

# Generate CSR for Third-Party Certificates and Download Unchained Certificates to the WLC

Document ID: 70584

---

## Introduction

### Prerequisites

- Requirements

- Components Used

- Conventions

### Background Information

- Support for Chained Certificate

### CSR

- Generate a CSR

- Download the Third-Party Certificate to the WLC

### Verify

### Troubleshoot

- Expired Intermediate VeriSign Certificate

### Related Information

---

## Introduction

This document explains how to generate a Certificate Signing Request (CSR) in order to obtain a third-party certificate and how to download an unchained certificate to a wireless LAN (WLAN) controller (WLC).

## Prerequisites

### Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure the WLC, lightweight access point (LAP), and wireless client card for basic operation
- Knowledge of how to use the OpenSSL application for Secure Socket Layer (SSL)

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco 4400 WLC that runs firmware version 4.2.61.0
- OpenSSL application for Microsoft Windows
- Enrollment tool that is specific to the third-party certification authority (CA)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

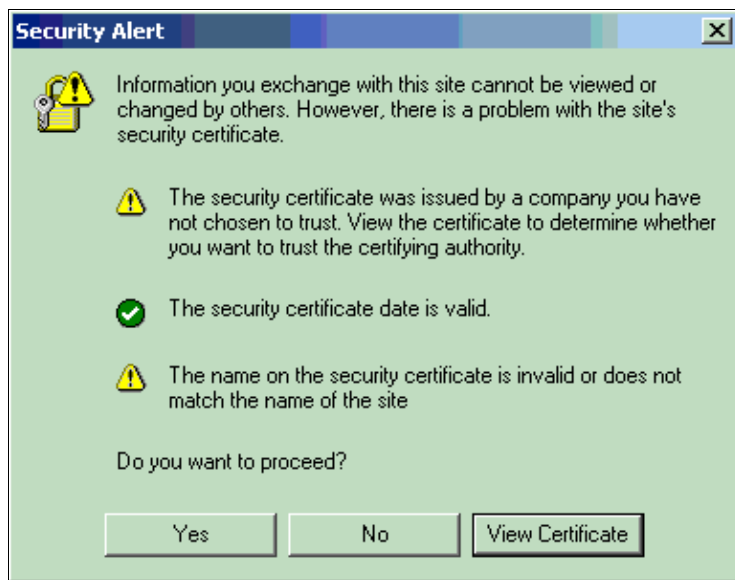
Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

By default, WLCs use a built-in self-signed SSL certificate. The WLCs use this SSL certificate in one of these situations:

- When the clients try to connect to the WLAN network with use of SSL-based web authentication
- When a user tries to log in to the WLC with use of Secure HTTP (HTTPS) (WebAdmin authentication)

In either case, on the first attempt to access the WLC, the you can receive a web-browser security alert that looks like this:



You are prompted to accept the certificate from the WLC because the clients do not have a trusted root certificate for the certificate that is installed on the WLC. The SSL certificate on the WLC is not in the list of certificates that the client system trusts. There are two ways to stop the generation of this web-browser security alert popup window:

- Use the self-signed SSL certificate on the WLC and configure the client stations to accept the certificate.

Include the self-signed certificate on the WLC in the list of certificates that are trusted on the client station.

- Generate a CSR and install a certificate that is signed by a source (a third-party CA) for which the clients already have the trusted root certificates installed, such as VeriSign.

You can do this off line from the WLC with the use of a program like OpenSSL. Refer to The OpenSSL Project for more information on OpenSSL.

This document explains how to generate a CSR for a third party certificate and how to download an unchained web authentication certificate to the WLC.

## Support for Chained Certificate

WLC software versions earlier than 5.1.151.0 do not support chained certificates. Use one of these options in order to workaround this issue:

- Acquire an unchained certificate from the CA, which means that the signing root is trusted.
- Have all valid intermediate CA root certificates, trusted or untrusted, installed on the client.

With version 5.1.151.0 and later, the WLCs support chained certificates for web authentication. Web authentication certificates can be any of these:

- Chained
- Unchained
- Autogenerated

Refer to Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC for information on how to use Chained certificates on WLC.

## CSR

A certificate is an electronic document that you use in order to identify a server, a company, or some other entity and to associate that identity with a public key.

CAs are entities that validate identities and issue certificates. The certificate that the CA issues binds a particular public key to the name of the entity that the certificate identifies (such as the name of a server or device). Only the public key that the certificate certifies works with the corresponding private key that is possessed by the entity that the certificate identifies. Certificates help prevent the use of fake public keys for impersonation.

A CSR is a message that an applicant sends to a CA in order to apply for a digital identity certificate. For the most part, a third-party CA company, like Entrust or VeriSign, requires a CSR before the company can create a digital certificate.

