisco Systems, North Carolina",  
      "deviceSupportLevel": "Supported",  
      "softwareType": "IOS-XE",  
      "softwareVersion": "17.3.1",  
      "inventoryStatusDetail": "<status><general code=\"SUCCESS\"/></status>",  
      "type": "Cisco Catalyst 9200L Switch Stack",  
      "role": "ACCESS",  
    }]
```

```
"instanceUuid": "2862a8ba-2e2c-4560-8d21-9e6188d862ed",
"instanceTenantId": "5e47482a7a804700bf8be0ed",
"id": "2862a8ba-2e2c-4560-8d21-9e6188d862ed"
},
],
"version": "1.0"
}
```

Response: (abbreviated)

```
{
  "response": [
    {
      "family": "Switches and Hubs",
      "hostname": "deadbeef-2.dna.local",
      "macAddress": "08:ec:f5:93:fb:00",
      "serialNumber": "JAE22490HGT",
      "collectionStatus": "Managed",
      "managementIpAddress": "192.168.0.102",
      "platformId": "C9200L-48T-4G",
      "reachabilityStatus": "Reachable",
      "series": "Cisco Catalyst 9200 Series Switches",
      "snmpContact": "Tomas de Leon - CX 919.867.5309",
      "snmpLocation": "Cisco Systems, North Carolina",
      "inventoryStatusDetail": "<status><general code=\"SUCCESS\"/></status>",
      "managementState": "Managed",
      "type": "Cisco Catalyst 9200L Switch Stack",
      "role": "ACCESS",
      "deviceSupportLevel": "Supported",
      "softwareType": "IOS-XE",
      "softwareVersion": "17.3.1",
      "instanceTenantId": "5e47482a7a804700bf8be0ed",
      "instanceUuid": "e0526635-4c7d-4908-b82b-563c80597d65",
      "id": "e0526635-4c7d-4908-b82b-563c80597d65"
    }
  ],
  "version": "1.0"
}
```

Two screenshots of the Postman API client showing the results of a GET request to Cisco DNA Center's Configuration Archive feature.

Screenshot 1 (Management IP Address: 192.168.0.101):

```

29     "managementIpAddress": "192.168.0.101",
30     "platformId": "C9200L-48T-4G",
31     "reachabilityFailureReason": "",
32     "reachabilityStatus": "Reachable",
33     "series": "Cisco Catalyst 9200 Series Switches",
34     "snmpContact": "Tomas de Leon - CX 919.867.5309",
35     "snmpLocation": "Cisco Systems, North Carolina",
36     "deviceSupportLevel": "Supported",
37     "softwareType": "IOS-XE",
38     "softwareVersion": "17.3.1",
39     "inventoryStatusDetail": "<status><general code=\"SUCCESS\"/></status>",
40     "lastUpdateTime": 1600597632020,
41     "roleSource": "AUTO",
42     "description": "Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 17.3.1, RELEASE SOFTWARE (fc5) Technical Support: http://www.Cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc. Compiled Fri 07-Aug-20 17:37 by mc",
43     "location": null,
44     "type": "Cisco Catalyst 9200L Switch Stack",
45     "role": "ACCESS",
46     "instanceUuid": "2862a8ba-2e2c-4560-8d21-9e6188d862ed",
47     "instanceTenantId": "5e47482a7a804700bf8be0ed",
48     "id": "2862a8ba-2e2c-4560-8d21-9e6188d862ed"
49   }
50
  
```

Screenshot 2 (Management IP Address: 192.168.0.102):

