CentralNic Reseller

SSL Documentation

Legacy System Reference Manual

2025-03-25

Table of Contents

AddCertificate

The AddCertificate command is used for the request of a new SSL certificate with its first sub-certificate.

Required Parameters

Command

COMMAND	= AddCertificate
APPROVEREMAIL[0-24]	= (TEXT)
PERIOD	= (INT)
OWNERCONTACT#	= (TEXT)
ADMINCONTACT#	= (TEXT)
BILLINGCONTACT#	= (TEXT)
TECHCONTACT#	= (TEXT)
CSR#	= (TEXT)
DOMAIN[0-24]	= (TEXT)
AUTHMETHOD	= EMAIL|DNS|FILE
WEBSERVERTYPE	= apachessl|apacheraven|apachessleay|c2net|Ibmhttp|Iplanet|Dominogo4625|Dominogo4626|Domino|iis4|iis5|Netscape|zeusv3|Other|apacheopenssl|apache2|apacheapachessl|cobaltseries|cpanel|ensim|hsphere|ipswitch|plesk|tomcat|WebLogic|website|webstar|iis
CLASS	= SSL123|SSLWebServer|SSLWebServerWC|SSLWebServerEV|SecureSite|SecureSitePro|SecureSiteEV|SecureSiteProEV|QuickSSLPremium|TrueBizID|TrueBizIDWC|TrueBizIDEV|RapidSSL|RapidSSLWC|InstantSSL|SGCWildcardSSL|PositiveSSL|PremiumSSL|ExtendedValidatedSSL|PositiveWildcardSSL
ALGORITHM	= SHA2-256|SHA256-FULL-CHAIN|SHA256-ECC-FULL|SHA256-ECC-HYBRID|PRIVATE-SHA1-PCA3G1|PRIVATE-SHA256-PCA3G1|PRIVATE-SHA1-PCA3G2|PRIVATE-SHA256-PCA3G2

Response

code	= (INT)
description	= (TEXT)
property[CERTIFICATE][#]	= (TEXT)
property[SUB][#]	= (TEXT)
property[STATUS][#]	= (TEXT)
property[SUB_STATUS][#]	= (TEXT)
property[FILEAUTH_NAME][#]	= (TEXT)
property[FILEAUTH_CONTENTS][#]	= (TEXT)
property[DNSAUTH_NAME][#]	= (TEXT)
property[BILLINGCLASS][#]	= (TEXT)

Attributes

APPROVEREMAIL	Email where the approval-link should be sent to
PERIOD	How many years the certificate should be valid (optional)
OWNERCONTACT0	Owner contact for the certificate (may not contain special chars / umlauts)
ADMINCONTACT0	Admin contact for the certificate (may not contain special chars / umlauts)
BILLINGCONTACT0	Billing contact for the certificate (may not contain special chars / umlauts)
TECHCONTACT0	Tech contact for the certificate (may not contain special chars / umlauts)
CSR#	The CSR to be used to generate the certificate
DOMAIN(0-24)	Additional domain for SAN, which will be charged separately (optional)
WEBSERVERTYPE	Type of the webserver where the certificate should be used (optional)
ALGORITHM	Algorithm used for signing the certificate (optional)
AUTHMETHOD	Method for authentication of the domainname (optional)
CLASS	Type of certificate to be added (optional)
CERTIFICATE	ID of the new certificate order
SUB	ID of the new certificate sub
STATUS	Status of the request - process for the certificate order
SUB_STATUS	Status of the request - process for the sub
FILEAUTH_NAME	Name for the file needed for file based authentication
FILEAUTH_CONTENTS	Content for the file needed for file based authentication
DNSAUTH_NAME	Name of the RR entry needed for DNS based authentication
BILLINGCLASS	Class used to bill this certificate in case of a SAN - certificate

CheckCertificate

The CheckCertificate command is used to check the certificate request for validation and information details. Please note, the CA does not check the WHOIS for email addresses when ordering/renewing the certificate. To work around this, call the CheckCertificate API command (with the optional parameters), and this will cache it for 24 hours, then place the order with this timeframe. The email address has to be one that returns from the response.