CSR generation is independent of the device on which you plan to install an external certificate. So a CSR and private key file can be generated on any individual Windows or UNIX machine. CSR generation is not switch-dependent or appliance-dependent in this case.

Because the WLC does not generate a CSR, you must use a third-party application such as OpenSSL in order to generate a CSR for the WLC.

The section Generate a CSR discusses the commands that you must issue on the OpenSSL application in order to generate a private key and the CSR.

Complete these steps in order to get a third-party certificate from a CA:

1. Generate a private/public key pair.
2. With use of the public key, generate a CSR.
3. Submit the CSR to a CA.
4. Retrieve the certificate that the CA produces.
5. Combine the certificate and private key into a pkcs12 file.
6. Convert the pkcs12 file to a privacy enhanced mail (PEM) encoding file.
7. Download the new third-party certificate (.pem file) onto the WLC.

# Generate a CSR

Complete these steps in order to generate a CSR and submit the CSR to the third-party CA:

1. Install and open the OpenSSL application.

**Note:** Cisco recommends you use OpenSSL version 0.9.8 for Microsoft Windows.

In Windows, by default, openssl.exe is located at c:\openssl\bin.

2. Issue this command:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
```

After you issue the command, there is a prompt for some information: country name, state, city, and so on.

3. Provide the required information.

The most important information that you need to provide correctly is the Common Name. Ensure that the host name that is used to create the certificate (Common Name) matches the Domain Name System (DNS) host name entry for the virtual interface IP on the WLC and that the name actually exists in the DNS as well. Also, after you make the change to the VIP interface, you must reboot the system in order for this change to take effect.

**Note:** The DNS host name must be entered in the WLC under **Interfaces > Edit** for the virtual interface. This is used to verify the source of certificates when Web Auth is enabled. Reboot the controller to have this change take effect.

After you provide all the required details, you end up with two files:

- ◆ a new private key that has the name mykey.pem
- ◆ a CSR that has the name myreq.pem

These files are stored in the default directory where OpenSSL is installed (c:\openssl\bin, in this case). The file myreq.pem is the file that contains the CSR information. This information must be submitted to the third-party CA so that the third-party CA can generate a digital certificate. Here is example command output when you issue this command with the use of the OpenSSL application:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
```

```
Loading 'screen' into random state - done
```

```
Generating a 1024 bit RSA private key
```

```
.....++++++
```

```
.....++++++
```

```
writing new private key to 'mykey.pem'
```

```
-----
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

```
-----
```

Country Name (2 letter code) [AU]:**US**

State or Province Name (full name) [Some-State]:**CA**

Locality Name (eg, city) []:**San Jose**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**ABC**

Organizational Unit Name (eg, section) []:**CDE**

Common Name (eg, YOUR name) []:**XYZ.ABC**

Email Address []:**Test@abc.com**

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:
OpenSSL>
```

**Note:** Remember the challenge password and preserve the key file. Most likely, you will need the password when you import the digitally signed certificate that the third-party CA sends (unless the third-party CA sends a new password along with the digital certificate that it generates for you or your organization).

4. Now that your CSR is ready, copy and paste the CSR information into any CA enrollment tool.

In order to copy and paste the information into the enrollment form, open the file in a text editor that does not add extra characters. Cisco recommends that you use Microsoft Notepad or UNIX vi. Refer to the website of the third-party CA for more information on how to submit the CSR through the enrollment tool.

After you submit the CSR to the third-party CA, the third-party CA digitally signs the certificate and sends back the signed certificate via e-mail.

5. Copy the signed certificate information that you receive back from the CA into a file.

This example names the file CA.pem.

6. Combine the CA.pem certificate with the private key, and then convert the file to a .pem file.

Issue this command in the OpenSSL application:

```
openssl>pkcs12 -export -in CA.pem -inkey mykey.pem -out CA.p12 -clcerts
-passin pass:check123 -passout pass:check123
```

*!--- This command should be on one line.*

```
openssl>pkcs12 -in CA.p12 -out final.pem -passin pass:check123 -passout pass:check123
```

**Note:** In this command, you must enter a password for the parameters **-passin** and **-passout**. The password that is configured for the **-passout** parameter must match the **certpassword** parameter that is configured on the WLC. In this example, the password that is configured for both the **-passin** and **-passout** parameters is **check123**. Step 4 of the procedure in the Download the Third-Party Certificate to the WLC section of this document discusses the configuration of the **certpassword** parameter.

The **final.pem** is the file that is transferred via TFTP to the Cisco WLC.

Now that you have the certificate from the third-party CA, you need to download the certificate to the WLC.

