Installation Scout Enterprise Management Suite 15

Kurzanleitung

Stand: 2023-07-21

0. Rechtliche Hinweise

Unicon GmbH
Ludwig-Erhard-Allee 26
76131 Karlsruhe
+49 (0)721 96451-0

1. Darstellung

Die folgenden Textdarstellungen und Konventionen werden in diesem Handbuch verwendet:

Darstellung	Beschreibung
Programmelemente	Alle Bedienelemente der Benutzeroberfläche werden **fett** dargestellt.
Menü > Menübefehl	Wenn Menübefehle, Dialoge oder Register nacheinander aufgerufen werden müssen, werden die einzelnen Bedienelemente durch **>** getrennt.
`Wert`	Daten, die eingegeben werden müssen oder den Wert eines Feldes bezeichnen, werden in `Courier New` dargestellt. Dateinamen und Pfadnamen werden ebenfalls in `Courier New` dargestellt.
STRG	Tasten, die Sie drücken müssen, werden in KAPITÄLCHEN dargestellt.
Platzhalter	Platzhalter in Anweisungen und Benutzereingaben werden *kursiv* dargestellt.
1.Handlungsaufforderung	Handlungsaufforderungen werden fortlaufend nummeriert.
Ergebnis	Zwischen- und Endergebnisse einer Handlung werden *kursiv* dargestellt.

Abkürzungen

Abkürzung	Bedeutung
AD	Active Directory, Verzeichnisdienst von Microsoft Windows Server
EBKGUI	Oberfläche des eLux Builder Kit (Tool zum Erstellen von eLux Software-Paketen)
EPM	eLux package module (`.epm`, Software-Paket)
FPM	Feature package module (`.fpm`, Teil eines Software-Paketes)
FQDN	Fully qualified domain name
GB	Gigabyte
GHz	GigaHertz (Prozessorgeschwindigkeit)
HDD	Hard disk drive (Flash-Speicher)
IDF	Image Definition File (`.idf`)
IIS	Microsoft Internet Information Services
MB	Megabyte

Abkürzung	Bedeutung
OU	Organizational unit Organisationseinheit oder Gruppe innerhalb der Organisationsstruktur
VPN	Virtual Private Network

2. Systemvoraussetzungen

Hinweis
Die folgenden Informationen beziehen sich auf die Installation der Scout Enterprise Management Suite 15.x.

Mindestanforderungen für Scout Server und Scout Console

- Festplattenspeicher 600 MB (nur Scout Enterprise Management Suite, ohne Software-Container)
- Scout Server und Scout Console: Microsoft Windows Server 2016, 2019 oder 2022
- Scout Console: Microsoft Windows 10 und 11

jeweils mit den von Microsoft zum Zeitpunkt der Installation zur Verfügung gestellten Software-Aktualisierungen

Hinweis
Wir empfehlen, die Scout Enterprise Management Suite auf einem Windows Server-System zu betreiben. Zum Ausführen der Scout Console ist eine Windows Workstation ausreichend.

- Microsoft .NET Framework Version 3.5 und
  Microsoft .NET Framework Version 4.5.1 oder höher
- Passender ODBC Treiber

Anforderungen an das Datenbanksystem

- Microsoft SQL Server 2016, 2017, 2019, 2022
- oder für kleinere Installationen:

  MS SQL Server Express LocalDB als integriertes Datenbank-Managementsystem basierend auf SQL, in der Scout-Installationsdatei enthalten

Mindestanforderungen für den eLux-Container

- nur bei Verwendung des klassischen ELIAS, Benutzer-definierte Installation -

- FTP- oder HTTP-Server, lokal installiert oder über Netzlaufwerk
- Der Platzbedarf ist abhängig von der Anzahl der vorgehaltenen Betriebssystem-Versionen. Für die Installation des aktuellen eLuxContainer empfehlen wir beispielsweise mindestens 2,5 GB freien Speicherplatz.

  Der Mindestbedarf kann aus der Größe abgeleitet werden, die für das `AllPackages`-Archiv auf unserem Portal myelux.com angegeben ist.

Empfohlene Systemanforderungen für ELIAS 18 und MongoDB auf einem Computer

- bei Verwendung von ELIAS 18, gesonderte Installation -

- Festplattenspeicher 30 GB (je nach Container-Installationen)
- 8 GB RAM oder mehr
- Microsoft Windows Server 2016 oder höher, 64-Bit-Version
  Microsoft Internet Information Service (IIS) Version 8.0 oder höher
  inklusive WebSocket Protocol für automatisches Neuladen der Seite

Mindestanforderungen für ELIAS 18 und MongoDB

- Festplattenspeicher 10 GB
- RAM 6 GB
- Microsoft Windows 10, 64-Bit-Version

Hinweis
Wenn Sie eine eigene MongoDB-Installation für ELIAS 18 verwenden, setzen Sie MongoDB in einer aktuellen und unterstützten Version ein.

Mindestanforderungen für die Web-Anwendungen Scout Board, ELIAS 18 und Scout Cloud Gateway[1]

- Webbrowser / Mindestversion
  - Mozilla Firefox ⇒ Version 96 ESR
  - Google Chrome ⇒ Version 96
  - Microsoft Edge ⇒ Version 96

[1] siehe auch Systemvoraussetzungen für Scout Cloud Gateway im SCG-Handbuch

Hinweis
Manche Funktionen verwenden Pop-up-Fenster. Stellen Sie sicher, dass Pop-up-Fenster nicht vom Browser blockiert werden. Diese Funktion finden Sie in den Browser-Einstellungen meistens unter **Datenschutz** oder **Sicherheit**.

