SSL-Einrichtung über das Server Setup

[Stand: 23.05.2019 | Programmversion: 12.00.000]

Diese Anleitung erklärt, wie HTTP-Verbindungen über das ELO Server Setup mittels X.509-Zertifikaten verschlüsselt werden können.

Inhalt

1 SSL-Einrichtung über das Server Setup 2
1.1 X.509-Zertifikate 2
1.1.1 Server-Zertifikat 2
1.1.2 Privater Schlüssel 2
1.1.3 Root-Zertifikat 3
1.1.4 Zertifikatskette 3
1.2 Einstellungen im ELO Server Setup 3
1.2.1 Hochladen der Zertifikate bei ELOprofessional 3
1.2.2 Hochladen der Zertifikate bei ELOenterprise 4
1.2.3 Laden der Zertifikate 4
1.2.4 Aktivieren von SSL im Application Server 5
1.3 Funktionsprüfung 5
1.4 Einstellung im Client 6
1.4.1 ELO Java Client 6
1.4.2 ELO Web Client 6

1 SSL-Einrichtung über das Server Setup

Im ersten Abschnitt wird beschrieben, wie Sie die für die HTTPS-Kommunikation notwendigen Zertifikate generieren. Darauffolgend wird erläutert, welche Einstellungen Sie im ELO Server Setup für das Aktivieren des HTTPS-Protokolls treffen müssen. Der nächste Abschnitt schildert, wie Sie überprüfen können, ob die Verschlüsselung funktioniert. Abschließend werden die notwendigen Einstellungen in den Clients dargelegt.

1.1 X.509-Zertifikate

Zum erfolgreichen Einrichten verschlüsselter HTTP-Kommunikation zwischen ELO Java Client und ELO Indexserver sowie der ELO Serverkomponenten untereinander sind X.509-Zertifikate notwendig. Diese können von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellt oder selbst generiert sein.

Mindestens benötigt wird:

- Server-Zertifikat
- Privater Schlüssel des Server-Zertifikats
- Root-Zertifikat, mit welchem das Server-Zertifikat unterschrieben wurde

Im Folgenden wird auf die Ansprüche der jeweiligen Anforderungen detaillierter eingegangen.

1.1.1 Server-Zertifikat

Das Server-Zertifikat muss DER- oder PEM-kodiert vorliegen, diese haben üblicherweise die Dateiendungen „crt“ oder „cer“ respektive „pem“. Zertifikate, die in einer anderen Kodierung oder einem Zertifikatsspeicher hinterlegt sind (z. B. PKCS #12 oder Java Keystore), können nicht verarbeitet werden.

Das Zertifikat muss die Erweiterung „Subject Alternative Name“ sowie darin enthalten mindestens einen „DNS Name“ besitzen, dessen Wert exakt dem Rechnernamen entspricht, auf welchem ELO innerhalb des Netzwerkes erreichbar sein soll. Das Zertifikat kann auch weitere „DNS Name“-Einträge mit anderen Namen enthalten, die nicht dem Rechnernamen entsprechen.

1.1.2 Privater Schlüssel

Für den privaten Schlüssel des Server-Zertifikats gelten dieselben Voraussetzungen wie für das Zertifikat selbst auch – er muss DER- oder PEM-kodiert vorliegen, ein Zertifikatsspeicher kann nicht verarbeitet werden. Die Dateinamenserweiterung für private Schlüssel ist gewöhnlich „key“.

1.1.3 Root-Zertifikat

Das Root-Zertifikat wird verwendet, um das Server-Zertifikat zu unterschreiben. Falls das verwendete Root-Zertifikat selbstgeneriert sein sollte, so gelten bereits beschriebene Voraussetzungen für die Kodierung des Zertifikats - DER oder PEM.

Zertifizierungsstellen bieten ihre Root-Zertifikate in der Regel öffentlich zum Download an.

1.1.4 Zertifikatskette

Als Zertifikatskette bezeichnet man die rekursive Verbindung eines Zertifikats zu seinem unterzeichnenden Zertifikat bis hin zum Root-Zertifikat. Es gibt zwei Situationen, in denen diese aus mehr als dem Root-Zertifikat und dem Server-Zertifikat besteht.

