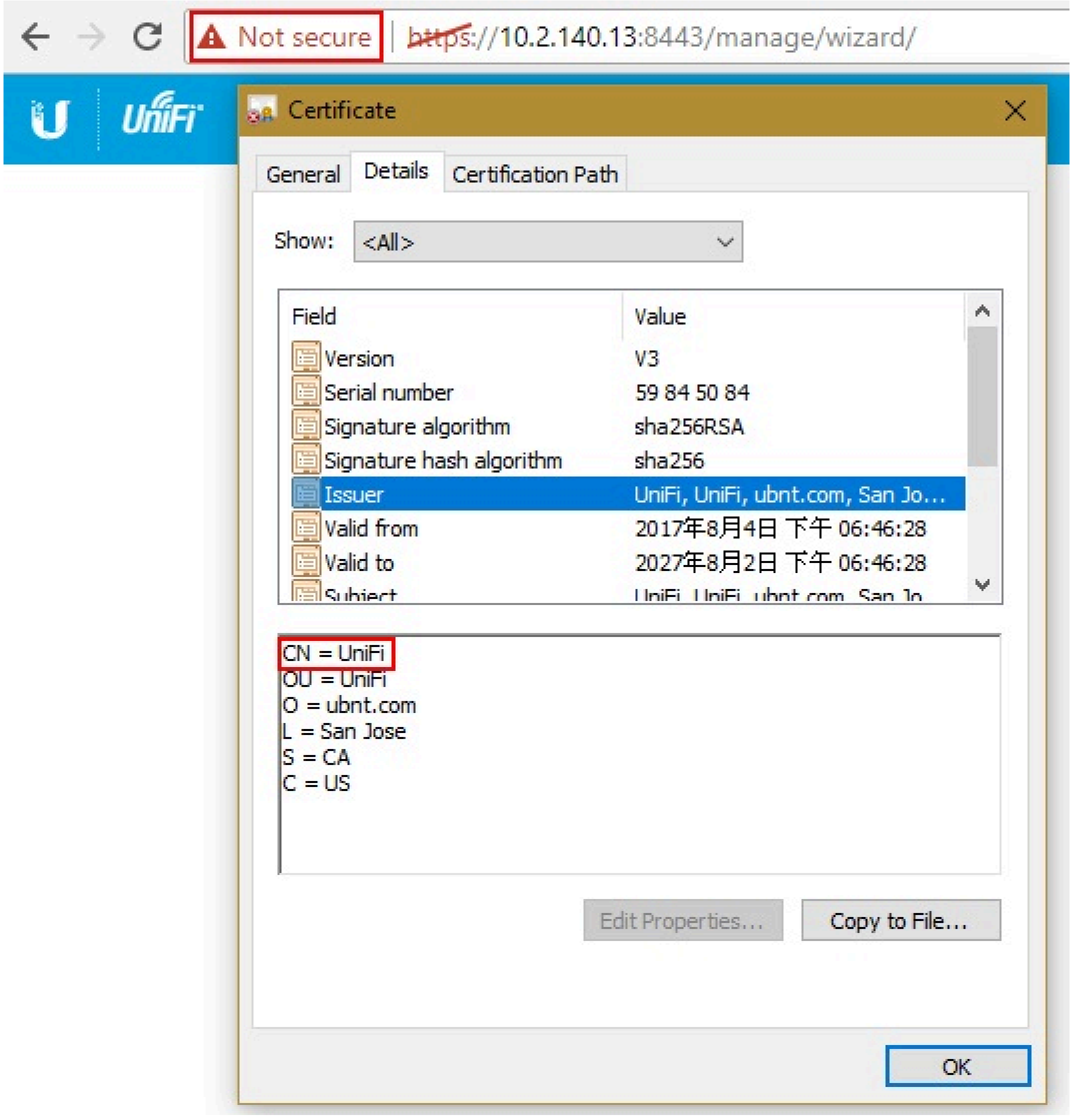
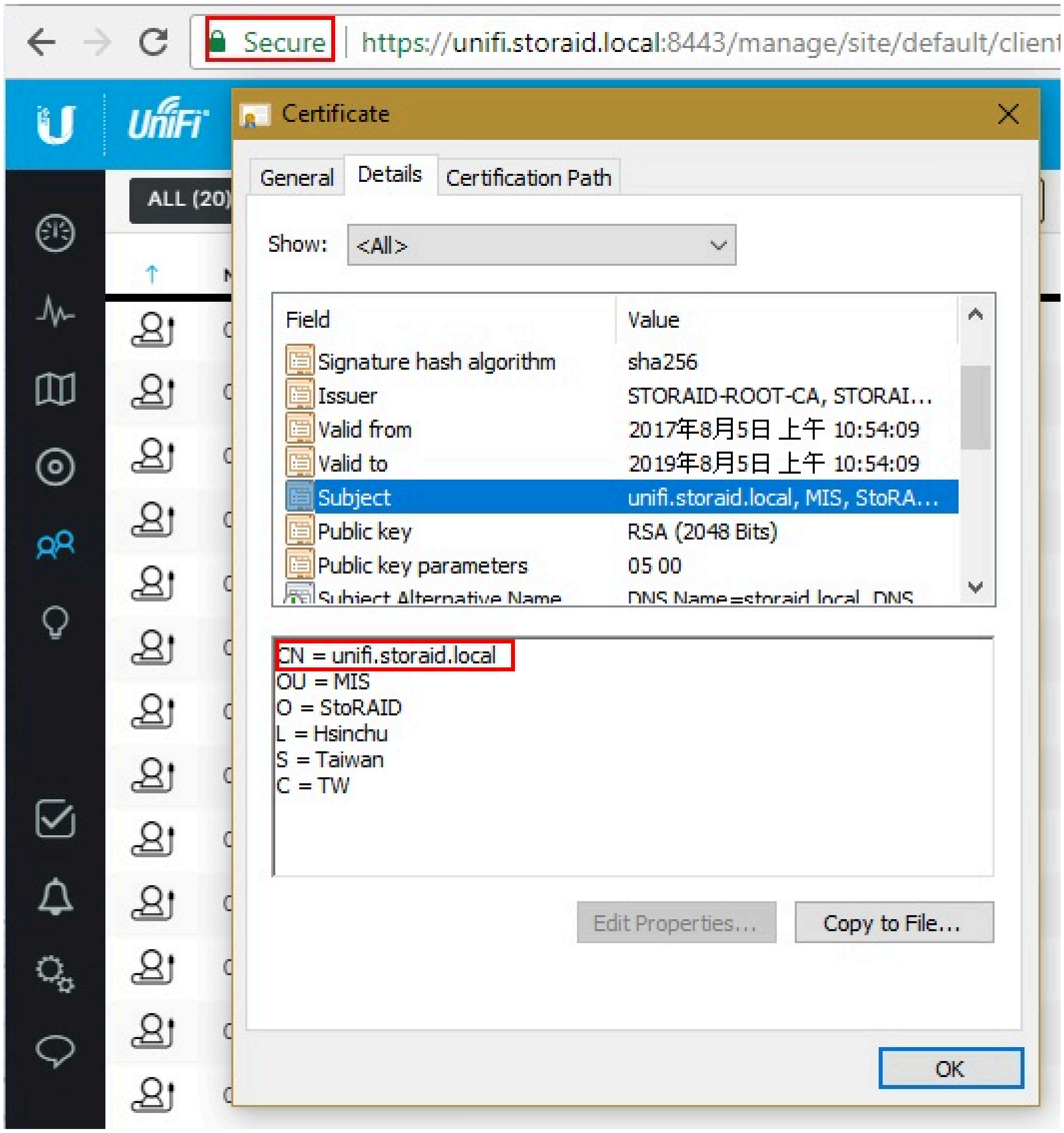
????????Web??, ????Not Secure??????????????:



Field	Value
Version	V3
Serial number	59 84 50 84
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	UniFi, UniFi, ubnt.com, San Jo...
Valid from	2017年8月4日 下午 06:46:28
Valid to	2027年8月2日 下午 06:46:28
Subject	UniFi, UniFi, ubnt.com, San Jo

CN = UniFi
OU = UniFi
O = ubnt.com
L = San Jose
S = CA
C = US

?????????? "?????????greenbar???" ????:



https://unifi.storaid.local:8443/manage/site/default/client

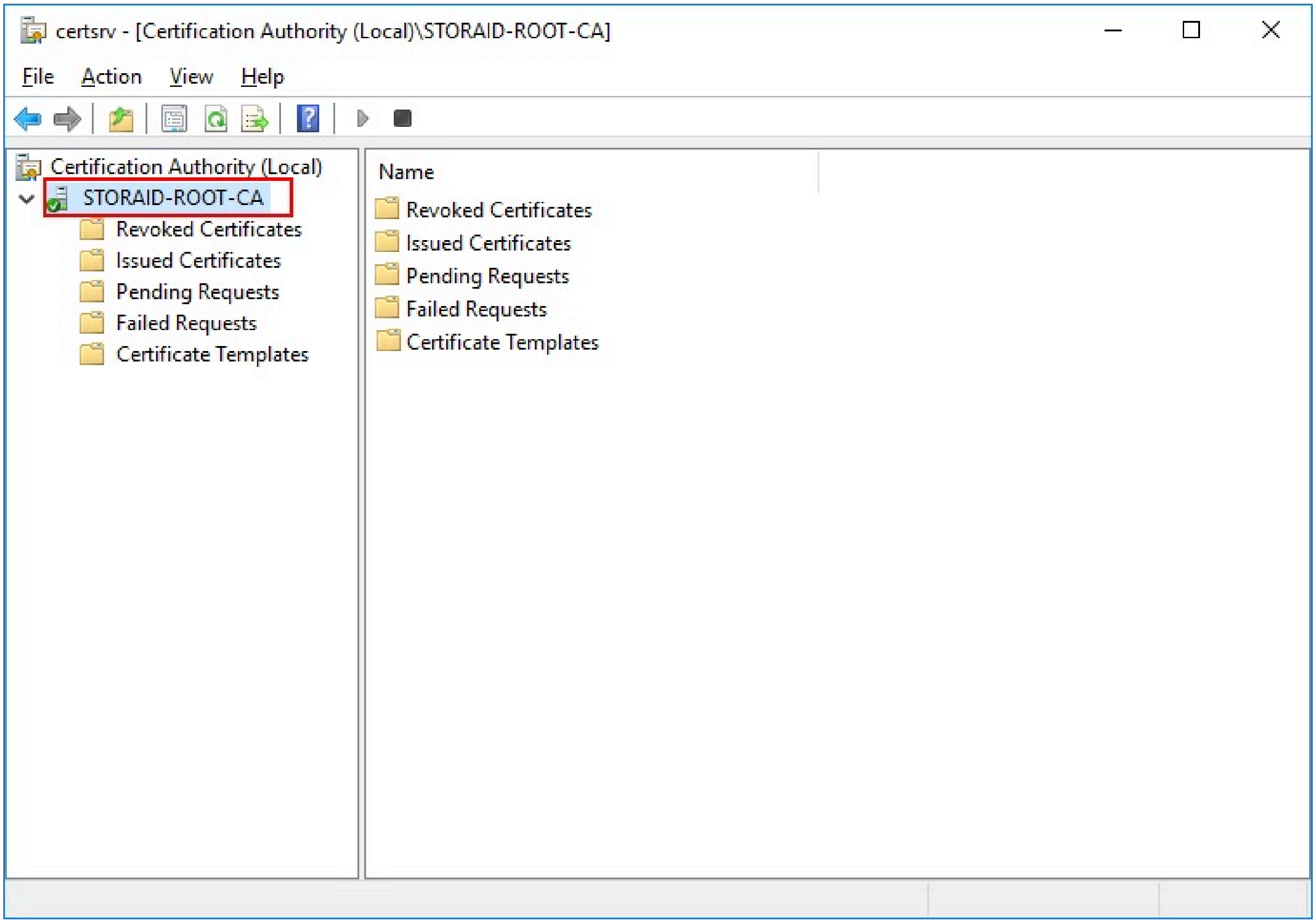
Show: <All>

Field	Value
Signature hash algorithm	sha256
Issuer	STORAID-ROOT-CA, STORAI...
Valid from	2017年8月5日 上午 10:54:09
Valid to	2019年8月5日 上午 10:54:09
Subject	unifi.storaid.local, MIS, StoRA...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Alternative Name	DNS Name=storaid.local, DNS

CN = unifi.storaid.local
OU = MIS
O = StoRAID
L = Hsinchu
S = Taiwan
C = TW

????????SSL??, ?????:
1. ??????EV SSL??.
2. ??let's encrypt????.
3. ????CA, ??????. ?????, ????CA????.