- Bildschirmauflösung Full HD

Support-Fristen und Kompatibilitäts-Matrix finden Sie im Whitepaper **Releases, Lebenszyklen und Kompatibilität**.

3. Systembeschränkungen

Systembeschränkungen sind für keine Komponente der Scout Enterprise Management Suite bekannt.

Andere Dienste wie z.B. Citrix XenApp können auf demselben PC laufen.

4. Datenbankunterstützung

Scout erfordert eine Datenbanksoftware, entweder Microsoft SQL Server oder für kleinere Umgebungen Microsoft SQL Server Express LocalDB.

4.1. Überblick

Microsoft SQL Server

Zur Nutzung von SQL-Datenbanken kann Microsoft SQL Server in einer Version mit verfügbarem Produktsupport eingesetzt werden. Wir empfehlen, die erforderlichen Datenbanken vor der Installation der Scout Enterprise Management Suite in SQL Server anzulegen.

Erforderlich ist mindestens eine **Scout-Datenbank** zur Verwaltung folgender Daten:

- Geräte-Konfigurationen
- Anwendungsdefinitionen
- Geräte-Bestandsdaten (statisch)
- Server-Einstellungen
- Administratorenverwaltung
- Konsolenverwaltung
- Lizenzinformationen
- Transaktionsprotokollierung

Eine Scout-Datenbank erfordert ungefähr 50 MB Speicherplatzbedarf pro 1.000 Geräte.

Für Scout-Versionen bis Scout 15 2204 war der Scout Statistikservice als optionale Komponente im "Funktionsumfang der Scout Enterprise Management Suite" auf Seite 32 enthalten, der zusätzlich eine Statistik-Datenbank erforderte. Ab Scout 15 2209 wurde der Scout Statistikservice durch den Scout Keep Alive-Service ersetzt. Die Keep Alive-Informationen werden in der Scout-Datenbank gespeichert.

Wenn die erforderlichen SQL Server-Berechtigungen vorhanden sind, können auch während der Installation der Scout Enterprise Management Suite in Microsoft SQL Server neue Datenbanken automatisiert erstellt werden.

Microsoft SQL Server Express LocalDB

Die Nutzung von Microsoft SQL Server Express LocalDB empfehlen wir ausschließlich für Installationen bis maximal 1.000 Clients oder für Test- und Evaluierungsumgebungen.

Die Scout-Datenbank wird automatisch während der Installation erstellt:

In der Scout-Installationsdatei ist Microsoft SQL Server Express LocalDB bereits enthalten. Während der Installation wird auf Wunsch die Datenbank vom Typ `LocalDB` erstellt. Der Datenbankname ist System-intern vorgegeben.

Mehrere Datenbankverbindungen

Mit dem Datenbank-Verbindungseditor können Sie mehrere Datenbank-Verbindungen für die Scout Console definieren, aus denen Sie beim Start der Konsole auswählen können. Auf einem Rechner können mehrere Verbindungen der Konsole zu unterschiedlichen Datenbanken parallel hergestellt werden.

Der Datenbank-Verbindungseditor befindet sich im Startmenü. Für weitere Informationen siehe "Datenbank-Verbindungen" auf Seite 60.

Datenbankbereinigung

Veraltete Daten können mit der Funktion **Datenbankbereinigung** gelöscht werden. Für weitere Informationen siehe Datenbankbereinigung.

4.2. SQL LocalDB

Die Nutzung der integrierten Datenbank als Minimalversion des Microsoft SQL Server zur Verwaltung kleinerer Client-Umgebungen empfehlen wir ausschließlich für Installationen bis maximal 1.000 Clients oder für Test- und Evaluierungsumgebungen. Die erforderlichen Softwaremodule für Microsoft SQL Server Express LocalDB sind in der Scout-Installationsdatei enthalten.

Während der Installation muss zur Nutzung der Datenbank unter Microsoft SQL Server Express LocalDB ein Scout-Windows-Benutzer angegeben werden, der als Eigentümer der LocalDB-Instanz agiert. Wir empfehlen, ein technisches Benutzerkonto zu verwenden, dessen Kennwort nicht abläuft und das von mehreren Benutzern für den Zugriff auf die LocalDB genutzt werden kann. Das Konto muss über das lokale Benutzerrecht **Anmelden als Dienst (Log on as a service)** verfügen und Mitglied der lokalen Administratorengruppe sein.

Einschränkungen bei der Nutzung von Microsoft SQL Server Express LocalDB gegenüber Microsoft SQL Server

- Der Betrieb der Scout Console ist ausschließlich in Verbindung mit dem Scout Serverdienst und der LocalDB-Datenbank auf einem Serversystem möglich. Dedizierte Scout Consolen mit Remote-Zugriff auf die LocalDB-Datenbank werden nicht unterstützt.
- Das Kommando **Konfigurationslauf** zur Vorbereitung der Geräte-Konfigurationen steht nicht zur Verfügung.