Required Parameters

Command

COMMAND	= checkCertificate
CSR#	= (TEXT)
CRT#	= (TEXT)

Response

code	= (INT)
description	= (TEXT)
queuetime	= (INT)
runtime	= (INT)
property[CSR_PUBLIC_KEY_ALGORITHM][#]	= (TEXT)
property[CSR_SIGNATURE_ALGORITHM][#]	= (TEXT)
property[CSR_SIZE][#]	= (INT)
property[CSR_SUBJECT][#]	= (TEXT)
property[CRT_PUBLIC_KEY_ALGORITHM][#]	= (TEXT)
property[CRT_SIGNATURE_ALGORITHM][#]	= (TEXT)
property[CRT_VALIDITY_NOT_BEFORE][#]	= (DATE)
property[CRT_VALIDITY_NOT_AFTER][#]	= (DATE)
property[CRT_SIZE][#]	= (INT)
property[CRT_VERSION][#]	= (TEXT)
property[CRT_SERIAL][#]	= (TEXT)
property[CRT_SUBJECT][#]	= (TEXT)
property[CRT_ISSUER][#]	= (TEXT)
property[CSR_SAN#][#]	= (TEXT)
property[CRT_SAN#][#]	= (TEXT)
property[CSR_KEY_USAGE#][#]	= (TEXT)
property[CRT_KEY_USAGE#][#]	= (TEXT)
property[CRT_EXTENDED_KEY_USAGE#][#]	= (TEXT)
property[CSR_EMAILADDRESS][#]	= (TEXT)
property[CSR_LOCATION][#]	= (TEXT)
property[CRT_SUBJECT_EMAILADDRESS][#]	= (TEXT)
property[CRT_SUBJECT_LOCATION][#]	= (TEXT)
property[CRT_ISSUER_EMAILADDRESS][#]	= (TEXT)
property[CRT_ISSUER_LOCATION][#]	= (TEXT)
property[CSR_COMMONNAME][#]	= (TEXT)

property[CRT_SUBJECT_COMMONNAME][#] = (TEXT)
property[CRT_ISSUER_COMMONNAME][#] = (TEXT)
property[CSR_STATE][#] = (TEXT)
property[CSR_COUNTRY][#] = (TEXT)
property[CRT_SUBJECT_STATE][#] = (TEXT)
property[CRT_SUBJECT_COUNTRY][#] = (TEXT)
property[CRT_ISSUER_STATE][#] = (TEXT)
property[CRT_ISSUER_COUNTRY][#] = (TEXT)
property[CSR_ORGANIZATION][#] = (TEXT)
property[CSR_ORGANIZATIONAL_UNIT][#] = (TEXT)
property[CRT_SUBJECT_ORGANIZATION][#] = (TEXT)
property[CRT_SUBJECT_ORGANIZATIONAL_UNIT][#]= (TEXT)
property[CRT_ISSUER_ORGANIZATION][#] = (TEXT)
property[CRT_ISSUER_ORGANIZATIONAL_UNIT][#] = (TEXT)

Attributes

CSR#	A base64 encoded certificate request
CRT#	A base64 encoded X509 certificate
CSR_PUBLIC_KEY_ALGORITHM	Public key algorithm used in the CSR
CSR_SIGNATURE_ALGORITHM	Signature algorithm used in the CSR
CSR_SIZE	Size of the CSR
CSR_SUBJECT	Subject encoded in the CSR
CRT_PUBLIC_KEY_ALGORITHM	Public key algorithm used for the CRT
CRT_SIGNATURE_ALGORITHM	Signature algorithm used for the CRT
CRT_VALIDITY_NOT_BEFORE	CRT only valid after this date
CRT_VALIDITY_NOT_AFTER	CRT only valid before this date
CRT_SIZE	Size of the CRT
CRT_VERSION	Version encoded in the CRT
CRT_SERIAL	Serial of the CRT
CRT_SUBJECT	Subject encoded in the CRT
CRT_ISSUER	Issuer of the CRT
CSR_SAN#	Domains encoded in the CSR
CRT_SAN#	Domains encoded in the CRT
CSR_KEY_USAGE#	Allowed usage of the CSR
CRT_KEY_USAGE#	Allowed usage of the CRT
CRT_EXTENDED_KEY_USAGE#	Details of the allowed usage of the CRT
CSR_EMAILADDRESS	Email given in the CSR
CSR_LOCATION	City given in the CSR
CRT_SUBJECT_EMAILADDRESS	Email given in the CRT
CRT_SUBJECT_LOCATION	City given in the CRT
CRT_ISSUER_EMAILADDRESS	Email given in the CRT
CRT_ISSUER_LOCATION	City given in the CRT
CSR_COMMONNAME	Common name given in the CSR
CRT_SUBJECT_COMMONNAME	Common name given in the CRT
CRT_ISSUER_COMMONNAME	Common name given in the CRT
CSR_STATE	State given in the CSR
CSR_COUNTRY	Country given in the CSR
CRT_SUBJECT_STATE	State given in the CRT
CRT_SUBJECT_COUNTRY	Country given in the CRT
CRT_ISSUER_STATE	State given in the CRT
CRT_ISSUER_COUNTRY	Country given in the CRT
CSR_ORGANIZATION	Organization given in the CSR
CSR_ORGANIZATIONAL_UNIT	Unit of the organization given in the CSR
CRT_SUBJECT_ORGANIZATION	Organization given in the CRT
CRT_SUBJECT_ORGANIZATIONAL_UNIT	Unit of the organization given in the CRT
CRT_ISSUER_ORGANIZATION	Organization given in the CRT
CRT_ISSUER_ORGANIZATIONAL_UNIT	Unit of the organization given in the CRT