```

25     "managementIpAddress": "192.168.0.102",
26     "platformId": "C9200L-48T-4G",
27     "reachabilityFailureReason": "",
28     "reachabilityStatus": "Reachable",
29     "series": "Cisco Catalyst 9200 Series Switches",
30     "snmpContact": "Tomas de Leon - CX 919.867.5309",
31     "snmpLocation": "Cisco Systems, North Carolina",
32     "tagCount": "0",
33     "tunnelUdpPort": null,
34     "uptimeSeconds": 2891785,
35     "waaDeviceMode": null,
36     "collectionInterval": "Global Default",
37     "inventoryStatusDetail": "<status><general code=\"SUCCESS\"/></status>",
38     "managementState": "Managed",
39     "location": null,
40     "type": "Cisco Catalyst 9200L Switch Stack",
41     "role": "ACCESS",
42     "deviceSupportLevel": "Supported",
43     "softwareType": "IOS-XE",
44     "softwareVersion": "17.3.1",
45     "roleSource": "AUTO",
46     "instanceTenantId": "5e47482a7a804700bf8be0ed",
47     "instanceUuid": "e0526635-4c7d-4908-b82b-563c80597d65",
48     "id": "e0526635-4c7d-4908-b82b-563c80597d65"
49
  
```

STEP 3 - EXPORT CONFIGURATION using DEVICE_IDMethod URLPOST https://<dnac.ip.address_>/dna/intent/api/v1/network-device-archive/cleartextBody

```
{  
  "deviceId": [  
    "2862a8ba-2e2c-4560-8d21-9e6188d862ed",  
    "e0526635-4c7d-4908-b82b-563c80597d65"  
,  
  "password": "Cisco123#"  
}
```

Response:

```
{  
  "response": {  
    "taskId": "fa033bb2-81ab-46df-a39c-4455e9410e36",  
    "url": "/api/v1/task/fa033bb2-81ab-46df-a39c-4455e9410e36"  
}
```

The screenshot shows the Postman application interface. The header bar displays 'TOTD -- Config Archive - EXPORT CONFIGURATION using DEVICE_ID'. The main area shows a POST request to <https://172.18.217.184/dna/intent/api/v1/network-device-archive/cleartext>. The 'Body' tab is selected, showing the JSON payload from the previous step. The response tab shows a 202 Accepted status with the task ID and URL. The bottom section shows the raw JSON response.

```
1  {  
2    "deviceId": [  
3      "2862a8ba-2e2c-4560-8d21-9e6188d862ed",  
4      "e0526635-4c7d-4908-b82b-563c80597d65"  
5    ],  
6    "password": "Cisco123#"  
7  }  
  
1  {  
2    "response": {  
3      "taskId": "fa033bb2-81ab-46df-a39c-4455e9410e36",  
4      "url": "/api/v1/task/fa033bb2-81ab-46df-a39c-4455e9410e36"  
5    },  
6    "version": "1.0"  
7  }
```

STEP 4 - GET FILE INFO using TASK_ID

Method URL

GET https://<dnac.ip.address>/api/v1/task/<_task.id_>

From Step 3:

"taskId": "**fa033bb2-81ab-46df-a39c-4455e9410e36**"

Response: (abbreviated)

```
{
  "response": {
    "version": 1600613167386,
    "endTime": 1600613169009,
    "startTime": 1600613167384,
    "progress": "Device configuration Successfully exported as password protected ZIP.",
    "additionalStatusURL": "/api/v1/file/4962fff5-33e7-49f5-a7b1-b7c9731600b3",
    "lastUpdate": 1600613167386,
  }
}
```

The screenshot shows the Postman interface with the following details:

- Method:** GET
- URL:** <https://172.18.217.184/api/v1/task/fa033bb2-81ab-46df-a39c-4455e9410e36>
- Headers:** (9) - This request does not have a body
- Body:** JSON - The response body is displayed in JSON format, matching the abbreviated response from Step 4.
- Status:** 200 OK
- Time:** 61 ms
- Size:** 1.06 KB