4.2.1. SQL LocalDB vor der Installation von Updates sichern

Bevor Sie eine bestehende Scout Enterprise Management Suite-Installation auf eine neuere Version aktualisieren, empfehlen wir, die bestehende LocalDB-Datenbank zu sichern.

Variante 1:

- Erstellen Sie eine Kopie der beiden Dateien `ScoutEnterpriseLocalDB.mdf` und `ScoutEnterpriseLocalDB_log.ldf` im Verzeichnis `C:\Users\<Name des Benutzers>\`

Nach der Scout-Installation kopieren Sie die Datenbank-Dateien zurück.

Variante 2 (erfordert SQL Server Management Studio):

1. Verbinden Sie sich in SQL Server Management Studio zur
   Datenbank `ScoutEnterpriseLocalDB`
   Instanz `(localdb)\.\ScoutEnterpriseManagementSuite_Shared`
2. Verwenden Sie die **Backup**-Funktion, um eine Sicherung zu erstellen.

   Für weitere Informationen siehe die Microsoft-Dokumentation zu SQL Server Management Studio, beispielsweise https://technet.microsoft.com/de-de/library/ms189621.

Nach der Scout-Installation verwenden Sie die Management Studio-Funktion **Restore** zum Wiederherstellen der Datenbank.

4.3. Authentifizierung am SQL-Server

Wenn Sie bei der Installation **Microsoft SQL Server** als Datenbanktyp wählen, können Sie zwischen den Authentifizierungsmethoden **Windows-Authentifizierung** und **SQL Server-Authentifizierung** wählen.

Die Authentifizierung erfordert entweder einen SQL-Benutzer oder einen Windows-Benutzer, der jeweils Mitglied bestimmter Datenbankrollen in SQL Server sein muss. Für weitere Informationen siehe "SQL Server-Benutzer und Anwendungsrollen " auf der nächsten Seite

Methode	Beschreibung
Windows-Authentifizierung	'Trusted connection': Die Benutzer-Identität wird von Windows bestätigt. Der Scout-Dienst muss mit einem Benutzerkonto ausgeführt werden, das die relevanten Berechtigungen in SQL Server besitzt. Die Anmeldedaten des Dienste-Kontos können im Dialog der Scout-Installation eingegeben werden.[1] ▸ Geben Sie im Dialog der Scout-Installation den Kontonamen in folgender Form an: `DOMÄNE\Benutzername` (Groß-/Kleinschreibung irrelevant) Beispiel: `INT\mmi` **Hinweis** Für die Scout-Installation muss auf dem Windows Server-System entweder ein Benutzer mit den relevanten Berechtigungen in SQL Server oder das zu verwendende technische Benutzerkonto (Anmelden als Dienst) angemeldet sein.
SQL Server-Authentifizierung	Benutzername und -Kennwort eines SQL Server-Benutzerkontos werden verwendet. Der SQL-Benutzer muss die entsprechenden Berechtigungen in SQL Server besitzen. ▸ Geben Sie im Dialog der Scout-Installation den SQL-Benutzernamen und das Kennwort an.

Wenn Sie die Scout Enterprise Management Suite vollständig installieren, werden drei Datenbanken benötigt. Den Zugriff auf die Datenbanken können Sie in folgenden Varianten konfigurieren:

- Wenn für alle Datenbanken dieselbe Authentifizierungsmethode verwendet wird, können Sie unterschiedliche Benutzer für die Datenbanken konfigurieren.
- Wenn für alle Datenbanken derselbe Benutzer verwendet wird, können Sie unterschiedliche Authentifizierungsmethoden für den Zugriff auf die Datenbanken konfigurieren.

[1] Ab Scout Enterprise Management Suite 15.5 wird die Verwendung von gMSA (Group Managed Service Accounts) unterstützt.

4.4. SQL Server-Benutzer und Anwendungsrollen

Die folgende Beschreibung gibt einen groben Überblick über die in SQL Server benötigten Berechtigungen, sowie über die Verwendung einer Anwendungsrolle. Eine Anwendungsrolle erhöht die Sicherheit, indem sie den operativen Administratoren nur die notwendigen Berechtigungen für die Dauer einer Sitzung zuweist.

Erstellen der Datenbanken

Wir empfehlen, die erforderlichen Datenbanken vor der Installation der Scout Enterprise Management Suite in SQL Server anzulegen.

Bitte beachten Sie folgendes:

- Zum Erstellen von Datenbanken in SQL Server ist mindestens die SQL Serverrolle **dbcreator** notwendig.
- Der Name einer Datenbank ist frei wählbar.
- Die Tabellen innerhalb der jeweiligen Datenbank werden durch den Installationsprozess der Scout Enterprise Management Suite erstellt.

> **Achtung** Löschen Sie beim Sichern und Wiederherstellen nicht die originale Datenbank! Die eindeutige Datenbank-ID muss erhalten bleiben für die Initialisierung der Lizenzdatenbank. Für weitere Informationen siehe "Problembehandlung" auf Seite 70.

Berechtigungen für die Nutzung der Scout Enterprise Management Suite

SQL Serverrolle
Grundsätzlich ist für die **Nutzung** der Scout Enterprise Management Suite die Serverrolle **public** ausreichend. Wenn Benutzer zusätzlich Aufgaben in SQL Server durchführen sollen, sind weitergehende Berechtigungen notwendig. Das Wiederherstellen von Datenbanken erfordert beispielsweise die Serverrolle **dbcreator**.

