ESA での証明書署名要求の作成

目次

[概要](#)
[ESA の CSR を作成して下さい](#)
[GUI のコンフィギュレーションのステップ](#)
[関連情報](#)

概要

この資料に E メール セキュリティ アプライアンス（ESA）の証明書署名要求（CSR）を作成する方法を記述されています。

ESA の CSR を作成して下さい

AsyncOS 7.1.1 現在で、ESA はあなた自身の使用のための自己署名証明書を作成し、認証局に入り、公共認証を得るために CSR を生成できます。 認証局はプライベートキーによって署名する信頼された公共認証を戻します。 自己署名証明書を作成し、CSR を生成し、信頼された公共認証をインストールするために GUI で**ネットワーク > 認証** ページか CLI で **certconfig** コマンドを使用して下さい。

認証をはじめて得るか、または作成する場合、推奨が組織の必要を満たすことインターネットを「認証局 サービス SSL サーバ証明」を捜し、サービスを選択して下さい。 認証を得るためにサービスの手順に従って下さい。

GUI のコンフィギュレーションのステップ

1. 自己署名証明書を作成するために、GUI のネットワーク > 認証 ページの**認証** 『Add』 をクリック して下さい（または CLI の **certconfig** コマンドを）。 Certificate ページ追加で**自己署名証明書を**『Create』 を選択 して下さい。
2. 自己署名証明書のためのこの情報を入力して下さい: Common Name -完全修飾ドメイン ネーム。組織-組織の正確で可能な名前。組織ユニット-組織のセクション。都市（局所性）-組織が合法的に見つけられる都市。状態（地域）-組織が合法的に見つけられる状態、郡、または領域。国-組織が合法的に見つけられる国の 2 文字国際標準化機構 （ISO）省略形。有効期限の前の期間-認証の前の日数は切れます。プライベートキー サイズ- CSR のために生成するべきプライベートキーのサイズ。 2048 ビットおよび 1024 ビットだけサポートされます。
3. 認証およびシグニチャ 情報を表示するために『Next』 をクリック して下さい。
4. 認証の名前を入力して下さい。 AsyncOS は Common Name をデフォルトで割り当てます。

5. 認証局に自己署名証明書のために CSR を入れたいと思う場合ローカルかネットワーク マシンにプライバシー強化メール（PEM）形式の CSR を保存するために**証明書署名要求を**『Download』 をクリック して下さい。
6. 認証を保存し、変更を保存するために『SUBMIT』 をクリック して下さい。 変更を行なわれていない残す場合、プライベートキーは失われて得、署名入り認証はインストールすることができません。

認証局がプライベートキーによって署名する信頼された公共認証を戻すとき認証 ページの認証の名前をクリックし、ローカルマシンまたはネットワークのファイルに認証をアップロードするためにパスを入力して下さい。 受け取る信頼された公共認証がアプライアンスにアップロードされる前に PEM に変換できる PEM 形式か形式にあることを確かめて下さい。 これを完了するツールは OpenSSL と、http://www.openssl.org で利用可能 な フリーソフト含まれています。

認証局からの認証をアップロードする場合、既存 の 認証は上書きされます。 また自己署名証明書に関する中間認証をアップロードできます。 宛先 ドメインへの公共か私用リスナー、IP インターフェイスの HTTPS サービス、Lightweight Directory Access Protocol（LDAP）インターフェイス、またはすべての発信 Transport Layer Security（TLS）接続と認証を使用できます。

関連情報

- ESA での TLS 向けの包括的な設定ガイド
- テクニカルサポートとドキュメント - Cisco Systems