Installationsvoraussetzungen für ESA-Zertifikate

Inhalt

Einführung

Dieses Dokument beschreibt die Anforderungen für die Zertifikatinstallation der Cisco E-Mail Security Appliance (ESA) und die Services, für die Zertifikate verwendet werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- AsyncOS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ESA, auf der eine beliebige Version von AsyncOS ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Installationsvoraussetzungen für ESA-Zertifikate

Sie müssen diese Artikel im Privacy Enhanced Mail (PEM)-Format zur Verfügung stellen, um ein Zertifikat auf der ESA zu installieren:

- Das X.509-Zertifikat
- Der private Schlüssel, der dem Zertifikat entspricht
- Alle Zwischenzertifikate, die von Ihrer Zertifizierungsstelle (Certificate Authority, CA) bereitgestellt werden.

ESA-Services, die Zertifikate erfordern

Zertifikate können für die folgenden vier Dienste verwendet werden:

- Inbound Transport Layer Security (TLS)
- Outbound-TLS
- HTTPS
- Lightweight Directory Access Protocol (LDAPS)

> **Tipp**: Sie können dasselbe Zertifikat für alle vier Services verwenden oder für jeden einzelnen separate Zertifikate verwenden.