## Download the Third-Party Certificate to the WLC

Use a TFTP server in order to load the new certificate. Follow these guidelines for the use of TFTP:

- If you load the certificate through the service port, the TFTP server must be on the same subnet as the WLC because the service port is not routable. However, if you load the certificate through the distribution system (DS) network port, the TFTP server can be on any subnet.
- The TFTP server cannot run on the same computer as the Cisco Wireless Control System (WCS) because WCS and the TFTP server use the same communication port.

Complete these steps in order to load an externally generated HTTPS certificate:

1. Move the final.pem file to the default directory on your TFTP server.
2. In the command-line interface (CLI), issue the **transfer download start** command in order to view the current download settings, and enter **n** at the prompt.

Here is an example:

```
>transfer download start
Mode..... TFTP
Data Type..... Admin Cert
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename.....
Are you sure you want to start? (y/n) n
Transfer Canceled
```

3. Issue these commands in order to change the download settings:

```
>transfer download mode tftp
>transfer download datatype webauthcert
>transfer download serverip <TFTP server IP address>

>transfer download path <absolute TFTP server path to the update file>

>transfer download filename final.pem
```

4. Enter the password for the .pem file so that the operating system can decrypt the SSL key and certificate.

```
>transfer download certpassword password

>Setting password to password
```

**Note:** Be sure that the **certpassword** is the same as the **-passout** parameter password that step 6 of the Generate a CSR section discusses. In this example, the **certpassword** must be **check123**.

5. Issue the **transfer download start** command in order to view the updated settings. Then enter **y** at the prompt in order to confirm the current download settings and start the certificate and key download.

Here is an example:

```
(Cisco Controller) >transfer download start

Mode..... TFTP
Data Type..... Admin Cert
TFTP Server IP..... 172.16.1.1
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... c:\OpenSSL\bin/
TFTP Filename..... final.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP Webadmin cert transfer starting.

Certificate installed.
Reboot the switch to use new certificate.
```

**Note:** In order to install a third-party certificate for administrative (admin) authentication (for a user who tries to log in to the WLC with use of HTTPS), change the data type to **webadmincert** in the **transfer download datatype** command, and repeat steps 3 through 5 of this procedure.

6. Issue this command in order to enable HTTPS:

```
>config network secureweb enable
```

7. Save the SSL certificate, key, and secure web password to NVRAM so that your changes are retained across reboots.

```
>save config
```

```
Are you sure you want to save? (y/n) y
```

```
Configuration Saved!
```

8. Reboot the controller.

```
>reset system
```

```
Are you sure you would like to reset the system? (y/n) y
```

```
System will now restart!
```

```
The controller reboots.
```

**Note:** If a certificate is already installed, the procedure to download a new one erases the old one.

## Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

You can use the **show certificate summary** command on the WLC in order to check if the WLC uses the third-party certificate as expected. Here is an example:

```
(Cisco Controller) >show certificate summary
```

```
Web Administration Certificate..... 3rd Party
```

```
Web Authentication Certificate..... 3rd Party
```

```
Certificate compatibility mode:..... off
```

The output confirms that a third-party certificate is used as the web administration certificate and web authentication certificate.

The next time that a user tries to log in to the WLAN network with use of SSL-based web authentication, the user is not prompted to accept a web security alert, provided that the third-party certificate that is installed on the WLC is in the list of trusted CAs that the client browser supports.

## Troubleshoot

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

You can use the **debug pm pki enable** command on the WLC. Run the command when you install the certificate on the WLC.

Whenever any transfers to or from the controller occur, it is helpful to turn on the **debug transfer all enable** command and re-run the transfer in order to see the details of what has occurred. Transfers can fail in transit (the appropriate number of bits or bytes do not move from the server to the controller), or once the file gets there, the contents are either illegible to the controller or are not found to be appropriate for the function desired.

# Expired Intermediate VeriSign Certificate

The intermediate VeriSign certificate has expired, and, when you log into the web page for web authentication, it gives a date error. You see this error message:

## **The security certificate has expired or is not yet valid**

This means that something is wrong with the certificate, and it can be due to these reasons:

- If you run Java on your site, you can run into this known issue: [Java Error Messages](#) .
- If your certificate is from VeriSign, it is likely that you do not have the intermediate certificate and you simply need to chain it up.
- Check the Root Certificate Authority certificate on the client; ensure that it is a valid certificate and has not actually expired.

---

## Related Information

- [Wireless LAN Controller \(WLC\) Software Upgrade](#)
- [Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC](#)
- [Wireless LAN Controller \(WLC\) Troubleshoot FAQ](#)
- [Cisco Wireless LAN Controller Configuration Guide, Release 4.0](#)
- [Wireless Product Support](#)
- [OpenSSL Project](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 17, 2009

Document ID: 70584

---