Understand Umbrella Proxy Certificate Expiration

Contents

Introduction

This document describes why the expiration of certificates from the Cisco Umbrella proxy is within days of the present date.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella Secure Internet Gateway (SIG).

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, ensure that you understand the potential impact of any command.

Overview

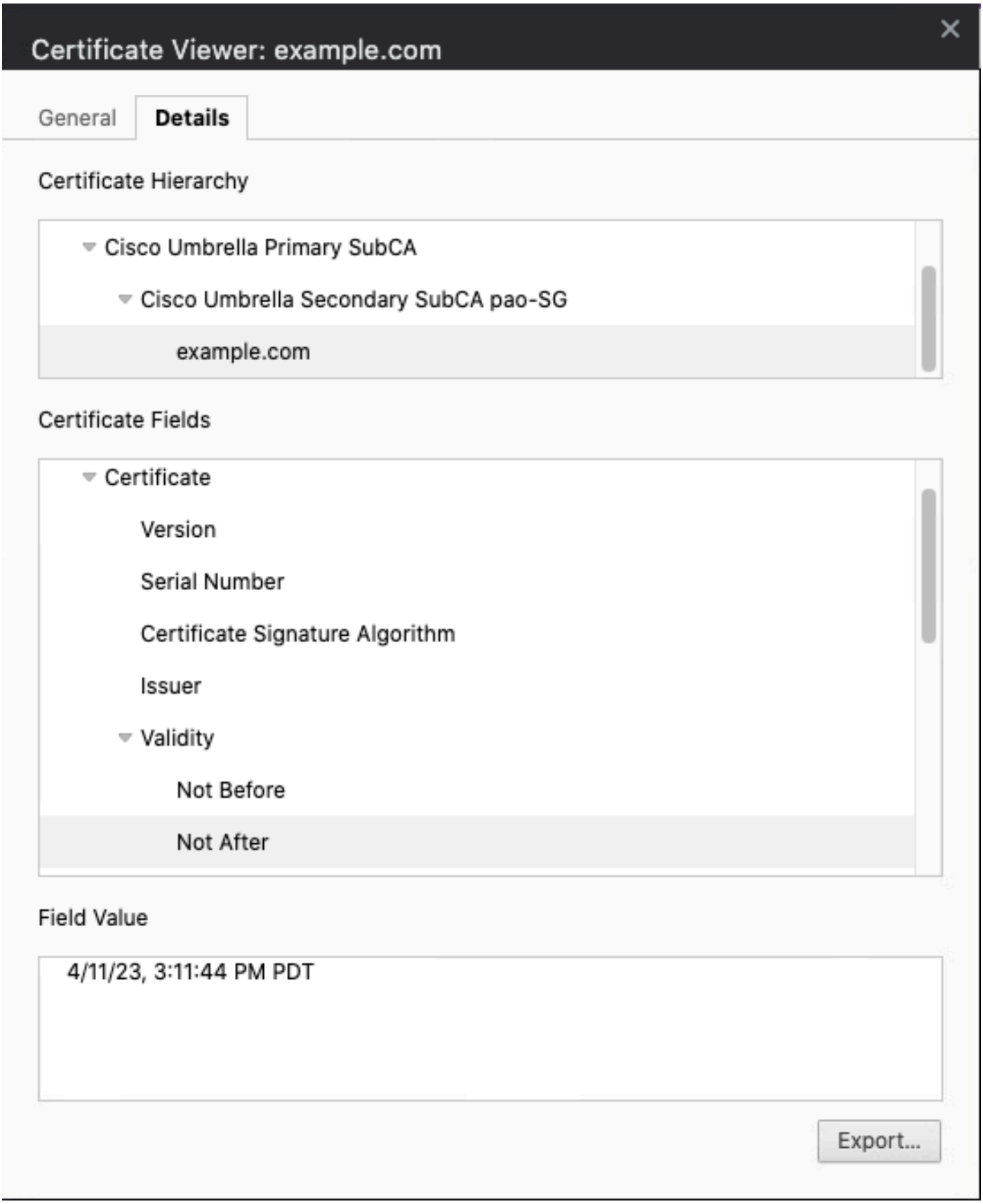
When a Cisco Umbrella web proxy is configured for decryption of HTTPS communication, the expiration date and time of the certificates received from the proxy can typically be within ten days of the present date and time. This is a security feature and requires no end-user action. Renewal is automatic.

