

June 20, 2023

Configuration for SSL certificate store on Citrix ADM resource.

Properties

(click to see [Operations](#))

Name	Data Type	Permissions	Description
key_file		Read-write	Key file name. Minimum length = 1 Maximum length = 128
id		Read-write	Id is system generated key for all certificate store entries. .
name		Read-write	Name or alias which identifies certificate and key pair. Minimum length = 1 Maximum length = 128
certchain_file_id		Read-write	Comma separated list of IDs against which cert chain contents are stored in cert_store_data table. Minimum length = 1 Maximum length = 128
update_cert_and_key		Read-write	Set to true,if certificate and key files needs to be updated during update operation.
cert_data		Read-write	Base64 encoded certificate file contents..
certchain_data	<cert_store_data[]>	Read-write	An array of Base64 encoded certificate chain contents..
password		Read-write	The pass-phrase that was used to encrypt the private-key.. Maximum length = 128
bound_entities_number		Read-write	Number of entities to which a certificate in store is bound.
update_cert_chain		Read-write	Set to true,if certificate chain needs to be updated during update operation.
			Base64 encoded key file contents..

key_data		Read-write	Maximum length = 16384
serial_number		Read-only	Serial Number.
signature_algorithm		Read-only	Signature Algorithm.
valid_from		Read-only	Valid From.
issuer		Read-only	Issuer.
store_code		Read-only	0 indicates no error.100: Failure in storing Server certificate file.200: Failure in storing key file. 300:Failure in storing password.400: Failure in storing certificate chain.
public_key_size		Read-only	Public Key Size.
valid_to		Read-only	Valid To.
version		Read-only	Version.
subject		Read-only	Subject.
public_key_algorithm		Read-only	Public Key Algorithm.
revision_number		Read-only	Certificate revision number.
cert_format		Read-only	Certificate Format.
subjaltname		Read-only	Comma separated Subject Alternative Names.
status		Read-only	Tells whether the certificate is still valid or not.
activity_id		Read-only	Activity Id used to track the progress of certificate operations..
days_to_expiry		Read-only	Days before SSL certificate expires.

Operations

(click to see [Properties](#))

- ADD
- DELETE
- GET (ALL)
- GET
- MODIFY

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// *<netScaler-ip-address>* /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: *<username>*

X-NITRO-PASS: *<password>*

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= *<tokenvalue>*

***Note:** * Mandatory parameters are marked in **red** and placeholder content is marked in *green*

The following parameters can be used in the nitro request : onerror *<String_value>*

Use this parameter to set the onerror status for nitro request. Applicable only for bulk requests.

Default value: EXIT

Possible values = EXIT, CONTINUE

add

URL: https://*<MGMT-IP>*/nitro/v2/config/cert_store?onerror=*<String_value>* **HTTPS**

Method: POST

Request Headers: Content-Type: application/json

X-NITRO-USER:username_value*<String>*

X-NITRO-PASS:password_value*<String>*

or

Cookie:NITRO_AUTH_TOKEN=token_value*<String>*

Request Payload:

```
{
  "cert_store": {
    <b>"name":<String_value></b>,
    "cert_data":<cert_store_data_value>,
    "certchain_data":[{
      "file_name":<String_value>,
      "id":<String_value>,
      "file_data":<String_value>}],
      "key_file":<String_value>,
      "password":<String_value>,
      "id":<String_value>,
      "key_data":<String_value>,
      "update_cert_and_key":<Boolean_value>,
      "bound_entities_number":<Integer_value>,
      "certchain_file_id":<String_value>,
      "update_cert_chain":<Boolean_value>}}
}
```

Response: HTTPS Status Code on Success: 200 OK HTTPS Status Code on Failure: 4xx (for general HTTPS errors) or 5xx (for NetScaler-MAS-specific errors). The response payload provides details of the error

Response Payload:

```
{
  "errorcode": 0, "message": "Done", "severity": ;ltString_value;gt
  "serial_number":<String_value>,
  "signature_algorithm":<String_value>,
  "valid_from":<String_value>,
  "issuer":<String_value>,
  "key_file":<String_value>,
  "store_code":<Integer_value>,
  "public_key_size":<Integer_value>,
  "key_file_id":<String_value>,
  "id":<String_value>,
  "password_id":<String_value>,
  "valid_to":<String_value>,
  "version":<Integer_value>,
  "subject":<String_value>,
  "name":<String_value>,
  "..."
}
```

delete

URL: https://<MGMT-IP>/nitro/v2/config/cert_store/id_value<String> **HTTPS Method:** DELETE

