PnP APIs

- Certificate Creation APIs, on page 1
- PnP Action APIs, on page 5
- PnP APIs, on page 6
- PnP Server APIs, on page 6

Certificate Creation APIs

Table 1: Certificate Creation APIs

Action	Method	Payload Required	API
To create a certificate signing request	POST	Yes	/api/operations/system/certificate/signing-request
To install a certificate, which will be used by the local portal and REST API	POST	Yes	/api/operations/system/certificate/install-cert
To switch between self-signed and CA signed certificates	POST	Yes	/api/operations/system/certificate/use-cert

Example for Signing Request Payload

```
<signing-request>
 <country-code>US</country-code>
```

```
 <state>California</state>
 <locality>San Jose</locality>
 <organization>Cisco</organization>
 <organization-unit-name>Cisco</organization-unit-name>
 <common-name>nfvis.cisco.com</common-name>
</signing-request>
```

Table 2: Description for Signing Request Payload

Property	Type	Description	Mandatory/Default Value
<country-code>	String	Two-letter ISO abbreviation for your country.	No
<state>	String	Name of the state where your organization's head office is located.	No
<locality>	Boolean	Name of the city where your organization's head office is located.	No
<organization>	Boolean	Name of the organization	No
<organization-unit-name>	String	Name of the department or group that will use the certificate.	No
<common-name>	URL	Fully qualified domain name that you want to secure.	Yes

Example for Install Certificate Payload

```
<install-cert>
  <path>file:///data/upload1/servercert.pem</path>
</install-cert>
```

Table 3: Description for Install Certificate Payload

Property	Type	Description	Mandatory/Default Value
<install-cert> <path>	URL	Full path of the certificate.	Yes

Example for Use Certificate Payload

```
<use-cert>
  <cert-type>ca-signed</cert-type>
</use-cert>
```

The <cert-type> parameter is mandatory in the use certificate payload. You can .

Table 4: Description for Use Certificate Payload

Property	Type	Description	Mandatory/Default Value

<use-cert> <cert-type>	string	The <self-signed> or <ca-signed> certificate type.	Yes

Example: POST Signing Request API

```
curl -k -v -u admin:admin -H Content-Type:application/vnd.yang.data+xml -X
POST -d <signing-request><country-code>US</country-code><state>California</state><locality>San
 Jose</locality><organization>Cisco</organization>
<organization-unit-name>Cisco</organization-unit-name><common-name>nfvis.cisco.com</common-name></signing-request>

https://209.165.201.1/api/operations/system/certificate/signing-request
* About to connect() to 209.165.201.1 port 443 (#0)
* Trying 209.165.201.1... connected
* Connected to 209.165.201.1 (209.165.201.1) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* warning: ignoring value of ssl.verifyhost
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Server certificate:
* subject: CN=Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* start date: Apr 04 23:26:13 2016 GMT
* expire date: Apr 02 23:26:13 2026 GMT
* common name: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* issuer: CN=Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> POST /api/operations/system/certificate/signing-request HTTP/1.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.16.2.3 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Host: 209.165.201.1
> Accept: */*
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 250
>
< HTTP/1.1 200 OK
< Server: nginx/1.6.3
< Date: Wed, 06 Apr 2016 23:29:39 GMT
< Content-Type: application/vnd.yang.operation+xml
< Content-Length: 85
< Connection: keep-alive
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Vary: Accept-Encoding
< Pragma: no-cache
<
<output xmlns='http://www.cisco.com/nfv'>
 <url>/download/nfvis.csr</url>
</output>
* Connection #0 to host 209.165.201.1 left intact
* Closing connection #0
```

Example: POST Install Certificate API

```
curl -k -v -u admin:admin -H Content-Type:application/vnd.yang.data+xml -X
POST -d <install-cert><path>file:///data/upload1/servercert.pem</path></install-cert>
 https://209.165.201.1/api/operations/system/certificate/install-cert
* About to connect() to 209.165.201.1 port 443 (#0)
```

```
* Trying 209.165.201.1... connected
* Connected to 209.165.201.1 (209.165.201.1) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* warning: ignoring value of ssl.verifyhost
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Server certificate:
* subject: CN=Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* start date: Apr 04 23:26:13 2016 GMT
* expire date: Apr 02 23:26:13 2026 GMT
* common name: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* issuer: CN=Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> POST /api/operations/system/certificate/install-cert HTTP/1.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.16.2.3 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Host: 209.165.201.1
> Accept: */*
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 81
>
< HTTP/1.1 204 No Content
< Server: nginx/1.6.3
< Date: Wed, 06 Apr 2016 23:19:33 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Pragma: no-cache
<
* Connection #0 to host 209.165.201.1 left intact
* Closing connection #0
```

