

# Wireless Control System (WCS) Certificate Signing Request (CSR) Installed on a Linux Server Configuration Example

Document ID: 107600

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Background Information**

**CSR Generation Using a WCS**

Using the Certificate for secure login (HTTPS)

**Verify**

**Troubleshoot**

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

This document describes how to generate a Certificate Signing Request (CSR) for Wireless Control System (WCS) that runs on a Linux server.

## Prerequisites

### Requirements

Before you attempt this configuration, Cisco requires that you have knowledge on these topics:

- Linux command–line interface (CLI)
- Wireless Control System

### Components Used

The information in this document is based on WCS version 4.1.91.0.

**Note:** CSR generation that uses a WCS is supported with WCS versions 4.1.91.0 and above.

### Conventions

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

## Background Information

A CSR is submitted to a third–party CA in order to obtain a certificate, which they digitally sign. This certificate is used by WCS for login authentication. Before the CSR is created, the applicant first generates a Public/Private key pair.

CSR contains information that identifies the applicant (such as Domain Name, organization, location, etc.) and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR can be accompanied by other credentials or proofs as required by the certificate authority. For the most part, a third-party CA company, such as Entrust or VeriSign, requires a CSR before the company can create a digital certificate.

## CSR Generation Using a WCS

You can use the *keyadmin.sh* tool available in the WCS installation directory (*/opt/WCS4.1/bin/*) in order to generate CSRs on a WCS.

Complete these steps in order to access the tool:

1. Open the shell prompt.
2. Go to the */opt/WCS4.1/bin* directory, and execute the CSR generation command as shown below:

```
#!/opt/WCS4.1/bin
openssl req -new -newkey rsa:2048 -nodes -keyout /opt/mykey.pem -out
/opt/myreq.pem
```

This results in the generation of the CSR in the file *myreq.pem* in the */opt* directory, which is used to request the certificate from the CA. The Public/Private key pair is stored in the file *mykey.pem* in the */opt* directory.

## Using the Certificate for secure login (HTTPS)

Refer to the web site of the third-party CA for more information on how to submit the CSR through the enrollment tool. Once you submit the CSR to a third-party CA, they verify the details that you provided, they create and digitally sign the certificate, and then send the signed certificate back to you via email. This certificate is combined with the private key to be used for final authentication.

Complete these steps in order to create the final certificate:

1. Assume the certificate from CA has the file name *certificate.pem*. Use this command in order to combine the certificate with the private key:

```
openssl pkcs12 -export -in /opt/certificate.pem -inkey /opt/mykey.pem -out
/opt/certificate.p12 -clcerts -passin pass:<give_a_password> -passout
pass:<give_same_password>
```

2. Convert it to .cer format.

```
openssl pkcs12 -in /opt/certificate.p12 -out /opt/certificate.cer
-passin pass:<give_same_password> -passout pass:<give_same_password>
```

**Note:** This results in the creation of the final certificate *certificate.cer* located in the */opt* directory.

**Note:** By default, WCS has a built-in self-signed SSL certificate. This self-signed certificate is stored as *server.cer* in the */opt/WCS4.1/webnms/apache/conf/ssl* directory, which is used by WCS software when someone tries to securely log in to WCS through https. The self-signed certificate/key pair should be replaced by certificate (*certificate.cer*) and the private key (*mykey.pem*) that we created so that it can be used for login authentication.

3. Use this copy command in order to replace the self-signed certificate with the certificate we created.

```
cp /opt/mykey.pem /opt/WCSx.x.x.x/webnms/apache/conf/ssl.crt/server.key
cp /opt/certificate.cer /opt/WCSx.x.x.x/webnms/apache/conf/ssl.crt/server.cer
```

# Verify

In order to check if the certificate from the third-party is being used for authentication, complete these steps:

1. Stop and restart the WCS for the changes to take effect.
2. Access the WCS using the web browser.

If the signed certificate is valid and has a matching domain name, the application should not display the certificate pop-up warning and should take you directly to the login page.

**Note:** There is an alternate way to test the certificate. If the third-party from whom the certificate was obtained is not in the trusted list in the client, then the certificate will be treated as an invalid certificate and you will receive a warning dialog when you try to log in to WCS. On the warning screen, click **View Certificate**. On the screen that appears, click the **Details** tab. Click the Issuer field, and check the attributes OU (Organizational Unit) and O (Organization). The default self-signed certificate will have the OU as WNBU and O as Cisco Systems. Check if these attributes correspond to the third-party that issued the certificate.

# Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

# NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Wireless
Wireless – Mobility: WLAN Radio Standards
Wireless – Mobility: Security and Network Management
Wireless – Mobility: Getting Started with Wireless
Wireless – Mobility: General

# Related Information

- [Installing WCS for Linux](#)
- [Cisco Wireless Control System Configuration Guide, Release 5.1](#)
- [Certificate Signing Request \(CSR\) Generation for a Third-Party Certificate on a Wireless Control System \(WCS\)](#)
- [Certificate Signing Request \(CSR\) Generation for a Third-Party Certificate on a WLAN Controller \(WLC\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