Request Headers: X-NITRO-USER:username_value<String>

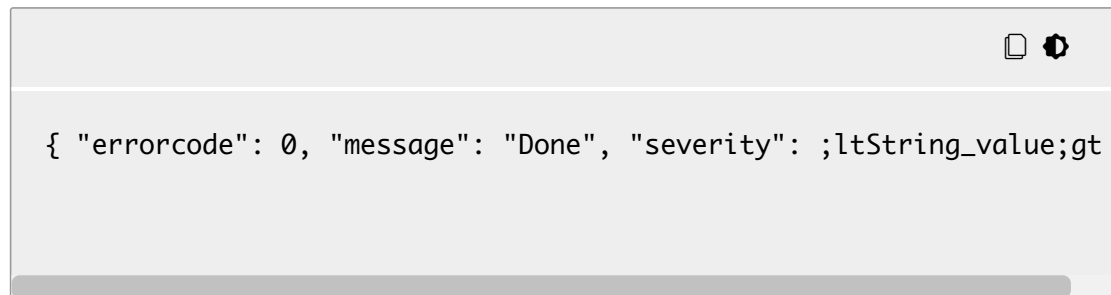
X-NITRO-PASS:password_value<String>

or

Cookie:NITRO_AUTH_TOKEN=token_value<String>

Response: HTTPS Status Code on Success: 200 OK HTTPS Status Code on Failure: 4xx (for general HTTPS errors) or 5xx (for NetScaler-MAS-specific errors). The response payload provides details of the error

Response Payload:



get (all)

URL: https://<MGMT-IP>/nitro/v2/config/cert_store **Query-parameters:**

filter https://<MGMT-IP>/nitro/v2/config/cert_store **?filter=property-name1:property-value1,property-name2:property-value2** Use this query-parameter to get the filtered set of cert_store resources configured on the system. You can set a filter on any property of the resource.

pagesize=#no;pageno=#no https://<MGMT-IP>/nitro/v2/config/cert_store **?**
pagesize=#no;pageno=#no Use this query-parameter to get the cert_store resources in chunks.

count https://<MGMT-IP>/nitro/v2/config/cert_store **?count=yes** Use this query-parameter to get the count of cert_store resources.

HTTPS Method: GET

Request Headers: Accept: application/json

X-NITRO-USER:username_value<String>

X-NITRO-PASS:password_value<String>

or

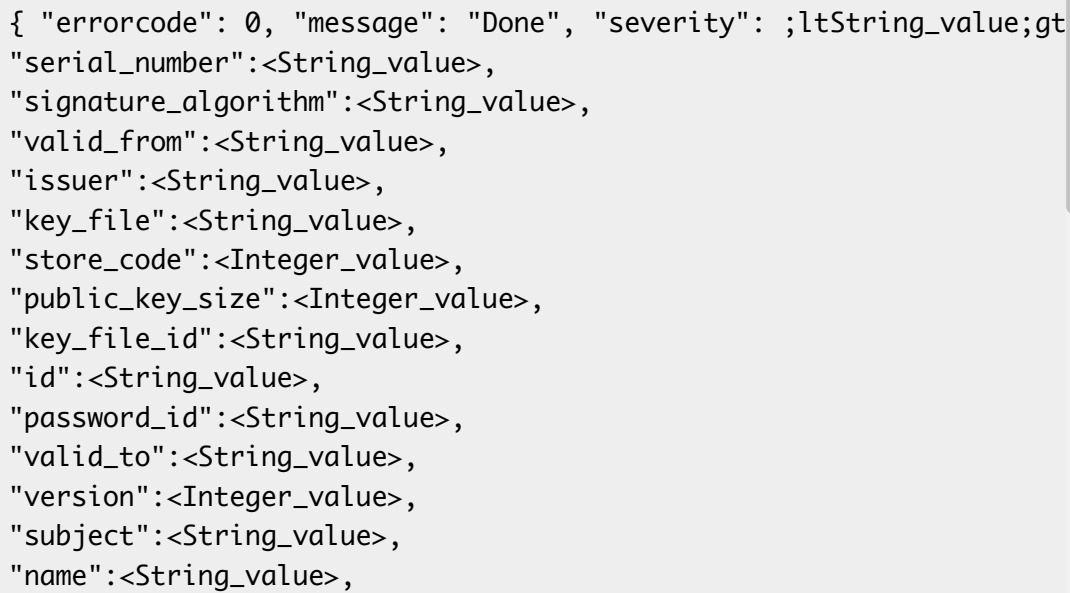
Cookie:NITRO_AUTH_TOKEN=token_value<String>