Zum einen benutzen manche Zertifizierungsstellen Zwischenzertifikate zum Unterschreiben von Zertifikaten dritter. Diese Zwischenzertifikate sind dann mit dem eigenen Root-Zertifikat unterschrieben.

Zum anderen besteht die Möglichkeit, selbst ein „Signing-Certificate“ zu erwerben, mit welchem man sich selbst Zertifikate unterschreiben kann.

In beiden Fällen ist es notwendig, neben dem Server- und dem Root-Zertifikat auch alle Zwischenzertifikate vorzuhalten, die notwendig sind, um die Gültigkeit des Server-Zertifikats bis hin zum Root-Zertifikat sicherstellen zu können.

1.2 Einstellungen im ELO Server Setup

Das Aktivieren des HTTPS-Protokolls findet über das ELO Server Setup in zwei Schritten statt. Zunächst werden die Zertifikatskette sowie der private Schlüssel des Server-Zertifikats ins Setup geladen. Im Anschluss wird für jeden Application Server, zu welchem verschlüsselte HTTP-Verbindungen aufgebaut werden sollen, SSL aktiviert.

Während das Aktivieren von SSL identisch ist, unterscheidet sich ELOprofessional und ELOenterprise beim Hochladen der Zertifikate.

1.2.1 Hochladen der Zertifikate bei ELOprofessional

Bei ELOprofessional finden Sie die Schaltflächen zu Hochladen der Zertifikate auf der Seite „Repositories“:

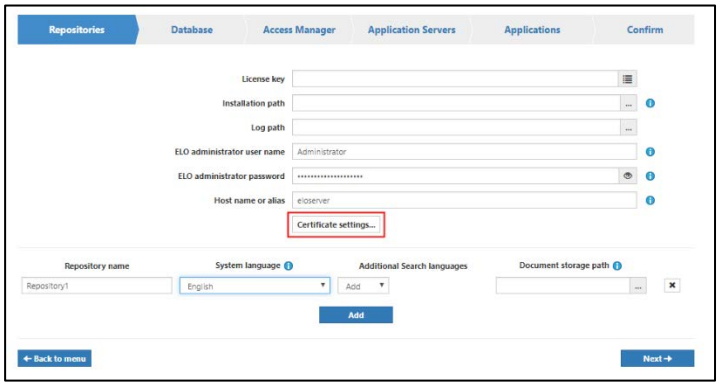


Abb. 1: ELO 10 Server Setup, ELOprofessional, Schaltfläche 'Certificate settings'

1.2.2 Hochladen der Zertifikate bei ELOenterprise

Bei ELOenterprise finden Sie die Schaltflächen zum Hochladen der Zertifikate auf der Seite „Servers“:

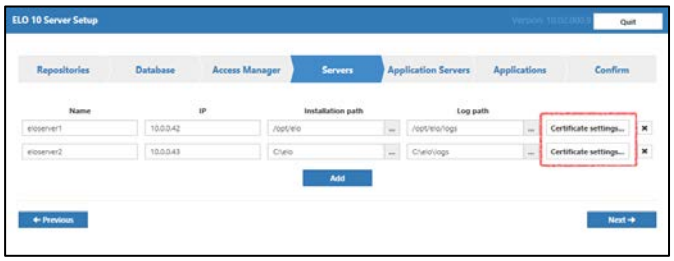


Abb. 2: ELO 10 Server Setup, ELOenterprise, Schaltfläche 'Certificate settings'

Die Zertifikate müssen für jeden Server, auf dem der eingehende HTTP-Verkehr verschlüsselt werden soll, hochgeladen werden. Dies gilt auch dann, wenn jeweils dasselbe Zertifikat Verwendung finden soll.