SQL Datenbankrolle
Auf Datenbankebene ist für die reine Nutzung der Konsole in Standard-Umgebungen die Kombination aus den Datenbankrollen **db_datareader** und **db_datawriter** ausreichend.
Die Datenbankrolle **db_owner** wird beispielsweise für Datenbank-Aktivitäten im Zusammenhang mit der Aktualisierung auf eine neue Scout-Version benötigt, ebenso zur Ausführung von Konfigurations- und Wartungsaktivitäten an der Datenbank.

Die Benutzer müssen dem Standardschema `dbo` zugeordnet sein.

> **Hinweis**
> Für Umgebungen mit SQL Server-Clustern sind zusätzliche Berechtigungen wie `VIEW SERVER STATE` und `VIEW ANY DEFINITION` erforderlich.

SQL Anwendungsrolle

Im Falle der **Windows-Authentifizierung** für SQL Server sind die Benutzer berechtigt, sich auch am SQL Server Management Studio anzumelden. Für solche Szenarien empfehlen wir, eine dedizierte Benutzergruppe für reine Konsolen-Benutzer zu verwenden, die mit beschränkten Datenbankrechten arbeitet.

Die Berechtigungen für den Zugriff auf SQL Server-Tabellen können für alle Datenbanken zusätzlich über eine systemweite SQL-Anwendungsrolle gesteuert und beschränkt werden. Die Anwendungsrolle muss in der jeweiligen Datenbank mit Namen und Kennwort hinterlegt werden.

Ein Konsolen-Benutzer benötigt dann für SQL Server nur die Datenbank-Rolle **public**, damit die gespeicherte Prozedur zum Aktivieren der Anwendungsrolle der SQL Server-Datenbank ausgeführt werden kann. Sobald die Anwendungsrolle aktiv ist, verliert die Verbindung zu SQL Server die Benutzer-Berechtigungen und nimmt die Berechtigungen der Anwendungsrolle an. Eine Anwendungsrolle kann auf keine anderen Datenbanken zugreifen, sofern deren **guest**-Konto deaktiviert ist. Die Berechtigungen der Anwendungsrolle bleiben für die Dauer der Sitzung aktiv.

Konsolen-Benutzer und Anwendungsrolle in SQL Server Management Studio konfigurieren

Die folgende Anleitung bezieht sich auf die Scout-Datenbank.

1. Fügen Sie im SQL Server Management Studio unter **Sicherheit > Anmeldungen** eine neue Benutzergruppe (Beispiel: **Konsolen-Benutzer**) hinzu mit folgender Konfiguration:

Serverrolle	Public
Benutzerzuordnung > Mitgliedschaft in Datenbankrolle	db_datareader
Sicherungsfähige Elemente	Setzen Sie nicht erforderliche Berechtigungen auf `Deny`. Beispiel auf Server-Ebene: **Alter any database** > `Deny`

2. Erstellen Sie unterhalb der Scout-Datenbank unter **Sicherheit > Schemas** ein neues Schema (Beispiel: **Konsolen-Benutzer-Schema**).
   Geben Sie im Feld **Schemabesitzer** die **Konsolen-Benutzer** an.
3. Erstellen Sie unterhalb der Scout-Datenbank unter **Sicherheit > Rollen > Anwendungsrollen** eine Anwendungsrolle (Beispiel: **Konsolen-Benutzer-Rolle**) mit folgender Konfiguration:

Standard-Schema	Konsolen-Benutzer-Schema
Kennwort	frei wählbar
Sicherungsfähige Elemente	Wählen Sie Ihre Scout-Datenbank und setzen Sie alle Berechtigungen außer **Connect** auf `Grant`

Anwendungsrolle in Scout-Datenbank definieren

1. Um die Daten der Anwendungsrolle verschlüsselt anzugeben, verschlüsseln Sie zunächst Namen und Kennwort der Rolle. Für weitere Informationen siehe "Werte verschlüsseln" auf Seite 73.
2. Bearbeiten Sie im SQL Server Management Studio für die Scout-Datenbank die Tabelle **System**.
3. Fügen Sie für Namen und Kennwort der Anwendungsrolle jeweils eine Zeile hinzu. Setzen Sie die verschlüsselten Werte in die Tabelle ein:

SystemID	ParamName	ParamVal
…		
<n>	RNameEx	*<verschlüsselter Name der Rolle>*
<n>	RPassEx	*<verschlüsseltes Kennwort der Rolle>*

Beim Starten der Scout Console werden die Felder ausgelesen und die Zugriffsberechtigungen der Anwendungsrolle gesetzt.

1.

EnvironmentInfoID	Key	Value
…		
<n>	RName	*<verschlüsselter Name der Rolle>*
<n>	RPass	*<verschlüsseltes Kennwort der Rolle>*

4.5. Scout Servercluster

Bei Verwendung einer SQL-Datenbank können mehrere Scout Server gleichzeitig zur Scout-Datenbank verbunden werden. Dadurch entsteht neben der Ausfall-Lastverteilung (FailureLoadBalancing) auch die Möglichkeit zur konfigurierbaren Lastverteilung (ManagerLoadBalancing).