```

1  [
2    "response": {
3      "version": 1600613167386,
4      "endTime": 1600613169009,
5      "startTime": 1600613167384,
6      "progress": "Device configuration Successfully exported as password protected ZIP.",
7      "additionalStatusURL": "/api/v1/file/4962fff5-33e7-49f5-a7b1-b7c9731600b3",
8      "lastUpdate": 1600613167386,
9      "isError": false,
10     "rootId": "fa033bb2-81ab-46df-a39c-4455e9410e36",
11     "serviceType": "NCAR",
12     "username": "NCAR88888",
13     "instanceTenantId": "5e47482a7a804700bf8be0ed",
14     "id": "fa033bb2-81ab-46df-a39c-4455e9410e36"
15   },
16   "version": "1.0"
17 ]

```

STEP 5 - GET FILE ZIPPED FILE using additionalStatusURL

<u>Method</u>	<u>URL</u>
GET	<a href="https://<_dnac.ip.address_>/<_additionalStatusURL.string_>">https://<_dnac.ip.address_>/<_additionalStatusURL.string_>

From Step 4:

"additionalStatusURL": "/api/v1/file/4962fff5-33e7-49f5-a7b1-b7c9731600b3",

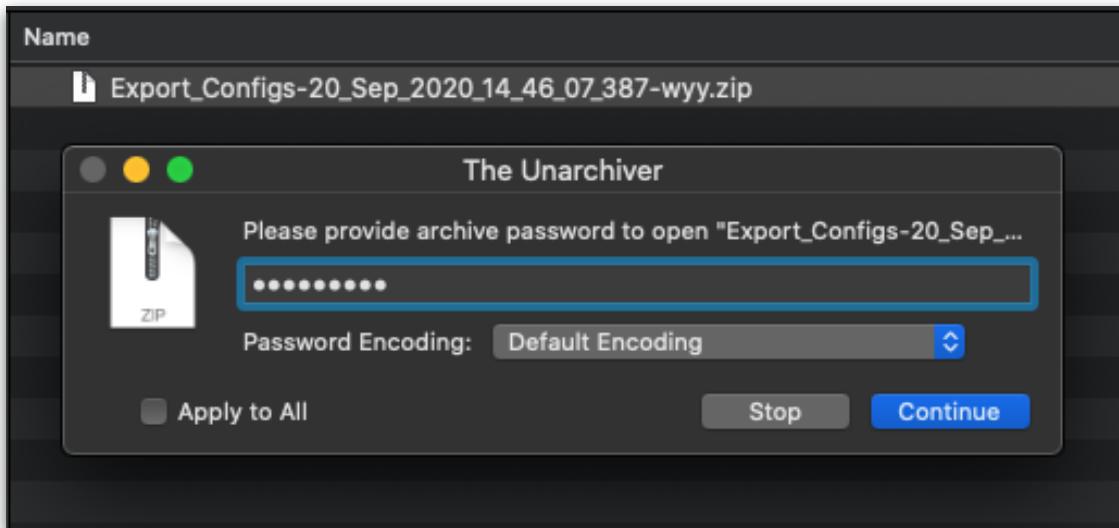
Response: (encoded text & symbols)

- Click on the "Save Response" Dropdown Arrow and Select "Save To a file"

- Select the [File Name](#), Select the [Download location](#) of the Zipped File, and [Save](#)



- Expand the downloaded zipped file
- Enter the Password used in Step 3



- Enclosed in the Directory for each Device will be the [RUNNING CONFIG](#), [STARTUP CONFIG](#), and [VLAN DATA](#)

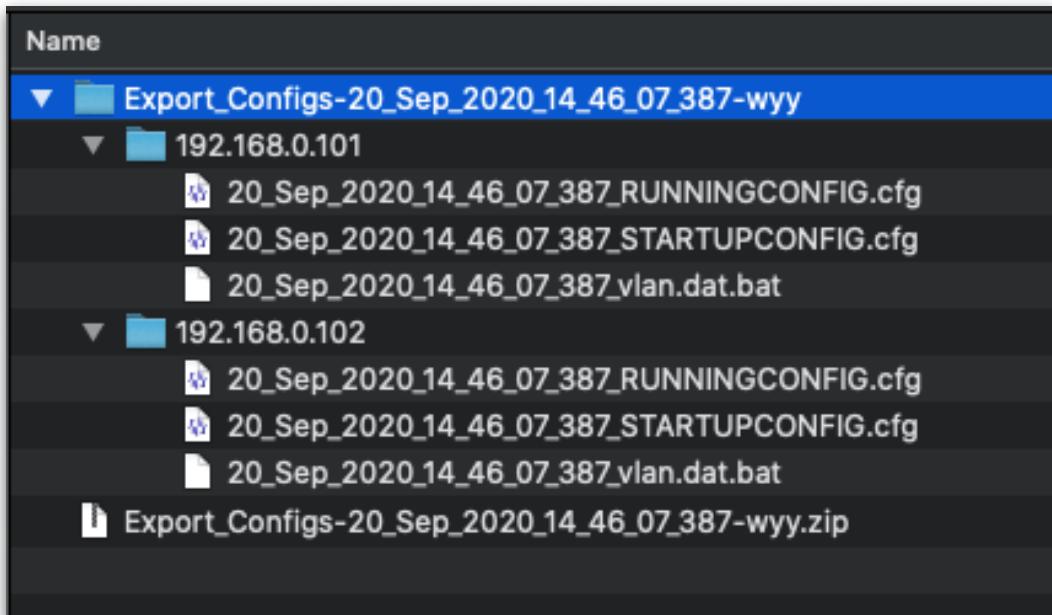
Export_Configs-20_Sep_2020_14_46_07_387-wyy.zip