???????3????SSL???Unifi Controller???. ??????????CA:



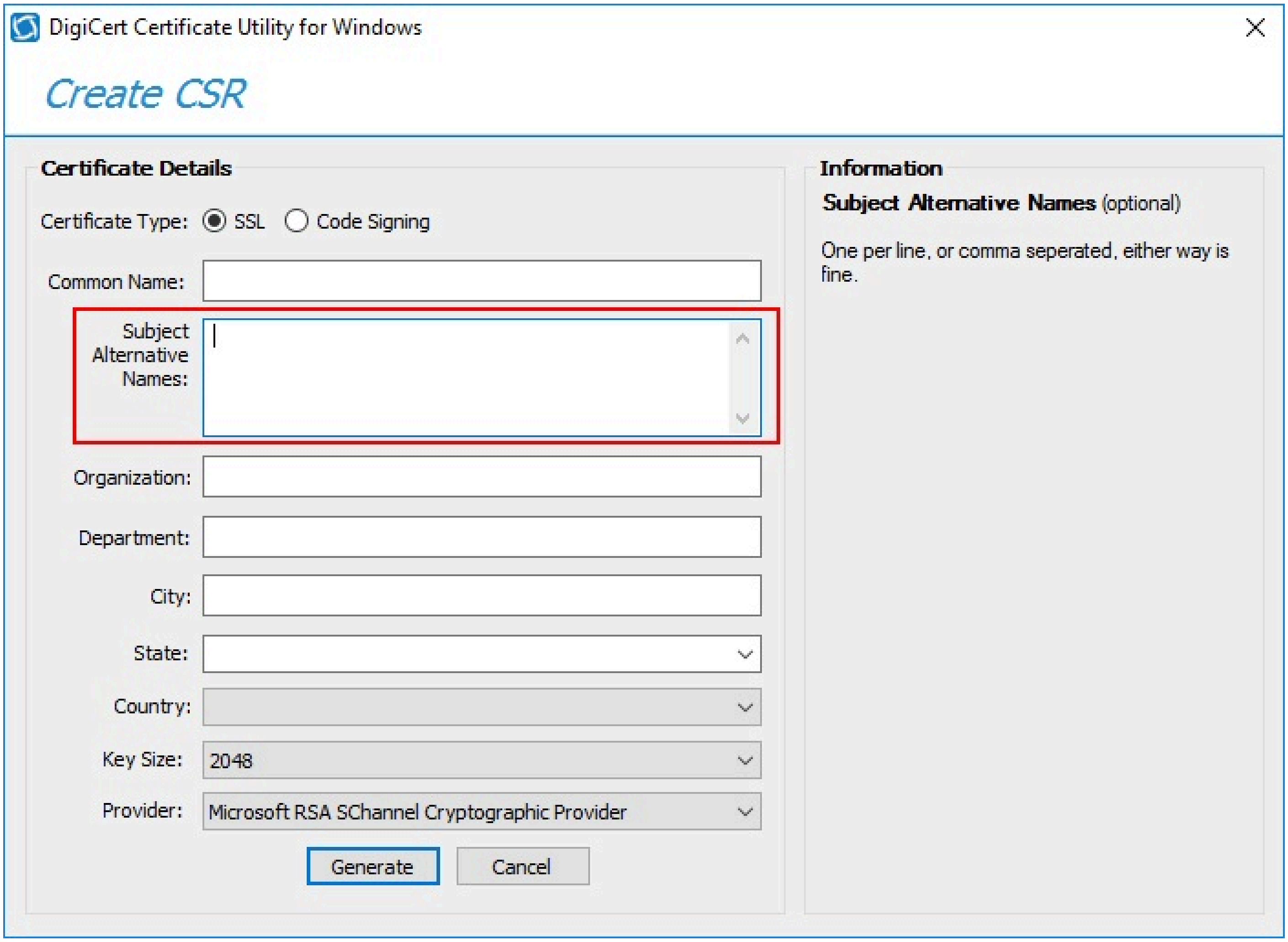
?????User??????CA?domain?. ??????, ?????Windows?????, ??????CSR???. ?Windows?????????:

1. ??certmgr??
2. ????????, ??DigiCertUtil, OpenSSL
3. ??IIS???????

??????IIS????????SAN(Subject Alternative Name)??. ???????????????, ??google chrome.

?????????????Not Secure.

?????DigiCertUtil??CSR???:



DigiCert Certificate Utility for Windows

Create CSR

Certificate Details

Certificate Type: ● SSL ○ Code Signing

Common Name:

Subject Alternative Names:

Organization:

Department:

City:

State:

Country:

Key Size: 2048

Provider: Microsoft RSA SChannel Cryptographic Provider

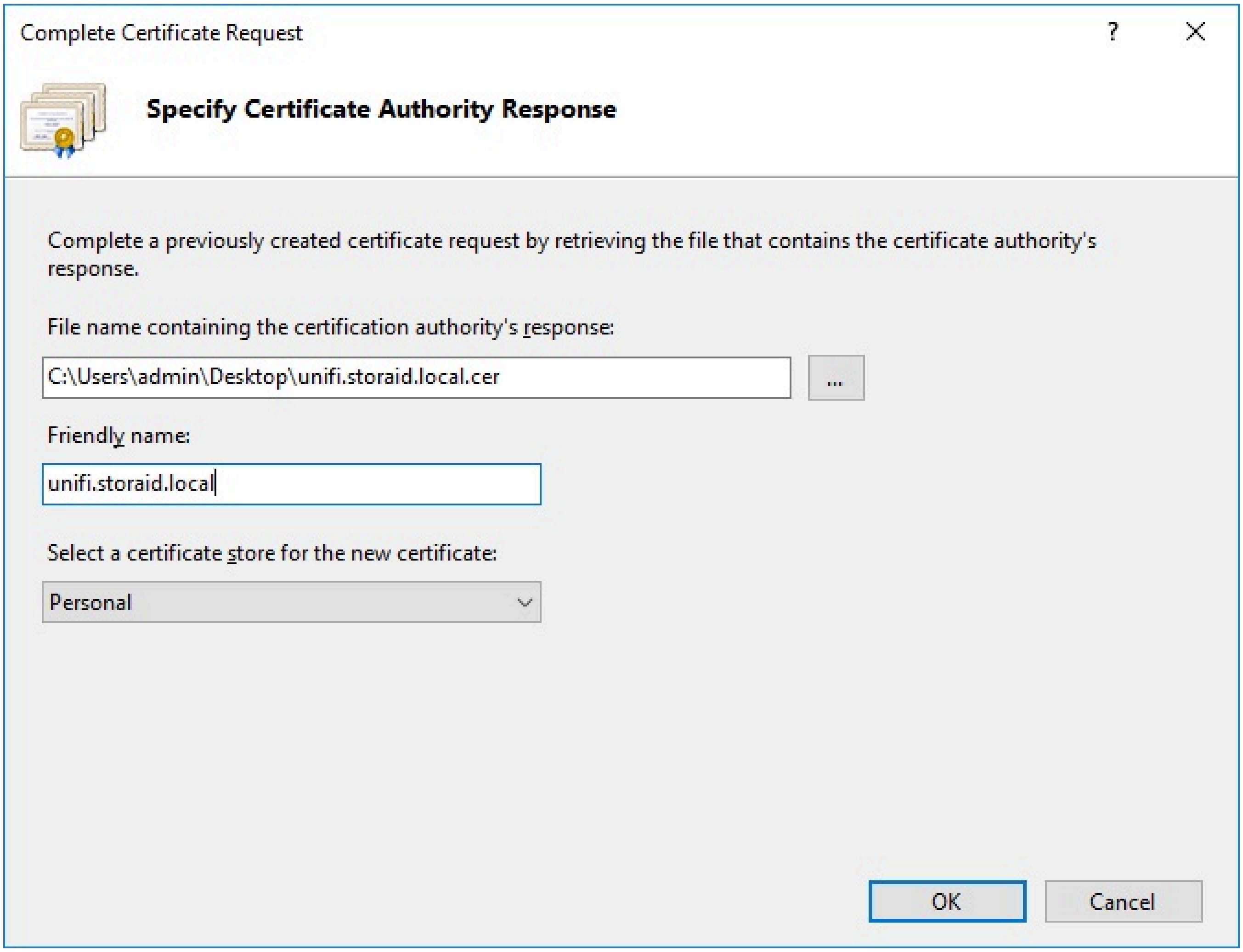
Information

Subject Alternative Names (optional)

One per line, or comma seperated, either way is fine.