Bei Kontakt zu einem Scout Server erhalten die Geräte grundsätzlich eine Liste aller Server, die auf die gemeinsame Scout-Datenbank zugreifen und zum Zeitpunkt des Client-Kontaktes gestartet sind.

FailureLoadBalancing

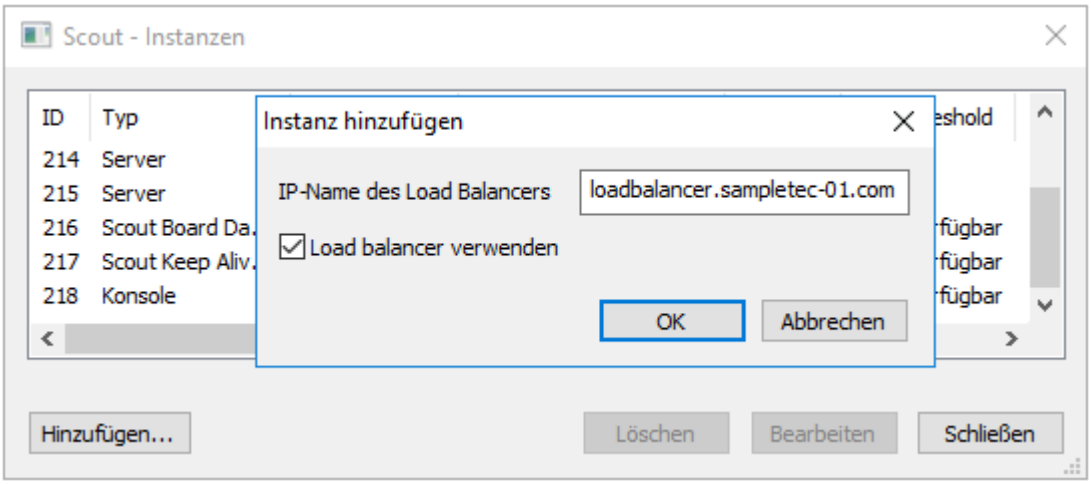
Wenn der Client bei einem Kontaktversuch auf den zuletzt verfügbaren Scout Server nicht mehr zugreifen kann, verbindet sich der Client mit dem nächsten Server aus der Serverliste. Dieser Server wird anschließend standardmäßig bei allen weiteren Verbindungsversuchen verwendet.

Der Mechanismus des FailureLoadBalancing greift erneut, sobald sich der Client nicht mehr auf den zuletzt verfügbaren Scout Server verbinden kann.

ManagerLoadBalancing mit dediziertem Load Balancer

Um einen dedizierten Load Balancer zu definieren, tragen Sie die Adresse (IP-Adresse oder Name) des bevorzugten Load Balancing-Servers, zu dem sich die Clients verbinden sollen, als neue Instanz ein:

- Fügen Sie in der Scout Console in **Ansicht > Scout-Instanzen**, eine neue Instanz hinzu und aktivieren Sie die Option **Load Balancer verwenden**.



Der Load Balancer-Eintrag bezieht sich auf einen vorhandenen Load Balancer, der auf den entsprechenden Scout Server verweist. Mit dem Load Balancer-Eintrag können Sie einem bestimmten Scout Server Geräte zuordnen ohne Änderungen in der Scout-Umgebung.

Der Load Balancer-Name wird von den Geräten bei jedem Neustart ausgewertet.

Ablauf:

- Gerät startet
- Gerät verbindet sich zum Load Balancer und wird zum ermittelten Scout Server weitergeleitet

Wenn der über den DNS-Eintrag `ManagerLoadBalancer` ermittelte Scout Server nicht verfügbar ist, greift der oben beschriebene Mechanismus des FailureLoadBalancing und der Client verbindet sich mit dem nächsten Server aus der Serverliste.

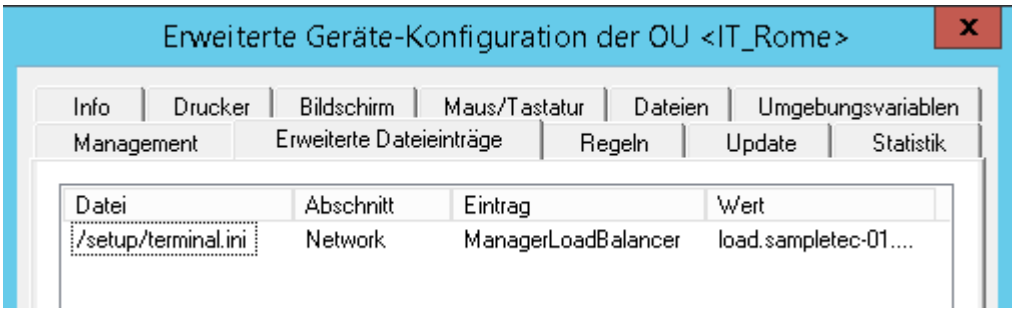
ManagerLoadBalancing über DNS-Eintrag

Einen bevorzugten Scout Server für den Verbindungsversuch können Sie alternativ über einen DNS-Eintrag vorgeben, auf den Sie in den Erweiterten Dateieinträgen verweisen.

- Verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Console, für alle Geräte, für eine OU oder für ein einzelnes Gerät:

Datei	`/setup/terminal.ini`
Abschnitt	`Network`
Eintrag	`ManagerLoadBalancer`
Wert	*<FQDN DNS-Eintrag>*

Für weitere Informationen siehe Erweiterte Dateieinträge.



Als `ManagerLoadBalancer` wird ein am DNS-Server gesondert zu setzender DNS-Eintrag verwendet, der auf den entsprechenden Scout Server verweist. Über den DNS-Eintrag können Sie einem bestimmten Scout Server Geräte zuordnen ohne Änderungen in der Scout-Umgebung.

Die Geräte werten den Parameter `ManagerLoadBalancer` bei jedem Client-Neustart aus.

Ablauf:

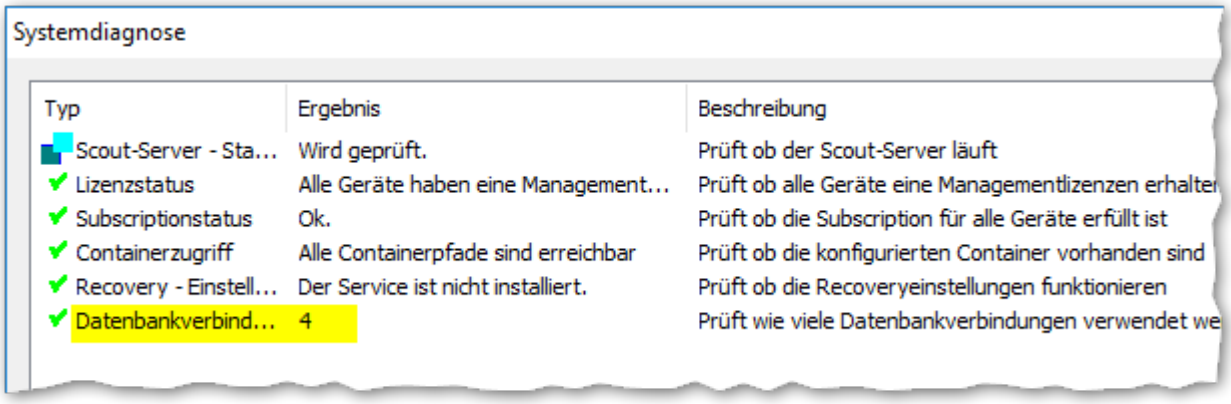
- Client startet
- DNS-Eintrag `ManagerLoadBalancer` wird aufgelöst
- Client wird zum ermittelten Scout Server weitergeleitet

Wenn der über den DNS-Eintrag `ManagerLoadBalancer` ermittelte Scout Server nicht verfügbar ist, greift der oben beschriebene Mechanismus des FailureLoadBalancing und der Client verbindet sich mit dem nächsten Server aus der Serverliste.

4.6. Anzahl der ODBC-Verbindungen

Die Anzahl der ODBC-Verbindungen zwischen Scout Server und der Scout-SQL-Datenbank wird dynamisch beim Start des Serverdienstes definiert. Pro CPU-Kern werden automatisch zwei ODBC-Verbindungen festgelegt und genutzt.

Die aktuelle Anzahl der Datenbankverbindungen können Sie durch einen Systemcheck (Scout Console **Ansicht > Systemdiagnose > Systemcheck**) ermitteln und anzeigen:



Erfahrungsgemäß führen zwei ODBC-Verbindungen pro CPU-Kern zu einem guten Ergebnis unter Berücksichtigung von

- maximaler Kommunikationsperformance zwischen Scout Server und SQL-Datenbank sowie
- einer optimalen CPU-Auslastung.

Statische statt dynamische Definition der ODBC-Verbindungen

Sie können die Anzahl der ODBC-Verbindungen fest vorgeben, um besonderen Systemanforderungen einer Scout-Installation zu entsprechen. Dafür setzen Sie folgenden Parametereintrag in der Konfigurationsdatei `eluxd.ini` des Scout Servers:

Datei	`%systemdrive%\Users\Public\Documents\UniCon\Scout\Server\eluxd.ini`
Abschnitt	`[ELUXD]`
Parameter	`DatabaseConnections=`
Wert	`n` *(n=1-128)*

Hinweis
Beachten Sie, dass das manuelle Erhöhen der Anzahl der Datenbankverbindungen zur CPU-Überlastung führen kann.

Für weitere Informationen zum Bearbeiten von `INI`-Dateien, siehe Erweiterte Dateieinträge.

5. Vorbereitung der Installation

Scout Server und Scout Keep Alive-Service bzw. Scout Statistikservice können auf der gleichen Maschine oder auf unterschiedlichen Maschinen installiert werden.

Stellen Sie sicher, dass das jeweilige Betriebssystem über die aktuellen Patches verfügt und die erforderliche Software installiert ist. Für weitere Informationen siehe "Systemvoraussetzungen" auf Seite 6.

Bevor Sie mit der Installation beginnen, beachten Sie die im folgenden zusammengestellten Informationen.

5.1. Scout Server im Netzwerk bekannt machen

Damit Clients automatisch in die Verwaltung aufgenommen werden können, konfigurieren Sie die IP-Adresse des Scout Servers entweder über DNS oder über DHCP:

- DNS: Weisen Sie der IP-Adresse den Hostnamen `ScoutSrv` zu. Dies ist die einfachste Möglichkeit.