```
Configuration-Archive $ ls -lR *
-rw-r--r--@ 1 tdeleon  staff  28681 Sep 20 10:52 Export_Configs-20_Sep_2020_14_46_07_387-wyy.zip
```

```
Export_Configs-20_Sep_2020_14_46_07_387-wyy:
total 0
drwxr-xr-x@ 5 tdeleon  staff   160 Sep 20 10:58 192.168.0.101
drwxr-xr-x@ 5 tdeleon  staff   160 Sep 20 10:58 192.168.0.102
```

```
Export_Configs-20_Sep_2020_14_46_07_387-wyy/192.168.0.101:
total 112
-rwxr-xr-x@ 1 tdeleon  staff  28539 Sep 20 2020 20_Sep_2020_14_46_07_387_RUNNINGCONFIG.cfg
-rwxr-xr-x@ 1 tdeleon  staff  22623 Sep 20 2020 20_Sep_2020_14_46_07_387_STARTUPCONFIG.cfg
-rwxr-xr-x@ 1 tdeleon  staff    556 Sep 20 2020 20_Sep_2020_14_46_07_387_vlan.dat.bat
```

```
Export_Configs-20_Sep_2020_14_46_07_387-wyy/192.168.0.102:
total 112
-rwxr-xr-x@ 1 tdeleon  staff  28504 Sep 20 2020 20_Sep_2020_14_46_07_387_RUNNINGCONFIG.cfg
-rwxr-xr-x@ 1 tdeleon  staff  22588 Sep 20 2020 20_Sep_2020_14_46_07_387_STARTUPCONFIG.cfg
-rwxr-xr-x@ 1 tdeleon  staff    804 Sep 20 2020 20_Sep_2020_14_46_07_387_vlan.dat.bat
```



```
Configuration-Archive $ ls -lR *
-rw-r--r--@ 1 tdeleon  staff  28681 Sep 20 10:52 Export_Configs-20_Sep_2020_14_46_07_387-wyy.zip
drwxr-xr-x@ 5 tdeleon  staff   160 Sep 20 10:58 192.168.0.101
drwxr-xr-x@ 5 tdeleon  staff   160 Sep 20 10:58 192.168.0.102

Export_Configs-20_Sep_2020_14_46_07_387-wyy/192.168.0.101:
total 112
-rw-rxr-x@ 1 tdeleon  staff  28539 Sep 20 2020 20_Sep_2020_14_46_07_387_RUNNINGCONFIG.cfg
-rw-rxr-x@ 1 tdeleon  staff  22623 Sep 20 2020 20_Sep_2020_14_46_07_387_STARTUPCONFIG.cfg
-rw-rxr-x@ 1 tdeleon  staff     556 Sep 20 2020 20_Sep_2020_14_46_07_387_vlan.dat.bat