???????SAN??, ?????????:
storaid.local
unifi.storaid.local

???CSR????, ????CA????CSR????SSL??. ??????IIS???????CSR??:


Complete Certificate Request
?
Specify Certificate Authority Response
...
OK
Cancel

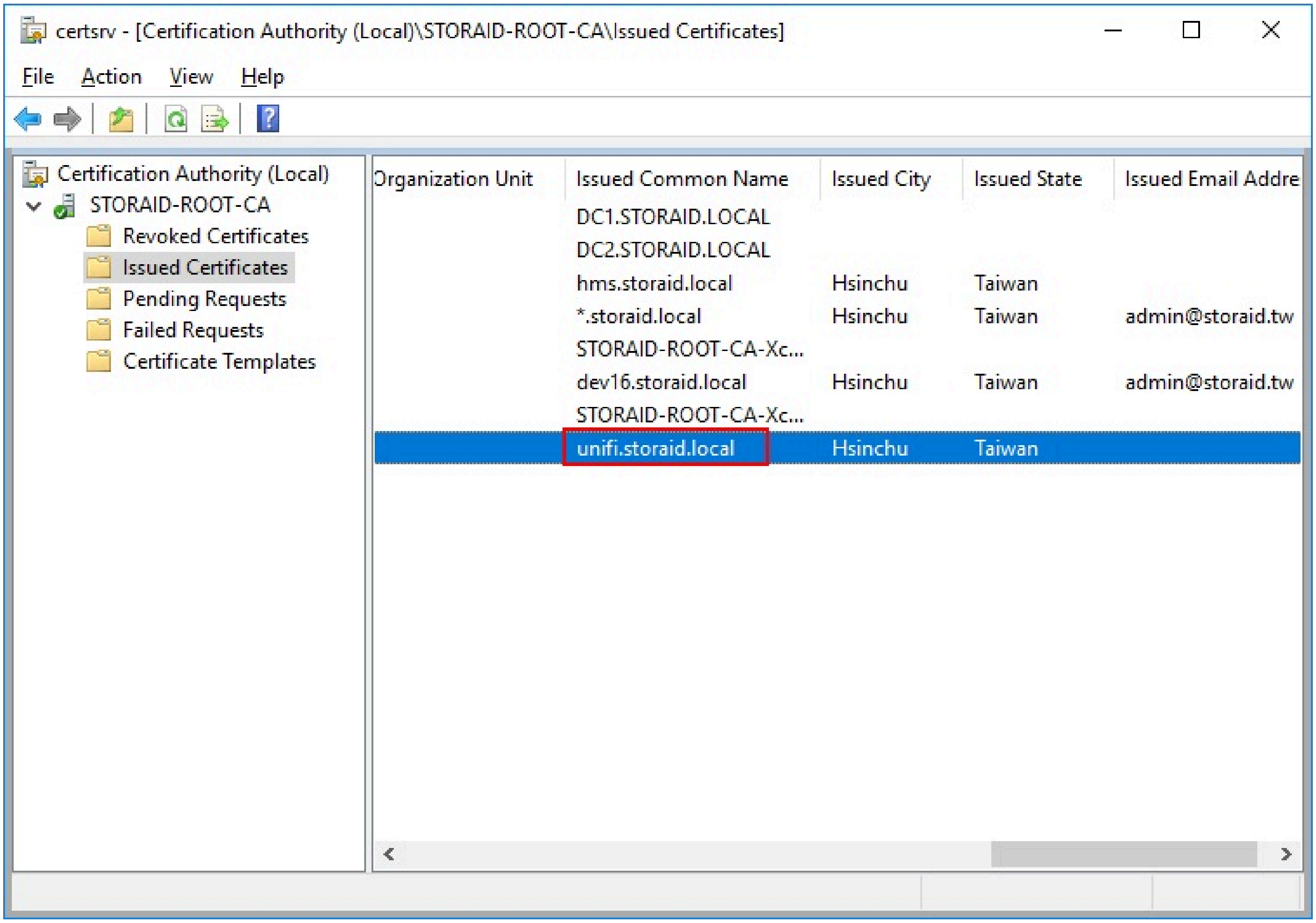
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response: C:\Users\admin\Desktop\unifi.storaid.local.cer

Friendly name: unifi.storaid.local

Select a certificate store for the new certificate: Personal

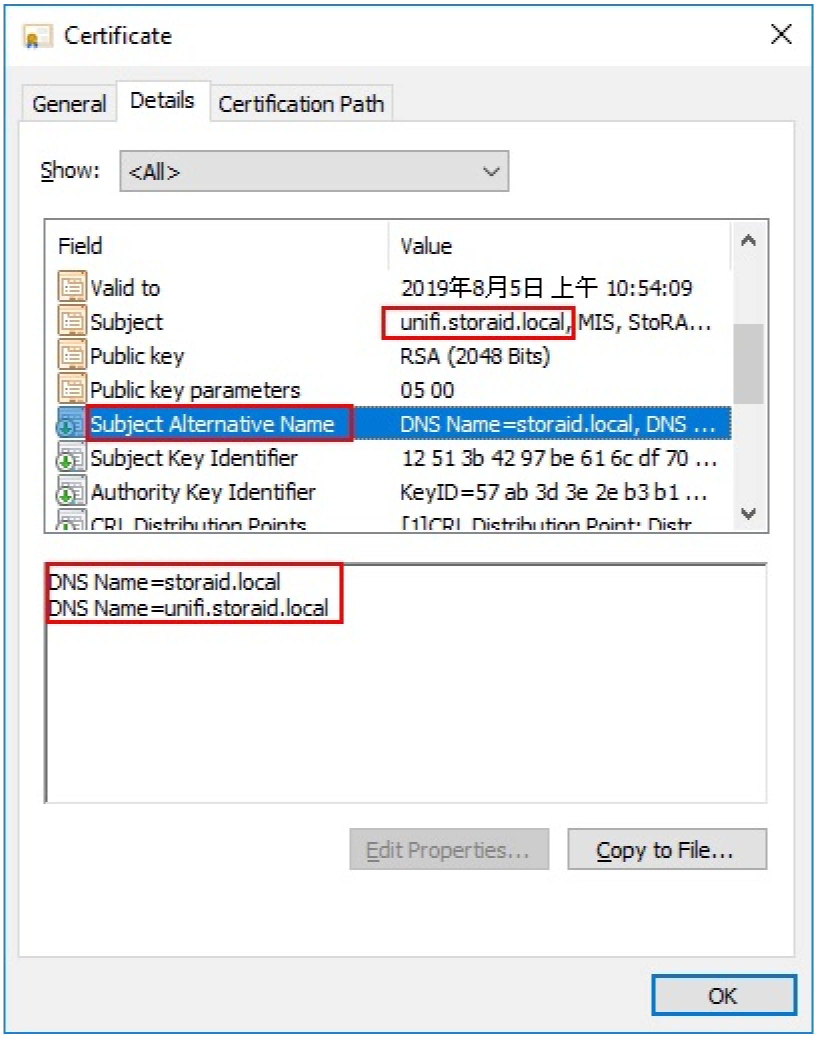
???, IIS??????????unifi.storaid.local?SSL??. ?????CA?????????SSL????.