  Oder:

- Konfigurieren Sie eine oder mehrere DHCP-Optionen. Für weitere Informationen siehe DHCP-Konfiguration.

Hinweis
Wenn Sie zu einem späteren Zeitpunkt einen anderen Scout Server zuweisen möchten, verwenden Sie dazu die Scout-Funktion **Geräteumzug**. Ändern Sie die DHCP-Konfiguration nicht im laufenden Betrieb der Clients.

Hinweis
Wenn Sie keine DHCP-Optionen für Scout einsetzen, empfehlen wir, in der **Geräte-Konfiguration > Netzwerk** die Option **Scout Server DHCP-Optionen ignorieren** zu aktivieren.

5.1.1. DHCP-Konfiguration

- optional -

Hinweis
DHCP-Optionen können nur auf eLux-Clients angewendet werden.

Ein Client kann beim ersten Bootvorgang folgende Informationen vom DHCP-Server beziehen:

- IP-Adresse oder Name des Scout Servers (Option 222)
- Liste der Scout Server (Option 224)
- ID für die Ziel-OU am Scout Server (Option 223)

Voraussetzung ist die Konfiguration des DHCP-Servers mit einer der beiden folgenden Methoden.

Mit Methode 1 (empfohlen) definieren Sie eine neue Herstellerklasse, setzen die neuen Optionen und geben die Werte für diese Optionen an.Methode 2 verwendet die Standardoptionen 222, 223 und 224.

Die folgenden Anleitungen basieren auf dem DHCP-Manager unter Windows Server 2012.

Methode 1: Benutzer-definierte Herstellerklasse erstellen

Voraussetzung
DHCP-Server nach RFC 2132, der benutzerdefinierte Herstellerklassen unterstützt.Andernfalls verwenden Sie Methode 2.

1. Öffnen Sie den DHCP-Manager.
2. Markieren Sie den relevanten DHCP-Server und wählen Sie **Aktion > Herstellerklassen definieren...**
3. Erstellen Sie mit **Hinzufügen...** eine neue Klasse mit folgenden Angaben:

Option	Wert
Anzeigename	eLux NG
Beschreibung	eLux-spezifische Optionen
Kennung (in Spalte **ASCII**)	ELUXNG *Diese Eingabe wird automatisch mit dem hexadezimalen Wert ergänzt (45 4C 55 58 4E 47).*

4. Wählen Sie die Menüfunktion **Aktion > Vordefinierte Optionen einstellen...** und dann im Listenfeld **Optionsklasse** den Eintrag `eLux NG`.
5. Wenn Sie einen Scout Server definieren möchten, erstellen Sie mit **Hinzufügen** eine neue Option mit folgenden Angaben:

Option	Wert
Name	Scout Server
Datentyp	Zeichenkette
Code	222
Beschreibung	Name oder IP-Adresse des Scout Servers

6. Wenn Sie mehrere Scout Server definieren möchten, erstellen Sie mit **Hinzufügen** eine Option mit folgenden Angaben:

Option	Wert
Name	Scout Serverliste

Option	Wert
Datentyp	Zeichenkette
Code	224
Beschreibung	Servernamen/IP-Adressen, Komma-getrennt

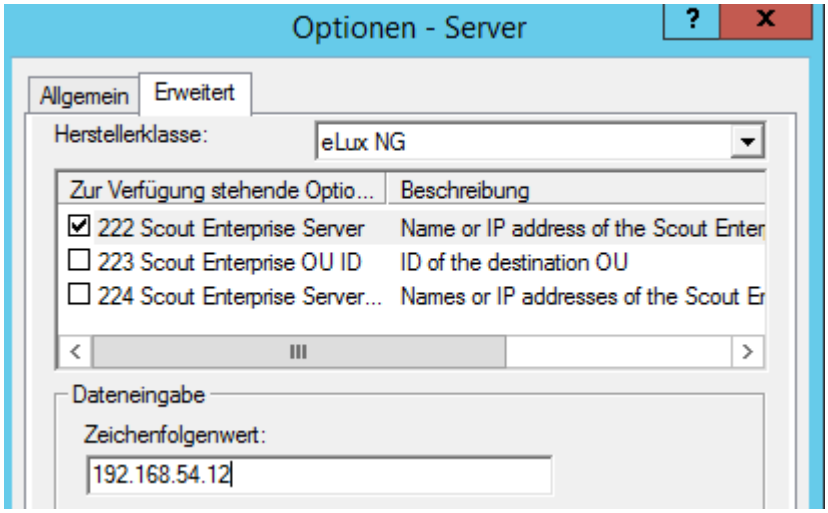
7. Wenn Sie neue Geräte über DHCP einer bestimmten OU zuordnen möchten, erstellen Sie mit **Hinzufügen** eine Option mit folgenden Angaben:

Option	Wert
Name	Scout OU-ID
Datentyp	Lang
Code	223
Beschreibung	OU-ID am Scout Server

8. Um die Optionen zuzuordnen, markieren Sie für den relevanten DHCP-Server entweder die **Serveroptionen**, die **Bereichsoptionen** oder die **Reservierungen** und wählen dann **Aktion > Optionen konfigurieren... > Erweitert**.