Optional Parameters

Command

```
COMMAND     = checkCertificate
DOMAIN      = (TEXT)
CLASS       = (TEXT)
```

Request

```
code                          = (INT)
description                   = (TEXT)
queuetime                     = (INT)
runtime                       = (INT)
property[approveremail][#]    = (TEXT)
property[approvertype][#]     = (TEXT)
property[column][#]           = (TEXT)
```

Attributes

approveremail	Email where the approval-link should be sent to
approvertype	Owner (base) of the domain

DeleteCertificate

Delete a certificate

Required Parameters

Command

```
COMMAND     = DeleteCertificate
CERTIFICATE = (TEXT)
SUB         = (TEXT)
```

Response

```
code        = (INT)
description = (TEXT)
```

Attributes

CERTIFICATE	The ID of the certificate order to be deleted
SUB	The ID of the certificate sub to be deleted (optional)

GetCertificateInfo

Required Parameters

Command

COMMAND	= GetCertificateInfo
CLASS	= (TEXT)

Response

property[class][#]	= (TEXT)
property[dns auth][#]	= 0|1
property[encyrption][#]	= (MIN INT)-(MAX INT) bit, (TEXT)
property[extended validation][#]	= 0|1
property[file auth][#]	= 0|1
property[name][#]	= (TEXT)
property[periods][#]	= (COMMA-SEPERATED-INTEGERS)
property[prefix][#]	= (2-CHAR-TEXT)
property[provider][#]	= thawte|symantec|geotrust|rapidssl|comodo
property[reissue][#]	= 0|1
property[revoke][#]	= 0|1
property[san][#]	= 0|1
property[validation method][#]	= domain|organization|extended
property[wildcard][#]	= 0|1

ModifyCertificate

Required Parameters

Command

COMMAND	= ModifyCertificate
CERTIFICATE	= (TEXT)
SUB	= (TEXT)
APPROVEREMAIL[0-24]	= (TEXT)
AUTHMETHOD	= EMAIL|DNS|FILE

Response

Code	= (INT)
description	= (TEXT)

Attributes

CERTIFICATE	Unique ID of the certificate to be changed
APPROVEREMAIL	New email - address where the approval - link should be send to

QueryCertificateList

Listing all certificate orders is possible with the QueryCertificateList command. This behaves like most Query...List - commands in the CentralNic Reseller Control Panel, allowing filtering and paging. By default all cancelled certificates are not returned.

Required Parameters

Command

Command	= QueryCertificateList
WIDE	= 0|1
LIMIT	= (INT)
FIRST	= (INT)
INCLUDESUB	= 0|1

Response

code	= (INT)
description	= (TEXT)
queuetime	= (INT)
runtime	= (INT)
property[column][#]	= certificate
property[column][1]	= status
property[column][2]	= domain
property[column][3]	= created date
property[column][4]	= owner contact
property[column][5]	= admin contact
property[column][6]	= tech contact
property[column][7]	= billing contact
property[column][8]	= webservertype
property[column][9]	= class
property[column][10]	= registrar
property[count][#]	= (INT)
property[first][#]	= (INT)
property[last][#]	= (INT)
property[limit][#]	= (INT)
property[total][#]	= (INT)
property[certificate][#]	= (TEXT)
property[status][#]	= EXPIRED
property[domain][#]	= (TEXT)
property[created date][#]	= (DATE)
property[owner contact][#]	= (TEXT)
property[admin contact][#]	= (TEXT)
property[tech contact][#]	= (TEXT)
property[billing contact][#]	= (TEXT)
property[webservertype][#]	= (TEXT)

property[class][#] = (TEXT)
property[registrar][#] = (TEXT)

Attributes

INCLUDESUB	Show sub-reseller certs

ReissueCertificate

This command will create a new sub-certificate in a certificate order (parameter "certificate") based on data of the most recent existing sub-certificate and the data given with the command (given values overwrite existing data). The expiration date of the new sub-certificate will not change since the new sub-certificate is only meant to be used as a replacement. Stating the CSR is not mandatory. If no CSR is stated the old one initially given durin certificate creation will be used. If you want to reissue the certificate order based on a different sub-certificate than the most recent, you have the option to use a specific sub-certificate (parameter "sub").