certsrv - [Certification Authority (Local)\STORAID-ROOT-CA\Issued Certificates]

Organization Unit	Issued Common Name	Issued City	Issued State	Issued Email Addre
	DC1.STORAID.LOCAL			
	DC2.STORAID.LOCAL			
	hms.storaid.local	Hsinchu	Taiwan	
	*.storaid.local	Hsinchu	Taiwan	admin@storaid.tw
	STORAID-ROOT-CA-Xc...			
	dev16.storaid.local	Hsinchu	Taiwan	admin@storaid.tw
	STORAID-ROOT-CA-Xc...			
	unifi.storaid.local	Hsinchu	Taiwan	

??SSL????????, ?????????SAN??:

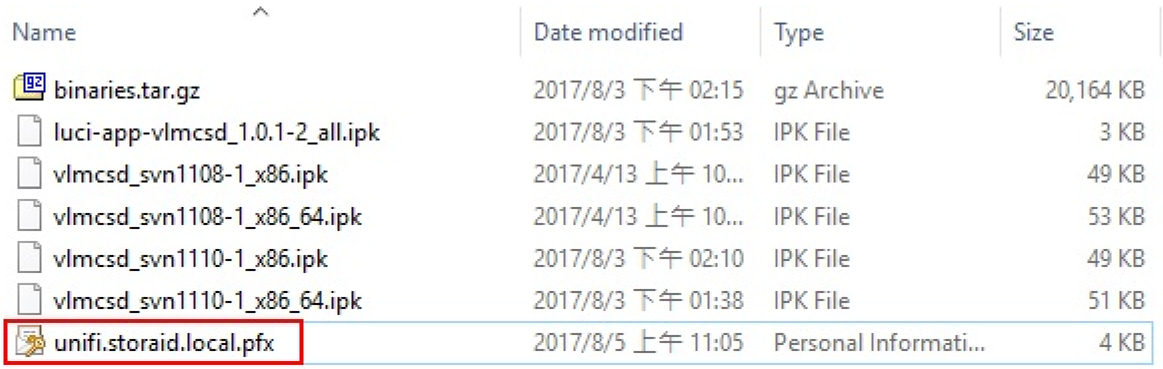


Show: <All>

Field	Value
Valid to	2019年8月5日 上午 10:54:09
Subject	unifi.storaid.local, MIS, StoRA...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Alternative Name	DNS Name=storaid.local, DNS ...
Subject Key Identifier	12 51 3b 42 97 be 61 6c df 70 ...
Authority Key Identifier	KeyID=57 ab 3d 3e 2e b3 b1 ...
CRL Distribution Points	[1]CRL Distribution Point: Distr

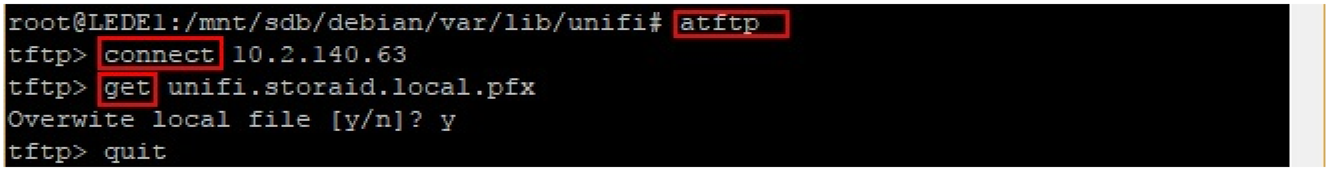
DNS Name=storaid.local
DNS Name=unifi.storaid.local

??????IIS????????pfx??????. pfx????private key??.



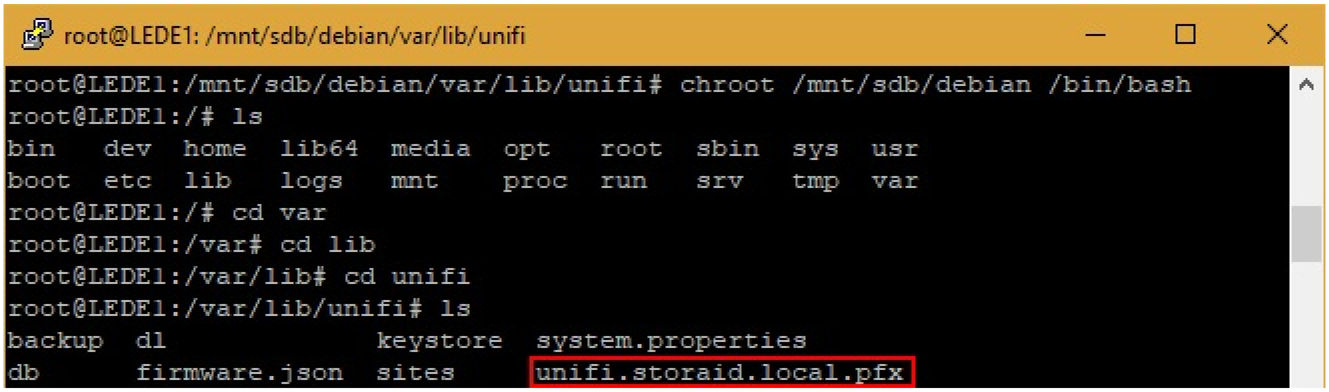
Name	Date modified	Type	Size
binaries.tar.gz	2017/8/3 下午 02:15	gz Archive	20,164 KB
luci-app-vlmcsd_1.0.1-2_all.ipk	2017/8/3 下午 01:53	IPK File	3 KB
vlmcsd_svn1108-1_x86.ipk	2017/4/13 上午 10...	IPK File	49 KB
vlmcsd_svn1108-1_x86_64.ipk	2017/4/13 上午 10...	IPK File	53 KB
vlmcsd_svn1110-1_x86.ipk	2017/8/3 下午 02:10	IPK File	49 KB
vlmcsd_svn1110-1_x86_64.ipk	2017/8/3 下午 01:38	IPK File	51 KB
unifi.storaid.local.pfx	2017/8/5 上午 11:05	Personal Informati...	4 KB

