

# AutoSSL Manager (SSL Automation) User Manual

This document will guide you to use OnlineNIC SSL Certificate Visual Automation.

Certificate ordering platform: <https://onlinenic.com/en/Certificates/ssl.html>

Automation consists of three aspects: Automated Re-issuance, Automated DCV, and Automated Certificate Deployment.

## i. Order an SSL certificate

1. Log in to your account (onlinenic.com) with your account ID and password.
2. Locate "Order SSL Cert" sub menu on the left.

The screenshot shows the 'SSL Order' page. On the left is a 'Main Menu' with 'SSL and Web Security' expanded to show 'Order SSL Cert'. The main content area has a checkbox 'Let SSL Wizard help you choose the right SSL Certificate.' Below it, a section 'I want to start from the specific product.' features a dropdown menu currently showing 'RapidSSL' with a list of other options including 'RapidSSL Wildcard', 'True BusinessID', 'QuickSSL Premium', etc. To the right of the dropdown is a 'Buy' button. Further right, there are promotional banners for 'GeoTrust' and 'SECTIGO'.

3. When placing an order, we use SectigoSSL as an example here, CSR generation: Select "System generates new CSR and private" for later Automated Deployment.

## SSL Order

|                     |                   |             |     |
|---------------------|-------------------|-------------|-----|
| Product             | Sectigo SSL       | Server type | AOL |
| How long to protect | 2 years - save 7% |             |     |

Existing CSR  The system generates CSR and private key; get it in Cert details.

|                    |                      |                    |                         |
|--------------------|----------------------|--------------------|-------------------------|
| Domain:            | <input type="text"/> | Country:           | Please select a country |
| State/Province:    | <input type="text"/> | City:              | <input type="text"/>    |
| Organization Name: | <input type="text"/> | Organization Unit: | <input type="text"/>    |
| Email:             | <input type="text"/> |                    |                         |

Include both **your-domain** and **www.your-domain** in the certificate (only relevant for single-domain SSL certificates)

Domain Validation Method:

Complete domain validation by clicking approval link in the approval emails which would be sent to domain Whois and default email addresses such as admin, administrator, hostmaster, webmaster@domainname etc.

Next

- Order is placed successfully. At the SSL certificate list, you may view its validation content for completing domain control validation.
- Follow the DNS verification instructions to create a DNS record with the domain's current registrar or DNS service provider (such as Cloudflare). The host and its content must be consistent with the content displayed in the panel (4 above).

| Type  | Name (required) <span style="color: red;">host</span>                 | Target (required) <span style="color: red;">value</span>                     | Proxy status  | TTL  |
|-------|---|--|---|------|
| CNAME | 335172E625B876872C50B<br>D5506B3B106<br><small>Use @ for root</small> | 94484FB28EF1BC1B6FA80.s<br>ectigo.com<br><small>E.g. www.example.com</small> | <input type="checkbox"/> <input checked="" type="checkbox"/> DNS only | Auto |

- After the DNS record (see 5) enters into effect (propagation worldwide), the certificate is verified and issued. The orders status is changed to COMPLETE.

|                          |                        |                         |          |            |          |                                     |
|--------------------------|------------------------|-------------------------|----------|------------|----------|-------------------------------------|
| <input type="checkbox"/> | <a href="#">330167</a> | olauto.ac[redacted].com | RapidSSL | 2026-06-09 | COMPLETE | <input checked="" type="checkbox"/> |
|--------------------------|------------------------|-------------------------|----------|------------|----------|-------------------------------------|

## ii. Automated Deployment Operation

This section describes how to Synchronize and push certificate orders to the Automation Platform.

- Right under the SSL list, tick the order that you want to set up "Automation".

