

How to Install a Chained SSL Certificate to the CSS SSL Module

Document ID: 45462

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Step-by-Step Instructions

Related Information

Introduction

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

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- CSS11506 SSL Module (Strong Encryption) – CSS 506–SSL–K9
- CSS11501 SSL Module (Strong Encryption) – CSS 501–SSL–K9
- CSS11506 Only Switch Module – CSS 506–SM
- WebNS 7.10 and 7.20

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

For more information on document conventions, see the Cisco Technical Tips Conventions.

Step-by-Step Instructions

This section shows how to install a chained certificate on the CSS SSL module with the CSS 11500.

If the chained certificate is in multiple files, use the procedure outlined below.

1. Convert all certificates to the same format. If the certificates are separate and not in Privacy Enhanced Mail (PEM) format, you need to convert them to PEM format and then concatenate.
2. Concatenate all the certificates into one file; ensure that they are concatenated as they appear in the chain. Server certificate should be the first one in the chain, followed by the intermediates (server certificates and intermediate CA certificates).
3. Import the concatenated certificate file into the CSS.
4. Associate the certificate to the `ssl-server`.
5. Apply the CA of the `ssl-server` within the `ssl-proxy-list`.

If all these certificates are chained into one PKCS#12 file (as many of the PKCS#12 certificates are), you should import the chained certificate as a PKCS#12, and associate/apply it as normal. PKCS#12 are not capable of being concatenated.

Note: Distinguished Encoding Rule (DER) formats do not support chains, so this should not be an issue.

To verify, the key that needs to be used is the key that generated the Certificate Signing Request (CSR) file to create the server certificate. There is only one key for a certificate, be it chained or regular. Make sure to verify the certificate and key after they are imported. You can issue the command shown below.

```
(config)# ssl verify myrsacert1 myrsakey1  
Certificate and key match
```

Related Information

- [CSS Advanced Configuration Guide](#)
- [Secure/Commerce Site Pro Server ID Installation – Intel NetStructure 7110 e-Commerce Accelerator](#)
- [Application Networking Services Product Support](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 04, 2004

Document ID: 45462
