Generate CSR for Third−Party Certificates and Download Chained Certificates to the WLC

Document ID: 109597

Contents

Introduction

This document describes how to generate a Certificate Signing Request (CSR) in order to obtain a third−party certificate and how to download a chained 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
- Knowledge of public key infrastructure and digital certificates

Components Used

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

- Cisco 4400 WLC that runs firmware version 5.1.151.0
- 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 the Cisco Technical Tips Conventions for more information on document conventions.

Chained Certificates

A certificate chain is a sequence of certificates, where each certificate in the chain is signed by the subsequent certificate. The purpose of certificate chain is to establish a chain of trust from a peer certificate to a trusted Certification Authority (CA) certificate. The CA vouches for the identity in the peer certificate by signing it. If the CA is one that you trust, which is indicated by the presence of a copy of the CA certificate in your root certificate directory, this implies you can trust the signed peer certificate as well.

Often, the clients do not accept the certificates because they were not created by a known CA. The client typically states that the validity of the certificate cannot be verified. This is the case when the certificate is signed by an intermediate CA, which is not known to the client browser. In such cases, it is necessary to use a chained SSL certificate or certificate group.

Support for Chained Certificate

In controller versions earlier than 5.1.151.0, web authentication certificates can be only device certificates and should not contain the CA roots chained to the device certificate (no chained certificates).

With controller version 5.1.151.0 and later, the controller allows for the device certificate to be downloaded as a chained certificate for web authentication.

Certificate Levels

- Level 0 Use of only a server certificate on WLC.
- Level 1 Use of server certificate on WLC and a CA root certificate.
- Level 2 Use of server certificate on WLC, one single CA intermediate certificate, and a CA root certificate.
- Level 3 Use of server certificate on WLC, two CA intermediate certificates, and a CA root certificate.

WLC does not support chained certificates more than 10KB size on the WLC. However, this restriction has been removed in WLC 7.0.230.0 and later releases.

Note: Chained certificates are supported for web authentication only; they are not supported for the management certificate.

Web authentication certificates can be any of these:

- Chained
- Unchained
- Auto generated

For WLCs with software versions earlier than 5.1.151.0, the workaround is to use one of these options:

- 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.

For information on how to use unchained certificates on the WLC, refer to Generate CSR for Third−Party Certificates and Download Unchained Certificates to the WLC.

This document discusses how to properly install a chained Secure Socket Layer (SSL) certificate to a WLC.

Generate a CSR

Complete these steps in order to generate a CSR:

1. Install and open the OpenSSL application. In Windows, by default, openssl.exe is located at **C:\ > openssl > bin**.

   Note: OpenSSL 0.9.8 is required as the WLC does not currently support OpenSSL 1.0.
2. Issue this command:

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

   Note: WLCs support a maximum key size of 2048 bits.

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

   Note: It is important that you provide the correct 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 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.

   Here is an example:

   ```
   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>
   ```

   After you provide all the required details, two files are generated:

   - a new private key that includes the name *mykey.pem*
   - a CSR that includes the name *myreq.pem*

4. Copy and paste the CSR information into any CA 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 chain through e−mail. In case of chained certificates, you receive the entire chain of certificates from the CA. If you only have one intermediate certificate in our example, you receive these three certificates from the CA:

   - Root certificate.pem
   - Intermediate certificate.pem
   - Device certificate.pem

   Note: Make sure that the certificate is Apache compatible with SHA1 encryption.
5. Once you have all the three certificates, copy and paste into another file the contents of each .pem file in this order:

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

6. Save the file as *All−certs.pem*.
7. Combine the All−certs.pem certificate with the private key that you generated along with the CSR (the private key of the device certificate, which is mykey.pem in this example), and save the file as *final.pem*.