### List SSL Order

Status: All
Product: All
Search
Advanced
Export

Selected: 1 order(s)
Reissue
Download Cert
AutoSSL
Auto-renew:  On
Clear

| <input type="checkbox"/>            | ORDER #                 | DOMAIN NAME          | PRODUCT     | ORDER TERM              | CERT EXPIRES ON | STATUS   | AUTO-RENEW                          |
|-------------------------------------|-------------------------|----------------------|-------------|-------------------------|-----------------|----------|-------------------------------------|
| <input type="checkbox"/>            | [redacted]              | [redacted]           | RapidSSL    |                         |                 | PENDING  | <input type="checkbox"/>            |
| <input type="checkbox"/>            | [redacted]              | [redacted]           | PositiveSSL |                         |                 | PENDING  | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> | <a href="#">#330167</a> | olauto[redacted].com | RapidSSL    | 2026-06-24 - 2027-06-09 | 2027-01-08      | COMPLETE | <input checked="" type="checkbox"/> |

- Create a sub-account for accessing the SSL Automation Panel.
  - A pop-up window of Sub Account options will appear after clicking "Automatic Deployment," as shown below:  
 Username: A **valid** and **active** email address (usually provided by the end user);  
 Password: Set your login password. You can use the quick tools to automatically generate it on its right.