Export_Configs-20_Sep_2020_14_46_07_387-wyy/192.168.0.102:
total 112
-rwrxr-x@ 1 tdeleon  staff  28504 Sep 20 2020 20_Sep_2020_14_46_07_387_RUNNINGCONFIG.cfg
-rwrxr-x@ 1 tdeleon  staff  22588 Sep 20 2020 20_Sep_2020_14_46_07_387_STARTUPCONFIG.cfg
-rwrxr-x@ 1 tdeleon  staff     804 Sep 20 2020 20_Sep_2020_14_46_07_387_vlan.dat.bat

Configuration-Archive $
```

OTHER WAYS TO GET DEVICE CONFIGURATION INFO FROM THE CISCO DNA CENTER UI

Cisco DNA Center UI provides some other ways to get device configuration information:

- Provision.Inventory.Device - **Export CLI Output**
- Provision.Inventory.Device - **Command Runner**

The screenshot shows the Cisco DNA Center Inventory page. The top navigation bar includes 'Provision', 'Network Devices', and 'Inventory'. On the right side of the header are search, help, and cloud icons. Below the header, the page title is 'DEVICES (2)' and the location is 'Global > Deadbeef'. The 'FOCUS' dropdown is set to 'Inventory'. The main content area displays two network devices in a table:

	Device Name	IP Address	Reachability	Manageability	Compliance	Health Score	Site	⋮
<input type="checkbox"/>	deadbeef-1.dna.local ASSURANCE, DEADBEEF	192.168.0.101	Reachable	Managed	Compliant	8	.../Area-1/Building-1	
<input type="checkbox"/>	deadbeef-2.dna.local DEADBEEF	192.168.0.102	Reachable	Managed	Compliant	8	.../Sub-Area-2/Buildir	

Export CLI Output

All Devices > deadbeef-1.dna.local

deadbeef-1.dna.local

Run Commands View 360 Last updated: 11:12 AM Refresh

ASSURANCE DEADBEEF

Reachable | Managed | IP Address: 192.168.0.101 | Device Model: Cisco Catalyst 9200L Switch Stack | Role: ACCESS | Uptime: 33 days 12 hrs | Site: Global/Deadbeef/Area-1/Building-1

DETAILS

- Interfaces
- Ethernet Ports
- VLANs
- Hardware & Software
- Configuration**
- Power
- Fans

COMPLIANCE

Building configuration...

```
Current configuration : 28541 bytes
!
! Last configuration change at 18:49:27 UTC Wed Sep 16 2020 by netadmin1
! NVRAM config last updated at 18:49:35 UTC Wed Sep 16 2020 by netadmin1
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone year
service password-encryption
service call-home
no platform punt-keepalive disable-kernel-core
!
```

Search Export CLI Output

All Devices > deadbeef-1.dna.local

deadbeef-1.dna.local

Run Commands View 360 Last updated: 11:12 AM Refresh

ASSURANCE DEADBEEF

Reachable | Managed | IP Address: 192.168.0.101 | Device Model: Cisco Catalyst 9200L Switch Stack | Role: ACCESS | Uptime: 33 days 12 hrs | Site: Global/Deadbeef/Area-1/Building-1

DETAILS

- Interfaces
- Ethernet Ports
- VLANs
- Hardware & Software
- Configuration**
- Power
- Fans

COMPLIANCE

Opening Configuration-deadbeef-1.dna.local@1...

You have chosen to open:

...dna.local@192.168.0.101-09202020_111346.txt
which is: CSV file (24.8 KB)
from: blob:

What should Firefox do with this file?

Open with Choose... Save File Do this automatically for files like this from now on.

Cancel OK

a+
-LOG: CLI_COMMANDS-->: \$_cli_msg"

Export CLI Output (cont.)

The screenshot shows the Cisco DNA Center interface for managing configuration archives. At the top, there's a navigation bar with icons for Home, Devices, Network Policies, Security Policies, and Configuration. Below that is a search bar and a user profile icon. The main area has a title 'Configuration-Archive' and a sub-section 'Configuration-Archive > Configuration'. A table lists configuration files with columns for Name, Last Modified, and Size. One file is selected: 'Configuration-deadbeef-1.dna.local@192.168.0.101-09202020_111346.txt'. Below the table is a large text area showing the contents of the selected configuration file. The configuration includes details like version 17.3, service timestamps, and AAA settings. The text area has scroll bars on the right and bottom.