?????pfx???Unifi Controller?, ????OpenWRT??debian??. ???????OpenWRT?atftp??pfx???. ????, ??????unifi?? ??????:



```
root@LEDE1:/mnt/sdb/debian/var/lib/unifi# atftp
tftp> connect 10.2.140.63
tftp> get unifi.storaid.local.pfx
Overwrite local file [y/n]? y
tftp> quit
```

?????, ?????Unifi Controller?SSL????. ??debian????????unifi????????:



```
root@LEDE1:/mnt/sdb/debian/var/lib/unifi# chroot /mnt/sdb/debian /bin/bash
root@LEDE1:/# ls
bin   dev  home  lib64  media  opt   root  sbin  sys  usr
boot  etc  lib   logs   mnt    proc  run   srv   tmp  var
root@LEDE1:/# cd var
root@LEDE1:/var# cd lib
root@LEDE1:/var/lib# cd unifi
root@LEDE1:/var/lib/unifi# ls
backup  dl             keystore  system.properties
db      firmware.json  sites     unifi.storaid.local.pfx
```

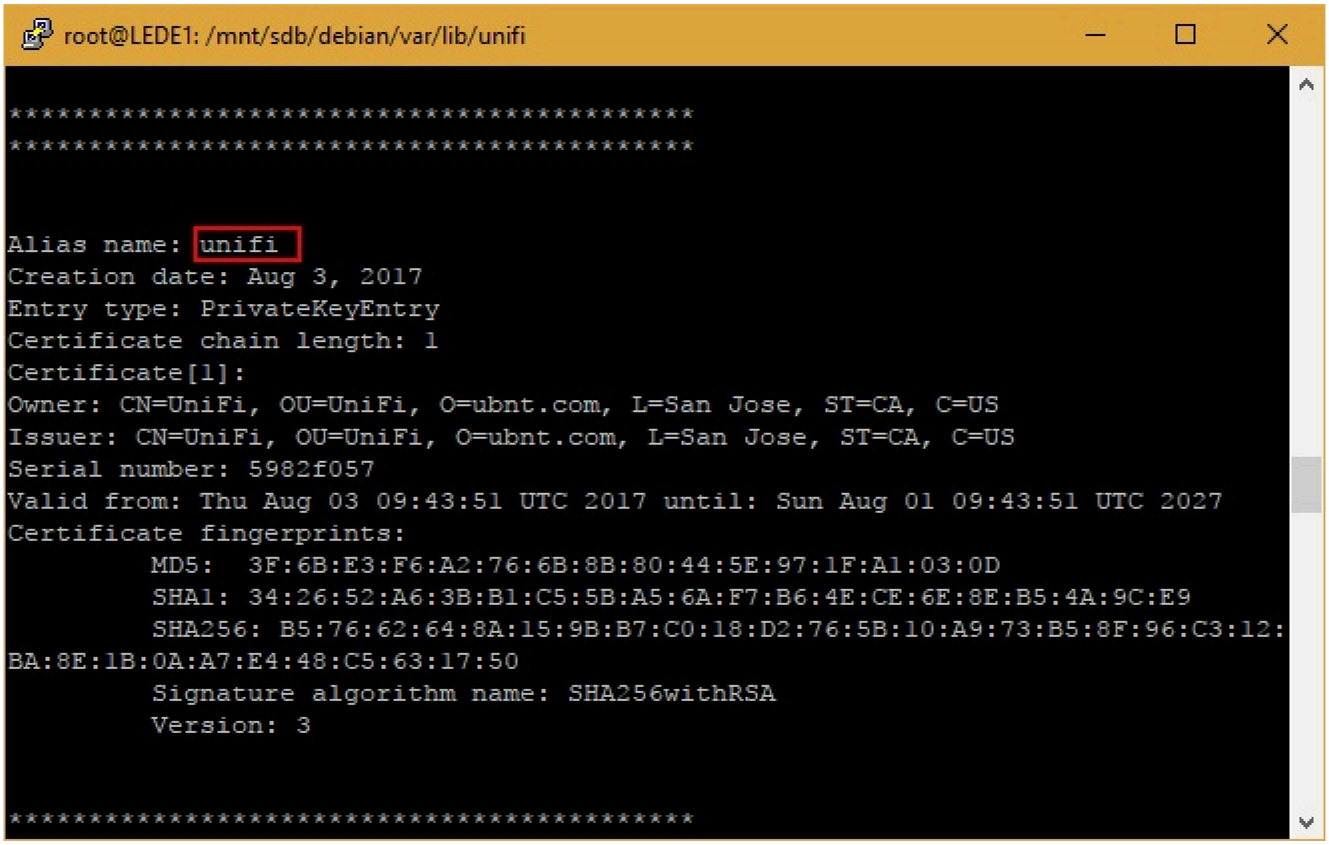
??????????????pfx???. ???????keystore???, ??????Unifi Controller???????.

?????, ?????????????????:

keytool -list -v -keystore keystore

????????keystore???. ??????? aircontrolenterprise

????????Unifi Controller?built-in SSL??:

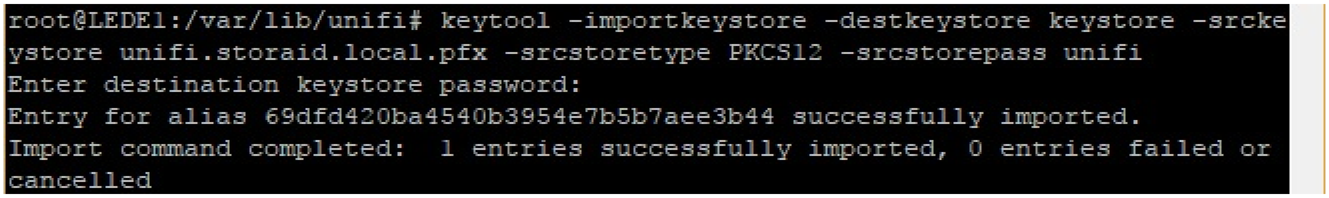


```

*******************************************
*******************************************


Alias name: unifi
Creation date: Aug 3, 2017
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=UniFi, OU=UniFi, O=ubnt.com, L=San Jose, ST=CA, C=US
Issuer: CN=UniFi, OU=UniFi, O=ubnt.com, L=San Jose, ST=CA, C=US
Serial number: 5982f057
Valid from: Thu Aug 03 09:43:51 UTC 2017 until: Sun Aug 01 09:43:51 UTC 2027
Certificate fingerprints:
         MD5:  3F:6B:E3:F6:A2:76:6B:8B:80:44:5E:97:1F:A1:03:0D
         SHA1: 34:26:52:A6:3B:B1:C5:5B:A5:6A:F7:B6:4E:CE:6E:8E:B5:4A:9C:E9
         SHA256: B5:76:62:64:8A:15:9B:B7:C0:18:D2:76:5B:10:A9:73:B5:8F:96:C3:12:
BA:8E:1B:0A:A7:E4:48:C5:63:17:50
         Signature algorithm name: SHA256withRSA
         Version: 3


*******************************************
```