SSL Automation Manager - Order #330167
✕

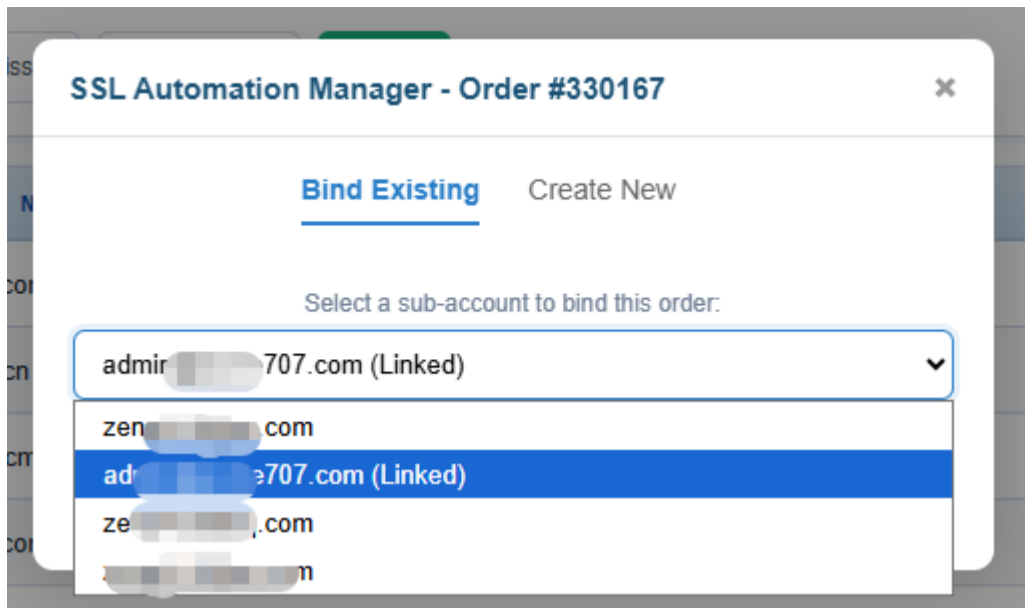
Bind Existing
Create New

🔄

Password will be encrypted before sync to DNS Manager

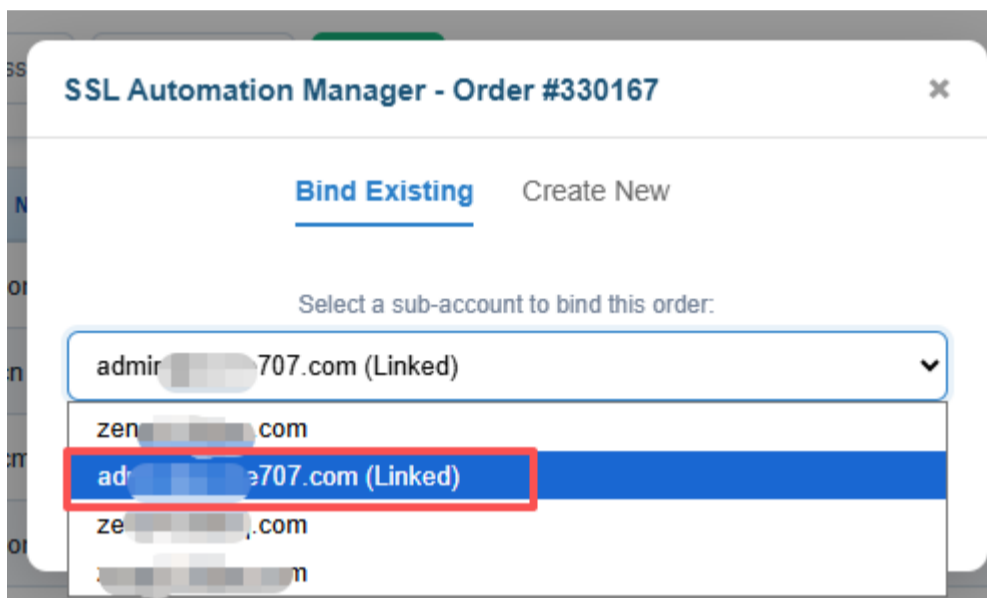
Create and Bind

- If the account already has sub-accounts, clicking "Automatic Deployment" will bring up a pop-up window as follows:  
 You can select one of the currently listed sub-accounts, or create a new account to associate with the certificate order to be deployed automatically.

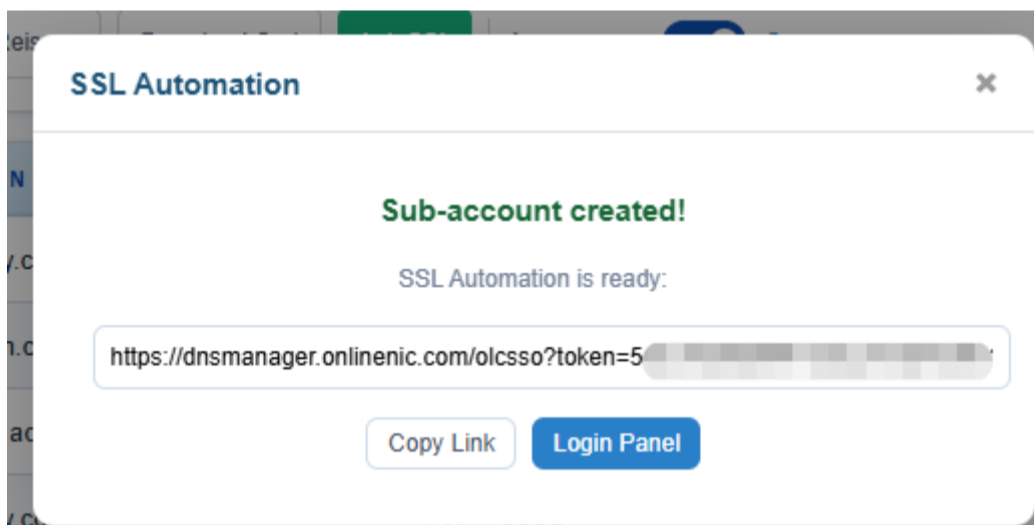


3. Confirm linking the SSL certificate orders

3.1. After completing step 2 above, Confirm and the next, and the certificate will be linked with the selected sub-account, as linked status.



3.2. Successful Synchronization



Login Panel: Click to open the Certificate Automation Management Panel;

Copy Link: one-time accessible link for the end user who you can sent it to.

Directly login: go to <https://dnsmanager.onlinenic.com> with the order's linked email address and password.

**iii. use the certificate automation management panel.**

**1. Login panel**

Panel URL: <https://dnsmanager.onlinenic.com>

Method 1, Username + Password

Username: The sub-account created in section 2.2 above

Password: The password you entered or generated in section 2.2 above

Method 2, the one-time accessible link mentioned in 3.2 above.

**2. Menu Introduction**

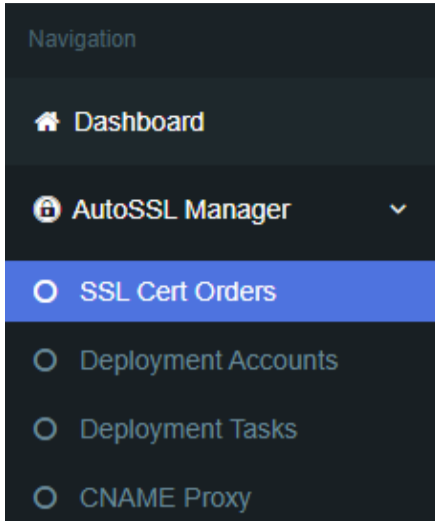
After logging into the panel, navigate to the "AutoSSL Manager" menu on the left.

SSL Cert Orders: Orders Synced from the BestCert account panel & linked with the sub account.