```
Configuration-Archive $ cat Configuration-deadbeef-1.dna.local@192.168.0.101-09202020_111346.txt

Building configuration...                               Interfaces
Current configuration : 28541 bytes                  Ethernet Ports
!
! Last configuration change at 18:49:27 UTC Wed Sep 16 2020 by netadmin
! NVRAM config last updated at 18:49:35 UTC Wed Sep 16 2020 by netadmin
!
version 17.3                                         Hardware & Software
service timestamps debug datetime msec               Configuration
service timestamps log datetime msec show-timezone year
service password-encryption
service call-home
no platform punt-keepalive disable-kernel-core NING
!
hostname deadbeef-1                                 Power
!
!
vrf definition Mgmt-vrf                           Fans
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
enable secret 8 xxxxxxxx
enable password 7 xxxxxxxx
!
!
!
!
aaa new-model
!
!
!
aaa group server tacacs+ dnac-network-tacacs-group
  server name dnac-tacacs_192.168.111.85
!
aaa group server radius dnac-client-radius-group
  server name dnac-radius_192.168.111.85
  ip radius source-interface Loopback0
!
aaa authentication login default local
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication login VTY_authen group dnac-network-tacacs-group local
aaa authentication dot1x default group dnac-client-radius-group
aaa authorization exec default local
aaa authorization exec VTY_author group dnac-network-tacacs-group local if-authenticated
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group dnac-client-radius-group
aaa accounting exec default start-stop group dnac-network-tacacs-group
!
!
```

Command Runner

This screenshot shows the Cisco DNA Center interface for the device `deadbeef-1.dna.local`. The top navigation bar includes links for `All Devices`, `deadbeef-1.dna.local`, `Run Commands` (which is highlighted with a red oval), `View 360`, `Last updated: 11:17 AM`, and `Refresh`. Below the navigation, device status information is displayed: `Reachable`, `Managed`, `IP Address: 192.168.0.101`, `Device Model: Cisco Catalyst 9200L Switch Stack`, `Role: ACCESS`, `Uptime: 33 days 12 hrs`, and `Site: Global/Deadbeef/Area-1/Building-1`.

The left sidebar contains sections for `ASSURANCE` and `DEADBEEF`, and a collapsed section for `DETAILS` which includes `Interfaces` (Ethernet Ports, VLANs), `Hardware & Software` (Configuration, Power, Fans), and `COMPLIANCE` (Summary). The `COMPLIANCE` section is currently selected.

The main content area displays a `Compliance Summary` with the message "No events detected to trigger compliance check". It includes three cards:

- STARTUP VS RUNNING CONFIGURATION**: In-sync since Aug 28th, 2020, 01:19:25 PM. Compliance last run on: Sep 19th, 2020, 07:00:00 PM. No. of lines in STARTUP Config: **588**. No. of lines in RUNNING Config: **588**.