Required Parameters

Command

```
COMMAND              = ReissueCertificate
CERTIFICATE          = (TEXT)
SUB                  = (TEXT)
CSR#                 = (TEXT)
REISSUEEMAIL[0-24]   = (TEXT)
DOMAIN[0-24]         = (TEXT)
AUTHMETHOD           = EMAIL|DNS|FILE
ALGORITHM            = SHA2-256|SHA256-FULL-CHAIN|SHA256-ECC-FULL|SHA256-ECC-
HYBRID|PRIVATE-SHA1-PCA3G1|PRIVATE-SHA256-PCA3G1|PRIVATE-SHA1-PCA3G2|PRIVATE-
SHA256-PCA3G2
```

Response

```
code                 = (INT)
description          = (TEXT)
property[CERTIFICATE][#]  = (TEXT)
property[SUB][#]     = (TEXT)
property[STATUS][#]  = (TEXT)
property[SUB_STATUS][#]   = (TEXT)
```

Attributes

CERTIFICATE	ID of the certificate order to be reissued
SUB	ID of the certificate sub to be reissued (optional)

Optional Parameters

Command

```
COMMAND     = ReissueCertificate
CERTIFICATE = (TEXT)
SUB         = (TEXT)
CSR#        = (TEXT)
REISSUEEMAIL= (EMAIL)
DOMAIN[0-24]= (TEXT)
AUTHMETHOD= EMAIL|DNS|FILE
ALGORITHM   = SHA2-256|SHA256-FULL-CHAIN|SHA256-ECC-FULL|SHA256-ECC-HYBRID|PRIVATE-SHA1-PCA3G1|PRIVATE-SHA256-PCA3G1|PRIVATE-SHA1-PCA3G2|PRIVATE-SHA256-PCA3G2
```

Response

```
code                              = (INT)
property[CERTIFICATE][#]          = (TEXT)
property[SUB][#]                  = (TEXT)
property[STATUS][#]               = (TEXT)
property[SUB_STATUS][#]           = (TEXT)
property[FILEAUTH_NAME][#]        = (TEXT)
property[FILEAUTH_CONTENTS][#]    = (TEXT)
property[DNSAUTH_NAME][#]         = (TEXT)
```

Attributes

CSR#	The CSR to be used to generate the certificate
REISSUEEMAIL	Change the emailaddress used for the reissue, default is the admin - address. For True BusinessID with EV and all Symantec and Thawte certificates, the ReissueEmail must be set to either the administrative or the technical email address. For all other types of orders, the ReissueEmail address must be the administrative, technical, billing, or approver email address (optional)
DOMAIN0	Additional domain for SAN, which will be charged separately. From 0 to a maximum of 24. (optional)
ALGORITHM	Algorithm used for signing the certificate (optional)
SHA2-256	SHA256 intermediate certificate with a SHA-1 RSA root certificate
SHA256-FULL-CHAIN	You can get certificates with a full SHA-256 certificate chain when the encryption algorithm is RSA. Compared to the default SHA2-256 option, which has a SHA-1 root, the SHA256-FULLCHAIN option has a SHA-256 root

SHA256-ECC-FULL	Used with an ECC CSR, sets the certificate chain to an ECC certificate with an ECC root. Same behaviour as SHA2-256 for ECC certificates
SHA256-ECC-HYBRID	Used with an ECC CSR, sets the certificate chain to an ECC certificate with an RSA root. This option provides the performance strength of ECC with the browser compatibility of the RSA root
PRIVATE-SHA1-PCA3G1	PRIVATE-SHA1-PCA3G1 for Secure Site Pro only
PRIVATE-SHA256-PCA3G1	PRIVATE-SHA256-PCA3G1 for Secure Site Pro only
PRIVATE-SHA1-PCA3G2	PRIVATE-SHA1-PCA3G2 for Secure Site Pro only
PRIVATE-SHA256-PCA3G2	PRIVATE-SHA256-PCA3G2 for Secure Site Pro only
AUTHMETHOD	Method for authentication of the domainname (optional)
EMAIL	EMAIL
DNS	DNS
FILE	FILE
CERTIFICATE	ID of the new certificate order
SUB	ID of the new certificate sub
STATUS	Status of the request - process for the certificate order
SUB_STATUS	Status of the request - process for the sub
FILEAUTH_NAME	Name for the file needed for file based authentication
FILEAUTH_CONTENTS	Content for the file needed for file based authentification
DNSAUTH_NAME	Name of the RR entry needed for DNS based authentication