Example: POST Use Certificate API

```
curl -k -v -u admin:admin -H Content-Type:application/vnd.yang.data+xml -X
POST -d <use-cert><cert-type>ca-signed</cert-type></use-cert>
https://209.165.201.1/api/operations/system/certificate/use-cert
* About to connect() to 209.165.201.1 port 443 (#0)
* Trying 209.165.201.1... connected
* Connected to 209.165.201.1 (209.165.201.1) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* warning: ignoring value of ssl.verifyhost
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Server certificate:
* subject: CN=Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* start date: Apr 04 23:26:13 2016 GMT
* expire date: Apr 02 23:26:13 2026 GMT
* common name: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* issuer: CN=Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> POST /api/operations/system/certificate/use-cert HTTP/1.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.16.2.3 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Host: 209.165.201.1
> Accept: */*
```

```
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 57
>
< HTTP/1.1 204 No Content
< Server: nginx/1.6.3
< Date: Wed, 06 Apr 2016 23:23:19 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Pragma: no-cache
<
* Connection #0 to host 209.165.201.1 left intact
* Closing connection #0
```

PnP Action APIs

Table 5: PnP Action API

Action	Method	Payload Required	API
To start, stop, and restart a PnP action	POST	Yes	/api/operations/pnp/action

Example for PnP action Payload

```
<input>
<command><start><stop><restart>
```

Example: POST PnP Action API

```
curl -k -v -u admin:admin -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml -X
POST  https://209.165.201.1/api/operations/pnp/action -d
'<input><command>start</command></input>'
*   Trying 209.165.201.1...
* Connected to 209.165.201.1 (209.165.201.1) port 443 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> POST /api/operations/pnp/action HTTP/1.1
> Host: 209.165.201.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.43.0
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 39
>
* upload completely sent off: 39 out of 39 bytes
< HTTP/1.1 204 No Content
< Server: nginx/1.6.3
< Date: Fri, 12 Aug 2016 14:38:13 GMT
< Content-Type: text/html
```

```
< Content-Length: 0
< Connection: keep-alive
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Pragma: no-cache
```

PnP APIs

PnP Server APIs

Table 6: PnP Server APIs

Action	Method	Payload Required	API
To get the PnP IP address and port number	GET	No	/api/config/pnp?deep
To get the PnP operational status	GET	No	/api/operational/pnp/status
To modify the PnP IP address and port number	PUT	Yes	/api/config/pnp
To delete the PnP IP address and port number	DELETE	No	/api/config/pnp
To add PnP static IPv6 address	PUT	Yes	/api/config/pnp

Example for PnP Server Payload (Static Mode)

```
<pnp>
<static>
<ip-address>192.0.2.1</ip-address>
<port>80</port>
</static>
<automatic>
<dhcp>disable</dhcp>
<dns>disable</dns>
<cco>disable</cco>
</automatic>
</pnp>
```

Example for PnP Server Payload (Automatic Mode)

```
<pnp>
<automatic>
<dhcp>enable</dhcp>
<dns>enable</dns>
<cco>enable</cco>
<timeout>100</timeout>
```

```
</automatic>
</pnp>
```

Table 7: PnP Server Payload Description

Property	Type	Description	Mandatory/Default Value
<static> <ip-address>	number	Static IP address	Yes (if you disable the automatic option)
<port>	number	Port number	Yes (in static mode)
<dhcp>disable</dhcp> <dhcp>enable</dhcp>	text	Enable or disable DHCP	Yes (one of the options is mandatory)
<dns>disable</dns> <dns>enable</dns>	text	Enable or disable DNS	Yes (one of the options is mandatory)
<cco>disable</cco> <cco>enable</cco>	text	Enable or disable CCO	Yes (one of the options is mandatory)
<timeout>	number	Timeout in seconds. Default is 60 seconds.	No