- SOFTWARE IMAGE**: Compliant since Aug 28th, 2020, 02:04:15 PM. Compliance last run on: Sep 19th, 2020, 07:00:00 PM. Version: **17.03.01...**. Golden Image Version: **17.03.01.0.351**.
- CRITICAL SECURITY ADVISORIES**: compliant since Aug 28th, 2020, 02:10:17 PM. Compliance last run on: Sep 19th, 2020, 07:00:00 PM. Count: **0**.

This screenshot shows the Cisco DNA Center interface for the device `deadbeef-1.dna.local`. The top navigation bar includes links for `All Devices`, `deadbeef-1.dna.local`, `Run Commands` (highlighted with a red oval), `View 360`, `Last updated: 11:19 AM`, and `Refresh`. Below the navigation, device status information is displayed: `Reachable`, `Managed`, `IP Address: 192.168.0.101`, `Device Model: Cisco Catalyst 9200L Switch Stack`, `Role: ACCESS`, `Uptime: 33 days 12 hrs`, and `Site: Global/Deadbeef/Area-1/Building-1`.

The left sidebar contains sections for `ASSURANCE` and `DEADBEEF`, and a collapsed section for `DETAILS` which includes `Interfaces` (Ethernet Ports, VLANs), `Hardware & Software` (Configuration, Power, Fans), and `COMPLIANCE` (Summary). The `COMPLIANCE` section is currently selected.

A red arrow points from the `Run Commands` button in the main header to a separate window titled `Command Runner`. This window displays the message "Welcome to Cisco DNA Center command runner." It provides instructions: "You can access this window from anywhere using the key combination Q+T. You can access recently viewed devices using the key combination Q+D." A note states: "Note: You can enter 'man' anytime to get the list of currently supported commands and shortcuts." The command prompt shows `deadbeef-1.dna.local>`.

Command Runner (cont.)

All Devices > deadbeef-1.dna.local

deadbeef-1.dna.local Run Commands View 360 Last updated: 11:19 AM Refresh

ASSURANCE DEADBEEF

Reachable | Managed | IP Address: 192.168.0.101 | Device Model: Cisco Catalyst 9200L Switch Stack | Role: ACCESS | Uptime: 33 days 12 hrs | Site: Global/Deadbeef/Area-1/Building-1

DETAILS

- Interfaces
- Ethernet Ports
- VLANs
- Hardware & Software
- Configuration
- Power
- Fans

COMPLIANCE

- Summary

Compliance Summary

No events detected to trigger compliance check

STARTUP VS RUNNING CONFIGURATION

In-sync since Aug 28th, 2020, 01:19:25 PM
Compliance last run on: Sep 19th, 2020, 07:00:00 PM

No. of lines in STARTUP Config: 588
No. of lines in RUNNING Config: 588

Command Runner deadbeef-1.dna.local@192.168.0.101

Welcome to Cisco DNA Center command runner.

You can access this window from anywhere using the key combination Q+T. You can access recently viewed devices using the key combination Q+D.

Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.