Deployment Account: to push the SSL certificate on to the various Website Management Toos/Panel, Server Management panel, Cloud Service Provider, and SSH Server;

Deployment Task: After Deployment Account is set up, the SSL certificate will be pushed to the target and deployed there.

CNAME Proxy: To set up domain (common name in the SSL certificate order) CNAME proxy, in order to complete DCV automatically.



## 2.1. SSL Cert Orders

You can view information such as Domain, Issuer, and expiration date of the listed SSL certificate.

Please enable "Auto-Reissue" feature if you want "automatic reissuance" before it expires.

| ID  | Cert Account | Domains | Cert Info  | Auto-Reissue                        | Issued     | Expires       | Status | Actions                    |
|-----|--------------|---------|--|-------------------------------------|------------|---------------|--------|----------------------------|
| 179 | BC(192)      | *.a...  | Algorithm:RSA(2048)<br>Issuer:Sectigo Public Server... | <input checked="" type="checkbox"/> | 2026-04-23 | 199 days left | Issued | Download Reissue Edit More |
| 173 | BC(192)      | www...m | Algorithm:RSA(2048)<br>Issuer:Sectigo Public Server... | <input checked="" type="checkbox"/> | 2026-04-23 | 199 days left | Issued | Download Reissue Edit More |

Showing 1 to 2 of 2 rows

## 2.2. Automated account deployment

Step 1, click "Add".

| ID  | Account Type | Account Name | Remark | Created             |
|-----|--------------|--------------|--------|---------------------|
| 193 | 宝塔面板         |              |        | 2026-04-23 11:15:15 |

Showing 1 to 1 of 1 rows

Step 2: Select the target. Here, we'll use the BT Panel (宝塔面板) and SSH server as examples to demonstrate how to add an Auto-Deployment Account.

Add Deployment Accounts

Panel / Tool

- 宝塔面板: 支持部署到宝塔面板&aaPanel搭建的站点、Docker、邮局与面板本身
- Kangle用户: 支持虚拟主机与CDN站点
- Kangle管理员: 支持虚拟主机与CDN站点
- 雷池WAF
- 宝塔云WAF
- Cdnfly
- LeCDN
- GoEdge: 支持GoEdge与FlexCDN
- 南墙WAF
- 1Panel: 更新面板证书管理内的SSL证书
- MW面板
- AcePanel: 支持 AcePanel 3.0+ 版本使用
- 耗子面板: 支持耗子面板 v2.5+ 版本使用
- 小皮面板
- AMH面板
- 群晖面板: 支持群晖DSM 6.x/7.x版本
- Lucky: 更新Lucky证书
- 飞牛OS: 更新飞牛OS的证书
- Proxmox VE: Deploy to PVE node
- K8S: Deploy to K8S cluster Secret & Ingress

### 2.2.1 Demonstration of adding "BT Panel" to the automatic deployment account

Panel address: The public IP address of the BT Panel

API key: The API key for the BT Panel - see below for how to obtain it.

#### 添加自动部署账户

\* 账户类型  宝塔面板 重新选择

\* 面板地址   
填写规则如: http://192.168.1.100:8888, 不要带其他后缀

\* 接口密钥

面板版本  Linux面板+Win经典版  Win极速版

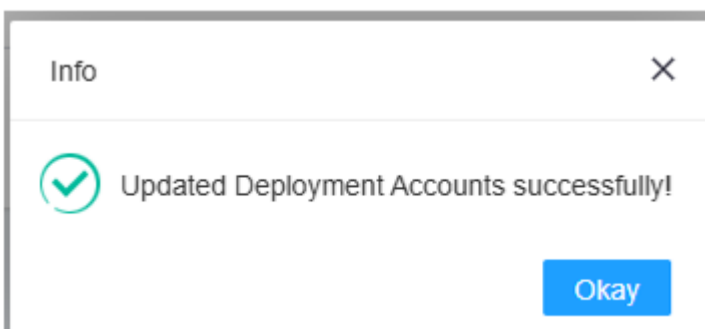
使用代理服务器  否  是

备注

How to obtain the API key for the BT Panel

The screenshot shows the BT Panel settings interface. On the left is a dark sidebar with menu items: Security, WAF, Mail Server, Files, Logs, Domains, Account, Terminal, Cron, App Store, and Settings. A red arrow points to the 'Settings' item. The main content area shows various settings. A red arrow points to the 'API' setting, which is currently turned on (green toggle) and has a 'Modify' button next to it. Other settings include 'CDN Proxy' (off), 'Auto Backup Panel' (on), 'Language' (English), 'Alias' (aaPanel Linux panel), 'Timeout' (24 Hour(s)), 'Default site folder' (/www/wwwroot), 'Default backup folder' (/www/backup), 'Server IP', 'Server time', and 'Panel user' (oumslgtj).