???????(alias)?unifi. ????pfx??????keystore, ??????:

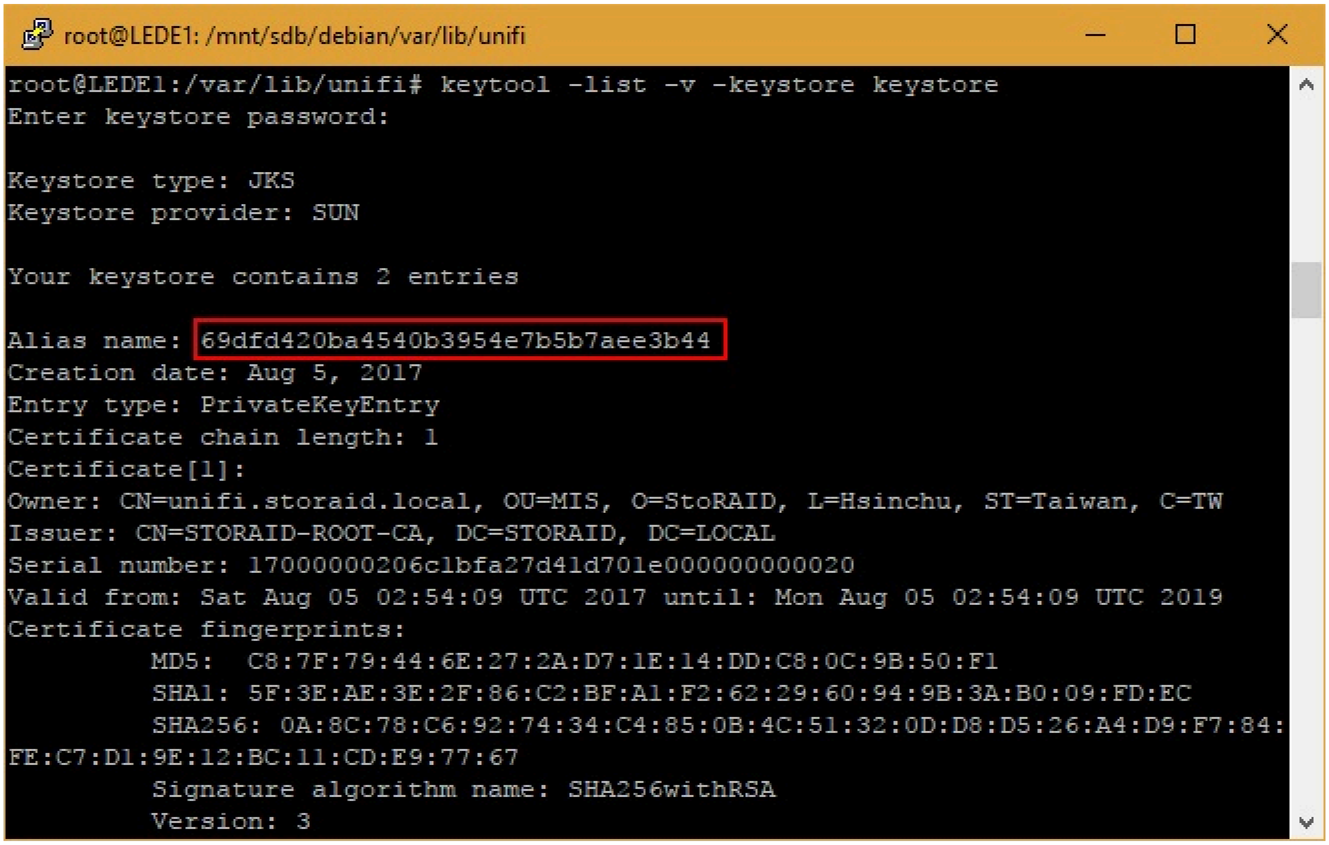
keytool -importkeystore -destkeystore keystore -srckeystore unifi.storaid.local.pfx -srcstoretype PKCS12 -srcstorepass unifi

-srcstorepass???????pfx??????. ?????unifi.



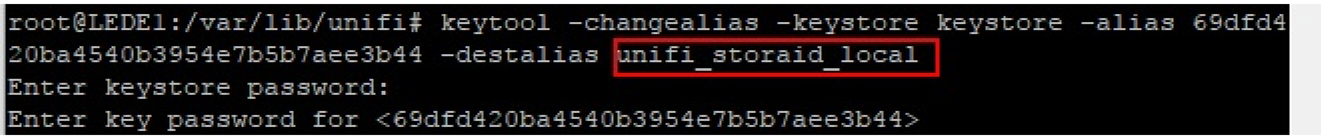
```
root@LEDE1:/var/lib/unifi# keytool -importkeystore -destkeystore keystore -srcke
ystore unifi.storaid.local.pfx -srcstoretype PKCS12 -srcstorepass unifi
Enter destination keystore password:
Entry for alias 69dfd420ba4540b3954e7b5b7aee3b44 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or
cancelled
```

?????????, ??????keystore???(aircontrolenterprise).
?????, ???keytool -list -v -keystore keystore??????????????pfx?????:



```
root@LEDE1:/var/lib/unifi# keytool -list -v -keystore keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: 69dfd420ba4540b3954e7b5b7aee3b44
Creation date: Aug 5, 2017
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=unifi.storaid.local, OU=MIS, O=StoRAID, L=Hsinchu, ST=Taiwan, C=TW
Issuer: CN=STORAID-ROOT-CA, DC=STORAID, DC=LOCAL
Serial number: 17000000206c1bfa27d41d701e000000000020
Valid from: Sat Aug 05 02:54:09 UTC 2017 until: Mon Aug 05 02:54:09 UTC 2019
Certificate fingerprints:
         MD5:  C8:7F:79:44:6E:27:2A:D7:1E:14:DD:C8:0C:9B:50:F1
         SHA1: 5F:3E:AE:3E:2F:86:C2:BF:A1:F2:62:29:60:94:9B:3A:B0:09:FD:EC
         SHA256: 0A:8C:78:C6:92:74:34:C4:85:0B:4C:51:32:0D:D8:D5:26:A4:D9:F7:84:
FE:C7:D1:9E:12:BC:11:CD:E9:77:67
         Signature algorithm name: SHA256withRSA
         Version: 3
```