Example: PUT PnP Server API

Use this API to enable static mode for PnP discovery.

```
curl -k -v -u admin:admin -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml -X
PUT https://209.165.201.1/api/config/pnp -d
'<pnp><static><ip-address>209.165.201.2</ip-address><port>50</port></static>
<automatic><dhcp>disable</dhcp><dns>disable</dns><cco>disable</cco></automatic></pnp>'
*   Trying 209.165.201.1...
* Connected to 209.165.201.1 (209.165.201.1) port 443 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> PUT /api/config/pnp HTTP/1.1
> Host: 209.165.201.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.43.0
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 154
>
* upload completely sent off: 154 out of 154 bytes
< HTTP/1.1 204 No Content
< Server: nginx/1.6.3
< Date: Fri, 12 Aug 2016 14:32:04 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Last-Modified: Fri, 12 Aug 2016 14:32:04 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1471-12324-598715
< Pragma: no-cache
```

```
<
* Connection #0 to host 209.165.201.1 left intact
```

Use this API to enable automatic mode for PnP discovery.

```
curl -k -v -u admin:admin -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml -X
PUT https://209.165.201.1/api/config/pnp -d
'<pnp><automatic><timeout>100</timeout><dhcp>enable</dhcp>
<dns>enable</dns><cco>enable</cco></automatic></pnp>'
*   Trying 209.165.201.1...
* Connected to 209.165.201.1 (209.165.201.1) port 443 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> PUT /api/config/pnp HTTP/1.1
> Host: 209.165.201.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.43.0
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 110
>
* upload completely sent off: 110 out of 110 bytes
< HTTP/1.1 204 No Content
< Server: nginx/1.6.3
< Date: Fri, 12 Aug 2016 14:34:38 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Last-Modified: Fri, 12 Aug 2016 14:34:37 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1471-12477-787708
< Pragma: no-cache
<
* Connection #0 to host 209.165.201.1 left intact
```

Example: GET PnP Server API

Use this API to get the PnP IP address and port number.

```
curl -X GET -v -k -u admin:admin https://192.0.2.2/api/config/pnp -H
Content-type:application/vnd.yang.data+xml
*   Trying 192.0.2.1...
* Connected to 192.0.2.2 (192.0.2.2) port 443 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> GET /api/config/pnp HTTP/1.1
> Host: 192.0.2.2
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.43.0
> Accept: */*
> Content-type:application/vnd.yang.data+xml
>
< HTTP/1.1 200 OK
< Server: nginx/1.6.3
< Date: Fri, 19 Aug 2016 09:04:21 GMT
< Content-Type: application/vnd.yang.data+xml
< Transfer-Encoding: chunked
```

```
< Connection: keep-alive
< Last-Modified: Fri, 19 Aug 2016 08:39:52 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1471-595992-889103
< Pragma: no-cache
<
<pnp xmlns="http://www.cisco.com/nfv/pnp" xmlns:y="http://tail-f.com/ns/rest"
xmlns:pnp="http://www.cisco.com/nfv/pnp">
  <static>
    <ip-address>192.0.2.1</ip-address>
    <port>32</port>
  </static>
  <automatic>
    <dhcp>disable</dhcp>
    <dns>disable</dns>
    <cco>disable</cco>
  </automatic>
  <y:operations>
    <action>/api/config/pnp/_operations/action</action>
  </y:operations>
</pnp>
```

Example: DELETE PnP Server API

```
curl -k -v -u admin:admin -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml -X
DELETE  https://209.165.201.1/api/config/pnp
*Trying 209.165.201.1...
*Connected to 209.165.201.1 (209.165.201.1) port 443 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: Cisco-Enterprise-NFVIS-Self-Signed-Certificate
* Server auth using Basic with user 'admin'
> DELETE /api/config/pnp HTTP/1.1
> Host: 209.165.201.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.43.0
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
>
< HTTP/1.1 204 No Content
< Server: nginx/1.6.3
< Date: Fri, 12 Aug 2016 14:36:30 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Last-Modified: Fri, 12 Aug 2016 14:36:30 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1471-12590-573502
< Pragma: no-cache
<
```