Certificate Lifetimes with Proxy Decryption

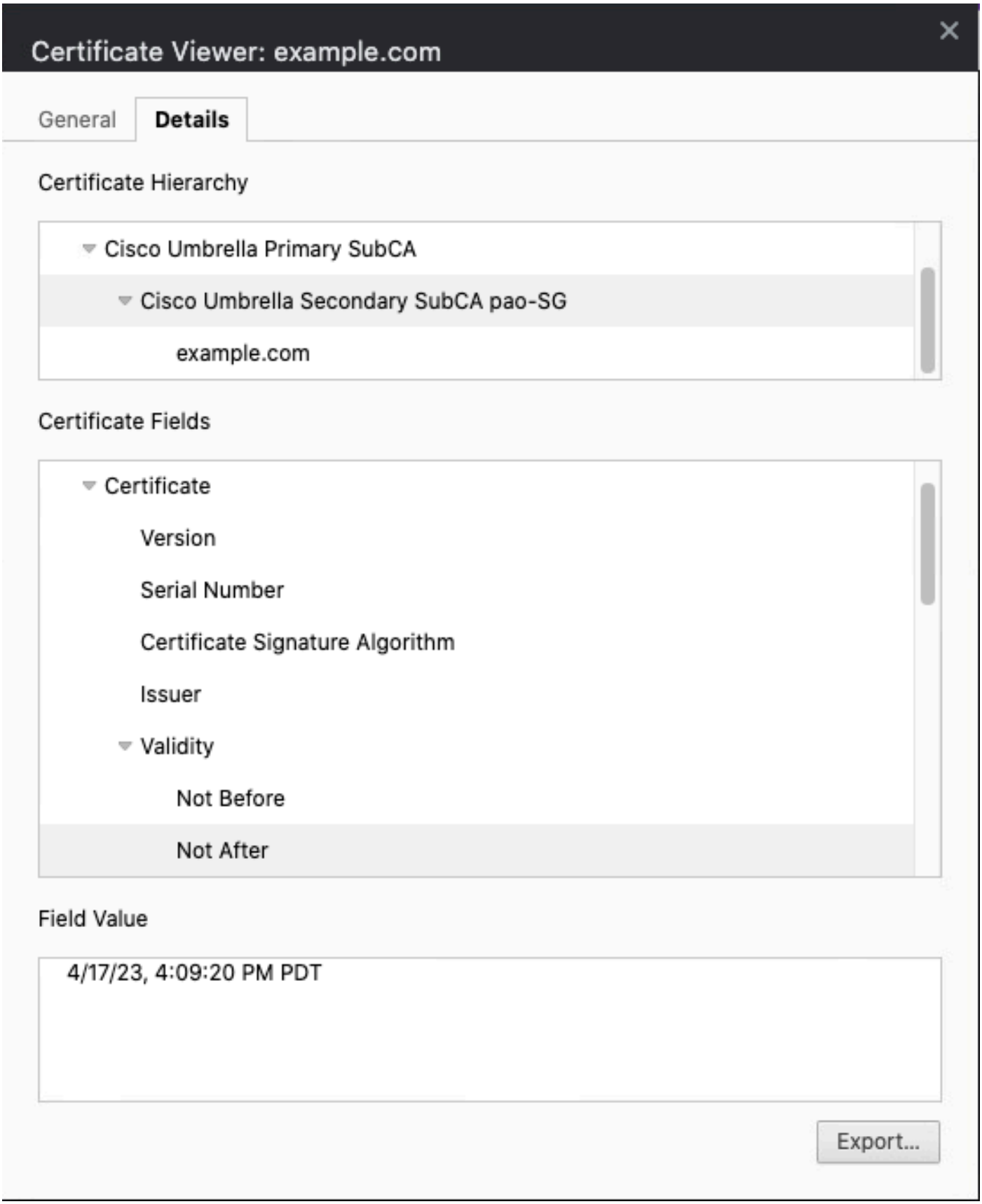
When web clients send HTTPS communication (HTTP requests encrypted with TLS) through the Umbrella Secure Web Gateway (SWG) proxy or the Intelligent Proxy (IP), and the proxy is configured to decrypt HTTPS communication, the proxy re-writes the leaf certificate belonging to the server, and replaces any intermediate certificates also sent by the server with Cisco intermediate certificates. This certificate chain replacement is the standard technique by which web proxies perform decryption of requests and responses that are encrypted in TLS.

The new leaf and intermediate certificates are created dynamically. When viewing the **Not Before** and **Not After** dates in the certificates, typically the certificates can be issued with short lifetimes of not more than ten days, as an enhanced security measure. Renewal is automatic, requiring no end-user action.

For example, in these images retrieved on April 8, 2023, the leaf certificate from example.com has a Validity **Not After** date of April 11, 2023 (3 days of validity remaining).



Similarly, the first intermediate certificate in the chain, the **Cisco Umbrella Secondary SubCA** certificate, has a Validity **Not After** (expiration) date of April 17, 2023.



The **Not Before** and **Not After** dates of certificates in the chain are typically not identical, as creation times vary depending on the retrieval of each certificate across all users of the proxy instance.

Short-lived certificate issuance does not apply to either of:

- The **Cisco Umbrella Root CA** root certificate (seen when using the default configuration)
- The **Cisco Umbrella Customers CA** intermediate certificate (seen when using Customer CA Signed Certificates)

In either configuration, the aforementioned certificates can have longer validity periods.