Click Submit: A validity check will be performed. If the information you entered is valid and correct, the following prompt will appear:



Click "Okay" to view your account information in the list.


| ID  | Account Type | Account Name               | Remark | Created             |
|-----|--------------|----------------------------|--------|---------------------|
| 193 | 宝塔面板         | https://1f[redacted]:23336 |        | 2026-04-23 11:15:15 |

## 2.2.1 Demonstration of adding " SSH Server " to the auto-deployment account


Step 1, Select SSH Server

Add Deployment Accounts

### Server



**SSH Server**  
Deploy certificates to Linux/Windows servers via...



**FTP Server**  
Upload certificates to FTP server

Step 2, enter the required server connection information.

Add Deployment Accounts

**\* Account Type**

SSH Server

Re-select

**\* Host**

**\* Port**

**\* Auth Method**  Password  Key-based

**\* Username**

**\* Password**

**\* Win OS**  No  Yes  
OpenSSH must be installed

**Remark**

**Tip:** Deploy via SSH connection. PHP ssh2 extension required. ✕

[Submit](#)

Clicking submit will trigger a validity check. Once the information is verified and accepted, you will see a success message, and view all the accounts in the list.

**\* Username**

**\* Password**

**\* Win OS**  No  Yes  
OpenSSH must be installed

**Remark**

Info ✕

✔ Added Deployment Accounts successfully!

[Okay](#)

**Tip:** Deploy via SSH connection. PHP ssh2 extension required.

Under the list,

**Search**

[Search](#)

[Refresh](#)

[+ Add](#)

[☰](#)

| ID  | Account Type | Account Name        | Remark | Created             | Actions  |
|-----|--------------|---------------------|--------|---------------------|--|
| 175 | SSH Server   | 47.8...104          |        | 2026-06-24 15:55:25 | <a href="#" style="background-color: #007bff; color: white; padding: 2px 5px;">Edit</a> <a href="#" style="background-color: #dc3545; color: white; padding: 2px 5px;">Delete</a> <a href="#" style="background-color: #6c757d; color: white; padding: 2px 5px;">Tasks</a> |
| 165 | 阿里云          | LTAI5t6L...cYN6K1hU |        | 2026-06-11 16:20:40 | <a href="#" style="background-color: #007bff; color: white; padding: 2px 5px;">Edit</a> <a href="#" style="background-color: #dc3545; color: white; padding: 2px 5px;">Delete</a> <a href="#" style="background-color: #6c757d; color: white; padding: 2px 5px;">Tasks</a> |

Showing 1 to 2 of 2 rows

### 2.2.3 Editing and Deleting

#### Actions

[Edit](#) [Delete](#) [Tasks](#)

The existing server login (connection) information can be updated by editing;

By deleting, the current automated deployment account can be removed;

Through the task: guides you to the automatic deployment of tasks, see below.

### 2.3. Automated Task Deployment

Prerequisites for automated deployment: Certificate order and automated deployment account are both in place and available.

The main problem that automated deployment tasks solve is: which certificate to deploy to which server.

#### 2.3.1 Add deployment task

**Demonstration 1: How to deploy the following certificate into the BT Panel:**

| ID  | Cert Account   | Domains | Cert Info                                       | Auto-Reissue                        | Issued     | Expires       | Status | Actions   |
|-----|----------------|---------|---|-------------------------------------|------------|---------------|--------|---|
| 179 | OnlineNIC(174) | olautc  | Algorithm:RSA(2048)<br>Issuer:RapidSSL TLS R... | <input checked="" type="checkbox"/> | 2026-06-24 | 199 days left | Issued | <a href="#">Download</a> <a href="#">Reissue</a><br><a href="#">Edit</a> <a href="#">More</a> |

Showing 1 to 1 of 1 rows

Click to add:

| ID | Deployment Accounts | Linked Certificate      | Remark | Enabled                  | Last Run            | Status    |
|----|---------------------|-------------------------|--------|--------------------------|---------------------|-----------|
| 25 |                     | ID:175 (Manual Reissue) |        | <input type="checkbox"/> | 2026-06-11 16:21:19 | Completed |

Add Deployment Tasks

\* Deployment Accounts

\* Linked Certificate

Remark

Select the BT panel.