1.2.3 Laden der Zertifikate

Der Dialog zum Laden der Zertifikate erfordert mehrere Schritte:

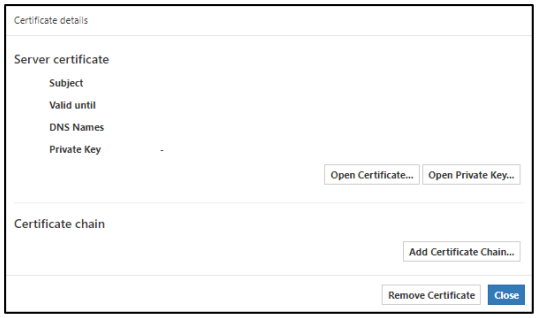


Abb. 3: Dialog 'Certificate details' im ELO 10 Server Setup

Open Certificate…: Es erscheint ein Dateiauswahldialog für das Server-Zertifikat. Nach Öffnen der korrekten Datei wird das Zertifikat in das Setup geladen und eingelesen. Im Erfolgsfall werden im Anschluss die Einträge „Subject“, „Valid until“ und „DNS Names“ mit den entsprechenden Werten aus dem Zertifikat gefüllt.

Open Private Key…: Es erscheint ein Dateiauswahldialog für den privaten Schlüssel des Server-Zertifikats. Nach Öffnen der korrekten Datei wird der private Schlüssel in das Setup geladen und eingelesen. Im Erfolgsfall zeigt das Setup im Anschluss bei „Private Key“ den Wert „Ok“ an.

Add Certificate Chain…: Die Funktionsweise ist analog zu den bisherigen Dialogen. Über diese Schaltfläche muss jedes Zertifikat der Zertifikatskette bis hin zum Root-Zertifikat ins Setup geladen werden.

1.2.4 Aktivieren von SSL im Application Server

Sie können bestimmen, zu welchem Application Server eine verschlüsselte Verbindung aufgebaut werden soll. Setzen Sie hierfür für den jeweiligen Server auf der Seite „Application Servers“ in der Spalte „Use SSL“ den Schalter auf „On“.

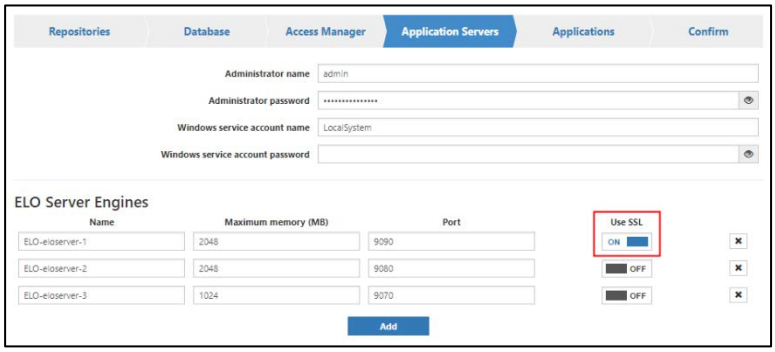


Abb. 4: ELO 10 Server Setup, Schalter 'Use SSL'

Diese Einstellung finden Sie ausschließlich in der Rubrik „ELO Server Engines“. Bei „ELO iSearch“ wird seit der Version 10.2 die Kommunikation zwischen ELO iSearch-Knoten und ELO Indexserver automatisch verschlüsselt. Die hierzu notwendigen Zertifikate werden durch das Setup während der Installation automatisch generiert.

1.3 Funktionsprüfung

Der HTTPS-Port ermittelt sich aus dem konfigurierten HTTP-Port+3. Ob die Verschlüsselung funktioniert, kann damit im Browser durch Aufrufen zum Beispiel der ELO Indexserver-Statusseite getestet werden. Exemplarisch wäre die URL dann etwa: https://eloserver:9093/ix-Repository1/. Wird die Statusseite angezeigt, ist der Test erfolgreich.

1.4 Einstellung im Client

1.4.1 ELO Java Client

Im ELO Java Client ist die URL für das Profil der Archive so zu ändern, dass sie auf den verschlüsselten Endpunkt des ELO Indexservers verweist: https://<Server>:9093/ix-<Archiv>/ix.

Wird ein selbstsigniertes Root-Zertifikat verwendet, muss dieses noch in den Truststore von Java importiert werden.

```
<java>\bin\keytool -import -alias <alias> -keystore
<java>\jre\lib\security\cacerts -file certificate.pem
```

1.4.2 ELO Web Client

Die Einstellung für den ELO Web Client wird vom ELO Server Setup automatisch konfiguriert, sie ist erreichbar unter https://<Server>:9093/web-<Archiv>/.