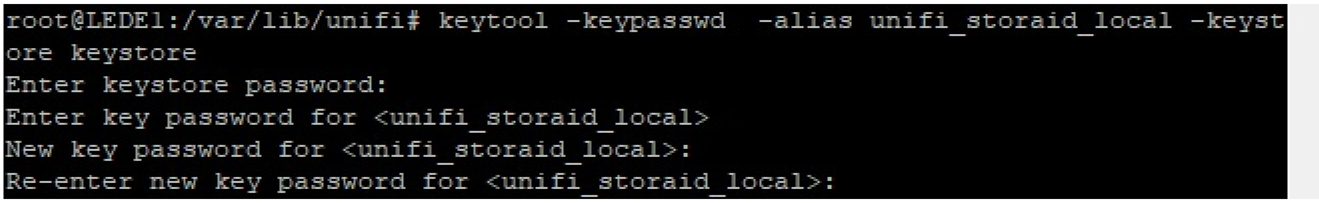
????????????????. ???????????(alias)??????, ???????????????????.
????????(alias)???, ??????:
keytool -changealias -keystore keystore -alias [alias of privateKey goes here] -destalias [new_alias_name]



```
root@LEDE1:/var/lib/unifi# keytool -changealias -keystore keystore -alias 69dfd4
20ba4540b3954e7b5b7aee3b44 -destalias unifi_storaid_local
Enter keystore password:
Enter key password for <69dfd420ba4540b3954e7b5b7aee3b44>
```

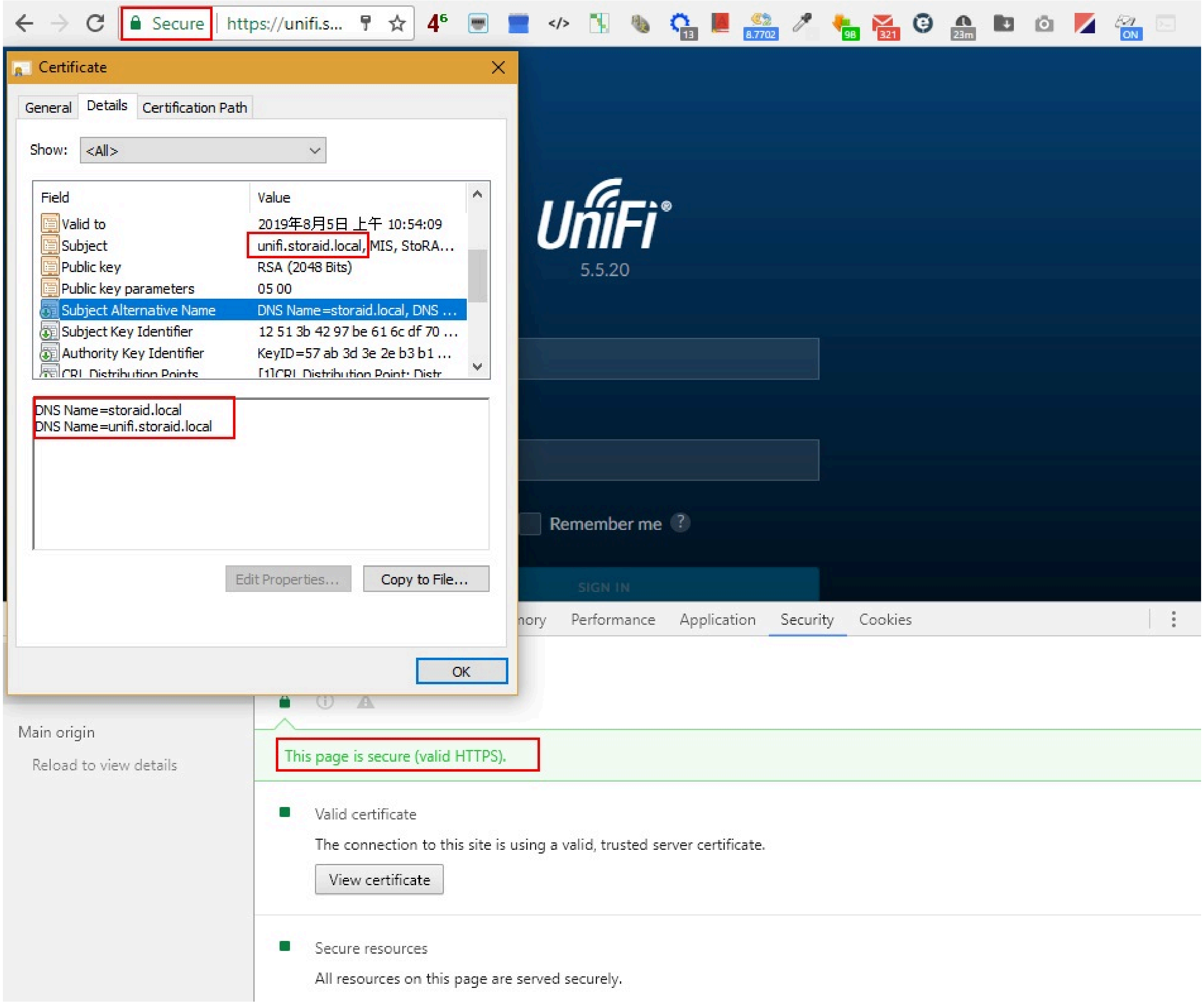
????????(alias)???unifi_storaid_local, ?????????????????.
????keystore???(aircontrolenterprise).
????pfx????????, ?????unifi.

????(alias)??????, ??????????pfx???????. ??????: keytool -keypasswd -alias [alias_name] -keystore keystore



```
root@LEDE1:/var/lib/unifi# keytool -keypasswd  -alias unifi_storaid_local -keyst
ore keystore
Enter keystore password:
Enter key password for <unifi_storaid_local>
New key password for <unifi_storaid_local>:
Re-enter new key password for <unifi_storaid_local>:
```

??????, ??????????.
????keystore??(aircontrolenterprise)
????pfx???????(unifi)
????????, ????? aircontrolenterprise
?????????, aircontrolenterprise
????????, ??????? shutdown -r now ????????. ??????OpenWRT???, ???????OpenWRT?reboot. reboot???, ???? ???????SSL??????domain name. ???????unifi.storaid.local.



Field	Value
Valid to	2019年8月5日 上午 10:54:09
Subject	unifi.storaid.local, MIS, StoRA...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Alternative Name	DNS Name=storaid.local, DNS ...
Subject Key Identifier	12 51 3b 42 97 be 61 6c df 70 ...
Authority Key Identifier	KeyID=57 ab 3d 3e 2e b3 b1 ...
CRL Distribution Points	[1]CRL Distribution Point: Distr

DNS Name=storaid.local
DNS Name=unifi.storaid.local

Main origin

Reload to view details

This page is secure (valid HTTPS).

Valid certificate

The connection to this site is using a valid, trusted server certificate.

Secure resources

All resources on this page are served securely.

?Greenbar, ?SAN??, ?????Secure. ??SSL?????????.