```
deadbeef-1.dna.local> show run
Building configuration...
Current configuration : 28541 bytes
!
! Last configuration change at 18:49:27 UTC Wed Sep 16 2020 by netadmin1
! NVRAM config last updated at 18:49:35 UTC Wed Sep 16 2020 by netadmin1
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone year
service password-encryption
service call-home
no platform punt-keepalive disable-kernel-core
!
hostname deadbeef-1
!
```

All Devices > deadbeef-1.dna.local

deadbeef-1.dna.local Run Commands View 360 Last updated: 11:19 AM Refresh

ASSURANCE DEADBEEF

Reachable | Managed | IP Address: 192.168.0.101 | Device Model: Cisco Catalyst 9200L Switch Stack | Role: ACCESS | Uptime: 33 days 12 hrs | Site: Global/Deadbeef/Area-1/Building-1

DETAILS

- Interfaces
- Ethernet Ports
- VLANs
- Hardware & Software
- Configuration
- Power
- Fans

COMPLIANCE

- Summary

Compliance Summary

No events detected to trigger compliance check

STARTUP VS RUNNING CONFIGURATION

In-sync since Aug 28th, 2020, 01:19:25 PM
Compliance last run on: Sep 19th, 2020, 07:00:00 PM

No. of lines in STARTUP Config: 588
No. of lines in RUNNING Config: 588

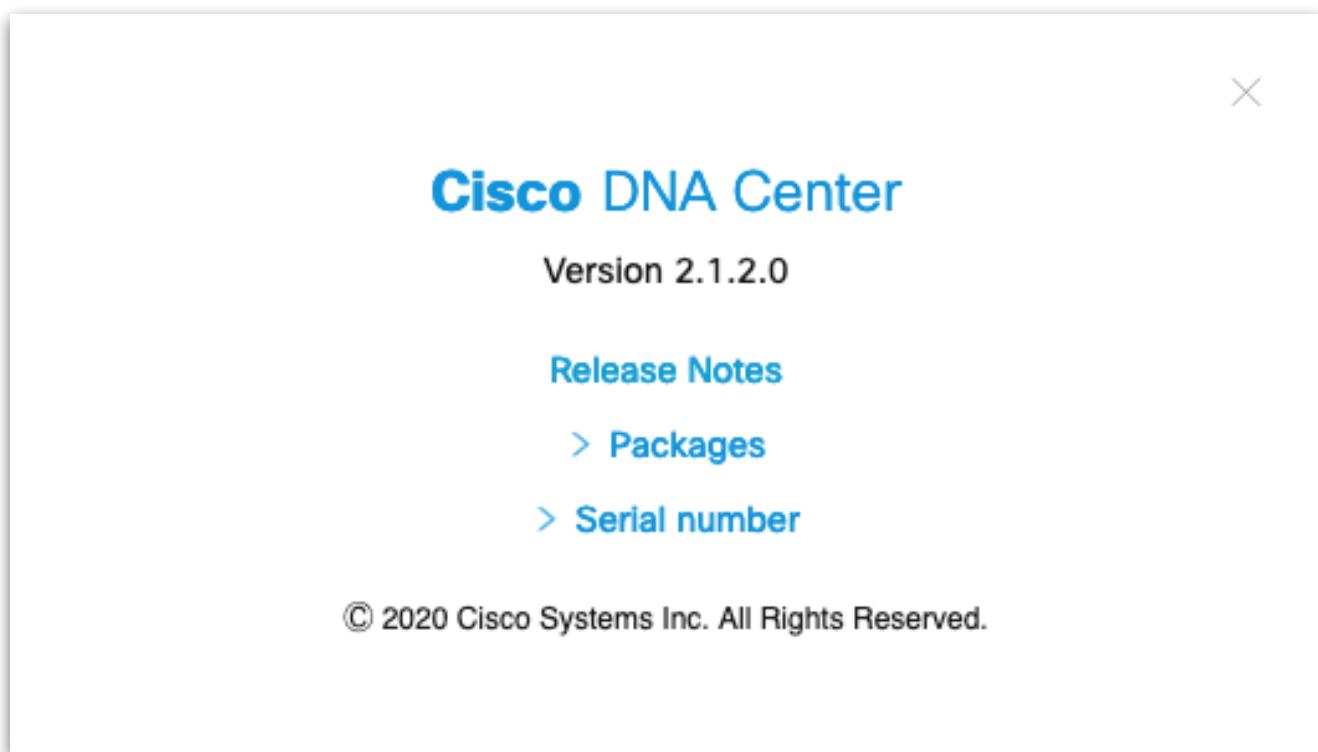
Command Runner deadbeef-1.dna.local@192.168.0.101

Welcome to Cisco DNA Center command runner.

You can access this window from anywhere using the key combination Q+T. You can access recently viewed devices using the key combination Q+D.

Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.

```
deadbeef-1.dna.local> show start
Using 22625 out of 2097152 bytes
!
! Last configuration change at 18:49:27 UTC Wed Sep 16 2020 by netadmin1
! NVRAM config last updated at 18:49:35 UTC Wed Sep 16 2020 by netadmin1
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone year
service password-encryption
service call-home
no platform punt-keepalive disable-kernel-core
!
hostname deadbeef-1
!
vrf definition Mgmt-vrf
```



The End.