RenewCertificate

As with the ReissueCertificate command, RenewCertificate will create a new sub-certificate in a certificate order (parameter "certificate") from the existing data of the most recent sub-certificate. The new sub-certificate will have a new expiration date based on the period given and it is not possible to change the CSR during a renew. If you want to renew the certificate based on a different sub-certificate than the most recent, you have the option to use a specific sub-certificate (parameter "sub").

Required Parameters

Command

Command	= RenewCertificate
CERTIFICATE	= (TEXT)
SUB	= (TEXT)
PERIOD	= (INT)
APPROVEREMAIL[0-24]	= (TEXT)
AUTHMETHOD	= EMAIL|DNS|FILE
ALGORITHM	= SHA2-256|SHA256-FULL-CHAIN|SHA256-ECC-FULL|SHA256-ECC-HYBRID|PRIVATE-SHA1-PCA3G1|PRIVATE-SHA256-PCA3G1|PRIVATE-SHA1-PCA3G2|PRIVATE-SHA256-PCA3G2

Response

Certificate	= (TEXT)
Sub	= (TEXT)
certificate_status	= (TEXT)
sub_status	= (TEXT)

Optional Parameters

Command

Command	= RenewCertificate
CSR#	= optional

StatusCertificate

This command will give you all information about your certificate order (parameter "certificate") with all information about the latest sub-certificate. If you want to see the status of the certificate based on a different sub-certificate than the most recent, you have the option to use a specific sub-certificate (parameter "sub"). In addition to the order information, this command will return the metadata of the selected (most recent or given in the command) sub-certificate, a complete list of sub-certificates of the certificate order and the status for each sub-certificate. You also have the option to look into

Required Parameters

Command

COMMAND	= StatusCertificate
CERTIFICATE	= (TEXT)
SUB	= (TEXT)
WIDE	= 0|1

Response

code	= (INT)
description	= (TEXT)
queuetime	= (INT)
runtime	= (INT)
property[admincontact][#]	= (TEXT)
property[algorithm][#]	= (TEXT)
property[approveremail][#]	= (TEXT)
property[authmethod][#]	= EMAIL|DNS|FILE
property[billingcontact][#]	= (TEXT)
property[certificate][#]	= (TEXT)
property[certificate expiration date][#]	= (DATE)
property[class][#]	= (TEXT)
property[created date][#]	= (DATE)
property[crt][#]	= (TEXT)
property[crt extended key usage][#]	= (TEXT)
property[crt issuer][#]	= (TEXT)
property[crt issuer commonname][#]	= (TEXT)
property[crt issuer organization][#]	= (TEXT)
property[crt issuer organizational unit][#]	= (TEXT)
property[crt key usage type][#]	= (TEXT)
property[crt public key algorithm][#]	= (TEXT)
property[crt serial][#]	= (TEXT)
property[crt signature algorithm][#]	= (TEXT)
property[crt size][#]	= (INT)
property[crt subject][#]	= (TEXT)
property[crt validity not after][#]	= (DATE)

property[crt validity not before][#]	= (DATE)
property[crt version][#]	= (INT)
property[csr][#]	= (TEXT)
property[csr commonname][#]	= (TEXT)
property[csr country][#]	= (TEXT)
property[csr emailaddress][#]	= (TEXT)
property[csr location][#]	= (TEXT)
property[csr organization][#]	= (TEXT)
property[csr organizational unit][#]	= (TEXT)
property[csr public key algorithm][#]	= (TEXT)
property[csr signature algorithm][#]	= (TEXT)
property[csr size][#]	= (INT)
property[csr state][#]	= (TEXT)
property[csr subject][#]	= (TEXT)
property[domain][#]	=(TEXT)
property[intermediate crt][#]	= (TEXT)
property[ownercontact][#]	= (TEXT)
property[root crt][#]	= (TEXT)
property[status][#]	= (TEXT)
property[sub][#]	= (TEXT)
property[sub created date][#]	= (DATE)
property[sub id][#]	= (TEXT)
property[sub status][#]	= (TEXT)
property[sub updated date][#]	= (DATE)
property[techcontact][#]	= (TEXT)
property[updated date][#]	= (DATE)
property[webservertype][#]	= (TEXT)