If the information entered is correct and valid, a prompt will appear: Automatic deployment task added successfully.

Info

✓ SSL certificate deploy task executed successfully!

Okay

The status in the list shows "Completed," meaning the certificate and private key have been pushed to the target server.

| <input type="checkbox"/> | ID | Deployment Accounts | Linked Certificate | Remark | Enabled                             | Last Run            | Status    |
|--------------------------|----|---------------------|--------------------|--------|-------------------------------------|---------------------|-----------|
| <input type="checkbox"/> | 42 | 宝塔面板(1...)          | *.ac...07.com      |        | <input checked="" type="checkbox"/> | 2026-04-24 10:38:02 | Completed |

You can view website data in the BT Panel: Website -> Configuration -> SSL

By checking, you can see that the data has been transmitted to the site.

Site modification [we...com] -- Time added [2026-04-23 06:11:52]

Domain Manager

Subdirectory binding

Site directory

Limit access

Traffic control

URL rewrite

Default document

Config

SSL ←

PHP version

Composer

Current Certs - [Deployed] Business certificate Let's Encrypt Certificate holder

Certificate type: Other certificate Certificate brand: Sectigo... ver Authen...

Certificate domain(s): \*.ac...acr...om Expired: 202...07, Exp in 196 days

Force HTTPS:

Private key (KEY)

```
-----BEGIN PRIVATE KEY-----
MIIIEvwiBADANBgkqhkiG9w0BAQEFAASCBAkkggSI
AgEAAoIBAQDHOHB6ImDxCiVvk
rWl/wfWKc6Dpto86iW5EXD9sU+c67C5MQG2n7Jq0
NbKFITwMh/bFg1R3EXG8CsGk
6Lw5pt0JG...K3ne/vTp5P5o
xeXNgny...yRI9/
fCqiXpWgSn0ULBVw1NvpW/Ass9o0K7ZO6Rq0bYN
dTEydZBKAqei68A7csuHPJ00R
vcXjbDx43oRwN+wLMapq3lQqnocb4TDeaBY1yg93
```

Certificate (CRT/PEM)

```
-----BEGIN CERTIFICATE-----
MIIGfjCCBOagAwIBAgIRALN4h+sSErhMO2OYcYc5qs
kwDQYJKoZIhvcNAQELBQAw
YDELMAkGA1UEBhMCRC0xGDAWBgNVBAoTD1NIY
3RpZ28gTGltaxRIZDE3MDUGA1UE
AxMuU2Vjc...ydmVylEF1dGh
lbnRpY2F0...
NjAeFw0yNjA0MjMwMDAwMDBaFw0yNjExMDcyM
zU5NTlaMBGxhZjAUBgNVBAMMSou
YWNtZTcwNy5jb20wggiMA0GCSqGSIb3DQEBAQU
```

### Demonstration 2: How to deploy the certificate to the SSH target server:

Automatic Deployment Account: Select SSH Server

Associate SSL Certificate: Select the certificate.

Add Deployment Tasks

\* Deployment Accounts: 175\_SSH Server

\* Linked Certificate: 179\_olaut...m (OnlineNIC)

\* Certificate Format: PEM格式 (Nginx/Apache等)

\* Certificate Path: /ect/ssl/sslcertificate.pem complete file path, including file name

\* Private Key Path: /ect/ssl/sslcertificate.key complete file path, including file name

Pre-upload Command: Optional, execute before upload

If the information entered is correct and valid, a prompt will appear: Automatic deployment task added successfully.

load Command

Optional

Deployment task

Task is added successfully!