   Issue these commands in the OpenSSL application in order to create the All−certs.pem and final.pem files:

```
openssl>pkcs12 −export −in All−certs.pem −inkey mykey.pem
       −out All−certs.p12 −clcerts −passin pass:check123
       −passout pass:check123

openssl>pkcs12 −in All−certs.p12 −out final−cert.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*.

   final.pem is the file that we need to download to the Wireless LAN Controller. The next step is to download this file to the WLC.

Download the Third−Party Certificate to the WLC using the CLI

Complete these steps in order to download the chained certificate to the WLC using the CLI:

1. Move the *final.pem* file to the default directory on your TFTP server.
2. In the CLI, 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
```

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

```
>transfer download certpassword password
```

Note: Be sure that the value for *certpassword* is the same as the *−passout* parameter password that was set in step 4 of the Generate a CSR section. In this example, the *certpassword* must be *check123*.

4. 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:

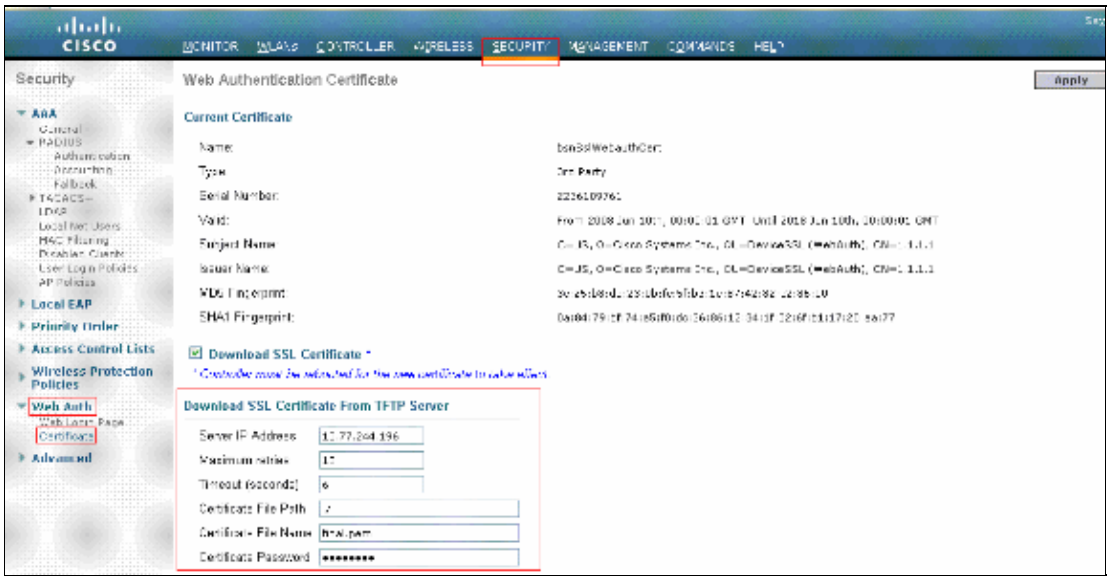
```
(Cisco Controller) >transfer download start

Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 10.77.244.196
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path......................................./
TFTP Filename............................ final.pem

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

TFTP EAP Dev cert transfer starting.

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

5. Reboot the WLC in order for the changes to take effect.

Download the Third−Party Certificate to the WLC using the GUI

Complete these steps in order to download the chained certificate to the WLC using the GUI:

1. Copy the device certificate final.pem to the default directory on your TFTP server.
2. Choose **Security > Web Auth > Cert** in order to open the Web Authentication Certificate page.
3. Check the **Download SSL Certificate** check box in order to view the Download SSL Certificate From TFTP Server parameters.
4. In the IP Address field, enter the IP address of the TFTP server.



5. In the File Path field, enter the directory path of the certificate.

6. In the File Name field, enter the name of the certificate.
7. In the Certificate Password field, enter the password that was used to protect the certificate.
8. Click **Apply**.
9. After the download is complete, choose **Commands > Reboot > Reboot**.
10. If prompted to save your changes, click **Save and Reboot**.
11. Click **OK** in order to confirm your decision to reboot the controller.

Related Information

- **Generate CSR for Third−Party Certificates and Download Unchained Certificates to the WLC**
- **Certificate Signing Request (CSR) Generation for a Third−Party Certificate on a Wireless Control System (WCS)**
- **Wireless Control System (WCS) Certificate Signing Request (CSR) Installed on a Linux Server Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 28, 2010 Document ID: 109597