Response: HTTPS Status Code on Success: 200 OK HTTPS Status Code on Failure: 4xx (for general HTTPS errors) or 5xx (for NetScaler-MAS-specific errors). The response payload provides details of the error

Response Headers:

Content-Type:application/json

Response Payload:



```
{ "errorcode": 0, "message": "Done", "severity": ;ltString_value;gt
"serial_number":<String_value>,
"signature_algorithm":<String_value>,
"valid_from":<String_value>,
"issuer":<String_value>,
"key_file":<String_value>,
"store_code":<Integer_value>,
"public_key_size":<Integer_value>,
"key_file_id":<String_value>,
"id":<String_value>,
"password_id":<String_value>,
"valid_to":<String_value>,
"version":<Integer_value>,
"subject":<String_value>,
"name":<String_value>,
```

get

URL: https://<MGMT-IP>/nitro/v2/config/cert_store/id_value<String> **HTTPS Method:** GET

Request Headers: Accept: application/json

X-NITRO-USER:username_value<String>

X-NITRO-PASS:password_value<String>

or

Cookie:NITRO_AUTH_TOKEN=token_value<String>

Response: HTTPS Status Code on Success: 200 OK HTTPS Status Code on Failure: 4xx (for general HTTPS errors) or 5xx (for NetScaler-MAS-specific errors). The response payload provides details of the error

Response Headers:

Content-Type:application/json

Response Payload:

```
{ "errorcode": 0, "message": "Done", "severity": ;ltString_value;gt
"serial_number":<String_value>,
"signature_algorithm":<String_value>,
"valid_from":<String_value>,
"issuer":<String_value>,
"key_file":<String_value>,
"store_code":<Integer_value>,
"public_key_size":<Integer_value>,
"key_file_id":<String_value>,
"id":<String_value>,
"password_id":<String_value>,
"valid_to":<String_value>,
"version":<Integer_value>,
"subject":<String_value>,
"name":<String_value>,
```

modify

URL: https://<MGMT-IP>/nitro/v2/config/cert_store/id_value<String> **HTTPS Method:** PUT

Request Headers: Content-Type: application/json

X-NITRO-USER:username_value<String>

X-NITRO-PASS:password_value<String>

or

Cookie:NITRO_AUTH_TOKEN=token_value<String>

Request Payload:

```
{"cert_store":{
<b>"id":<String_value></b>,
"cert_data":<cert_store_data_value>,
"certchain_data":[{
"file_name":<String_value>,
"id":<String_value>,
"file_data":<String_value>}],
"key_file":<String_value>,
"password":<String_value>,
"key_data":<String_value>,
"update_cert_and_key":<Boolean_value>,
"name":<String_value>,
"bound_entities_number":<Integer_value>,
"certchain_file_id":<String_value>,
"update_cert_chain":<Boolean_value>}}
```

Response: HTTPS Status Code on Success: 200 OK HTTPS Status Code on Failure: 4xx (for general HTTPS errors) or 5xx (for NetScaler-MAS-specific errors). The response payload provides details of the error

Response Payload:

```
{ "errorcode": 0, "message": "Done", "severity": ;ltString_value;gt
"serial_number":<String_value>,
"signature_algorithm":<String_value>,
"valid_from":<String_value>,
"issuer":<String_value>,
"key_file":<String_value>,
"store_code":<Integer_value>,
"public_key_size":<Integer_value>,
"key_file_id":<String_value>,
"id":<String_value>,
"password_id":<String_value>,
"valid_to":<String_value>,
"version":<Integer_value>,
"subject":<String_value>,
"name":<String_value>,
```

IN THIS ARTICLE

Properties

Operations

Was this helpful