Okay

You can choose "Run now" to run the deployment task.

| ID | Deployment Accounts | Linked Certificate | Remark | Enabled                             | Last Run            | Status    | Actions           |
|----|---------------------|--------------------|--------|-------------------------------------|---------------------|-----------|-------------------|
| 30 | SSH Server(175)     | ID:179 (OnlineNIC) |        | <input checked="" type="checkbox"/> | Not yet             | Pending   | Run Now Edit More |
| 25 | 阿里云(165)            |                    |        | <input type="checkbox"/>            | 2026-06-11 16:21:19 | Completed | Re-run Edit More  |

Log in to the SSH server and you will see that the SSL certificate has been pushed to the target server.

```
root@izt4n2c3z:~# cd /etc/ssl/certificate/ && ls
cert.pem no.f key no.f pem_private.key rapidssl.sup_key.pem rapidssl.s ter.com.pem star_ ter_com.crt star_ er_com.key
```

## 2.4 CNAME Proxy

CNAME proxy is an important step in enabling automatic domain control (DCV) transfer after certificate resignation.

### 2.4.1 Glossary

The domain name being proxied: that is, the main domain name (common name) in the order;

Host record: The DNS record host header for the main domain name;

CNAME record value: The current CNAME record value for "hosthead.domain".

### 2.4.2 Example Description

Taking the following image as an example, we need to set a DNS CNAME record.

[pki-validation.example.com](http://pki-validation.example.com)

CNAME

[7336442fc8ef5314.onlinedns.net](http://7336442fc8ef5314.onlinedns.net)

| ID  | Proxy Domain       | Host            | CNAME Record                   | Status   | Created             | Actions |
|-----|--------------------|-----------------|--------------------------------|----------|---------------------|---------|
| 119 | olauto.acme707.com | _dnsauth.olauto | 7336442fc8ef5314.onlinedns.net | Verified | 2026-06-11 10:30:23 | Delete  |

Showing 1 to 1 of 1 rows

Got you your domain name or DNS service provider and set up a DNS CNAME record with the value showed in the panel. Once the DNS record is verified, the status will show "Verified".

After adding the CNAME record with your domain registrar or DNS provider, wait for it to take effect, which usually takes 1-24 hours. Please consult your current domain service provider for details.

### 2.4.3 CNAME proxy takes effect

Once the record takes effect, in the CNAME proxy list, click refresh to the right of the record; the status will display as "Verified." This indicates that the automated CNAME proxy has taken effect. Note: Records at both the DNS provider and the CNAME proxy must be retained and cannot be deleted.

### 2.4.4 Automated Certificate Re-signing

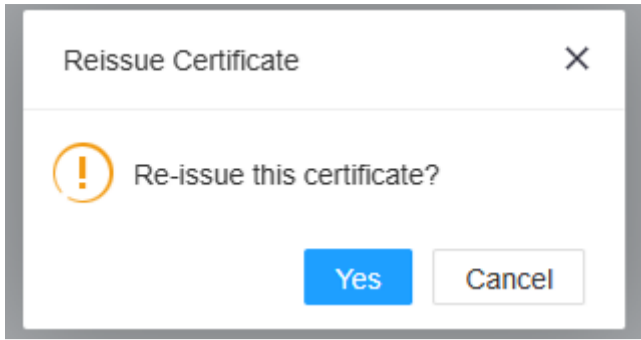
In the certificate list, find the SSL certificate order for the domain that has been "CNAME proxied" successfully – CNAME proxy status is "Verified".

| ID  | Cert Account   | Domains | Cert Info                  | Auto-Reissue                        | Issued     | Expires       | Status | Actions          |
|-----|----------------|---------|----------------------------|-------------------------------------|------------|---------------|--------|------------------|
| 179 | OnlineNIC(174) |         | Issuer:RapidSSL TLS RSA... | <input checked="" type="checkbox"/> | 2026-06-24 | 199 days left | Issued | Download Reissue |

Showing 1 to 1 of 1 rows

Click "Reissue" to confirm the reissuance of SSL certificate.

(Note: This is a manual Reissue example only. In normal procedure, Reissue will be performed automatically 30 days before the certificate expires.)



The order has entered the "pending verification" status.



Wait 5 minutes around for the certificate to be automatically issued. Once issued, the status will be changed "issued" and it will be pushed to the target device according to your setup on "Deployment Task".

#### iv. Customer Support

If you have question regarding SSL Automation or need assistance when using SSL Automation, please feel free to contact our customer support or account manager via ticket or Email.

Email: [onlinenic-partner@onlinenic.com](mailto:onlinenic-partner@onlinenic.com)