   Wählen Sie im Listenfeld **Herstellerklasse** den Eintrag `elux NG`.Aktivieren Sie die erstellten Optionen und geben Sie die entsprechenden Werte ein:

Option	Wert
222 Scout Server	*<Name oder IP-Adresse des Scout Servers>*
223 Scout OU-ID	*<ID der Ziel-OU am Scout Server>*
224 Scout Ser-verliste	*<Namen oder IP-Adressen der Scout Server, durch Kommata getrennt>*



Methode 2: Standardoptionen verwenden

Voraussetzung
Die Standardoptionen `222`, bzw. `223` und `224` müssen verfügbar sein.Andernfalls verwenden Sie Methode 1.

1. Öffnen Sie den DHCP-Manager.
2. Markieren Sie den relevanten DHCP-Server und wählen Sie **Aktion > Vordefinierte Optionen einstellen...** und dann im Listenfeld **Optionsklasse** den Eintrag `DHCP-Standardoptionen`.
3. Erstellen Sie mit **Hinzufügen** folgende Standard-Optionen nach dem in Methode 1 beschriebenen Muster:
   - Scout Server, Zeichenkette, 222
   - Scout Serverliste, Zeichenkette, 224
   - Scout OU-ID, Lang, 223
4. Um die Optionen zuzuordnen, markieren Sie für den relevanten DHCP-Server entweder die **Serveroptionen**, die **Bereichsoptionen** oder die **Reservierungen** und wählen dann **Aktion > Optionen konfigurieren... > Allgemein**.Aktivieren Sie die erstellten Optionen und geben Sie die entsprechenden Werte ein:

Option	Wert
222 Scout Server	*<Name oder IP-Adresse des Scout Servers>*
223 Scout OU-ID	*<ID der Ziel-OU am Scout Server>*
224 Scout Serverliste	*<Namen oder IP-Adressen der Scout Server, durch Komma getrennt>*

Übernahme des Hostnamens aus DHCP-Option unterdrücken

Wenn Sie die DHCP-Option 12 (Hostname) konfiguriert haben, können Sie die Hostnamen beim Anbinden neuer Geräte über DHCP setzen.Um den Hostnamen **nicht** über DHCP sondern aus einer anderen Quelle zu beziehen, beispielsweise über die in der Scout Console definierte Namensschablone, unterdrücken Sie die Übernahme aus der DHCP-Option 12.Verwenden Sie dazu einen `terminal.ini`-Parameter:

Datei	`/setup/terminal.ini`	
Abschnitt	`Network`	
Eintrag	`IgnoreDHCPHostname`	
Wert	`true`	Standardmäßig steht der Wert auf `false`.

5.1.2. Neue Geräte bestimmten Scout Servern zuweisen

Wenn Sie mehrere Scout Server einsetzen, können Sie für die Registrierung neuer Geräte im Voraus festlegen, welchem Scout Server ein Gerät zugeordnet werden soll.Als Kriterium für die Zuordnung dient ein Filter (regulärer Ausdruck) auf die MAC-Adresse.

Die Filterregeln werden in einer `.ini`-Datei definiert, die dann mit Hilfe eines benutzerdefinierten Feature-Paketes im Image auf die Geräte übertragen wird.Auf diese Weise erhalten neue Geräte die Information, zu welchem Scout Server sie sich verbinden sollen, bereits vor dem ersten Kontakt zu Scout.

Die `.ini`-Datei, beispielsweise `scoutmapping.ini` ist eine Textdatei, die nach folgendem Muster aufgebaut wird:

```
[Mapping1]
```

```
 identifier=MAC   pattern=[AB][0-9A-F]$   scoutsrv=scout1.sampletec-01.com
[Mapping2]   identifier=MAC   pattern=[CD][0-9A-F]$   scoutsrv=scout2.sampletec-01.com
[Mapping3]   identifier=MAC   pattern=[EF][0-9A-F]$   scoutsrv=scout3.sampletec-01.com
```

Beachten Sie folgendes:

- In Scout wird die MAC-Adresse als 12-stellige Zahl ohne Trennzeichen dargestellt (Beispiel: `901B0E01CE84`)
- Der Filter muss ein regulärer Ausdruck sein, der auf einen Teil-String der MAC-Adresse filtert.
- In einem PostInstall-Skript und PreUninstall-Skript des Feature-Paketes muss auf die `.ini`-Datei verwiesen werden, Beispiel: `./setup/scoutmapping.ini`

Bitte wenden Sie sich für weitere Details an den Unicon-Support.

5.2. Firewall freischalten

- Öffnen Sie folgende Ports in der Firewall:[1]

Port	Typ	von	nach
1433	TCP	Scout Server	MS SQL Server
1434	UDP	Scout Server	MS SQL Server (Browserdienst)
22123	TCP	Scout Server (Scout Management /secure)	eLux-Clients
22125	TCP	Scout Server (Scout Management / TLS 1.2)	eLux-Clients
22124	TCP	Scout Server	Scout Keep Alive-Service
5900	TCP	Scout Console (Spiegelung des eLux Desktop)	Client-Geräte
80/443	TCP	Clients (HTTP/HTTPS)	Webserver
80/443	TCP	Clients (Firmware-Updates über HTTP/HTTPS)	Webserver

Beachten Sie, dass MS SQL Server seinen Clients nach dem Verbindungsaufbau dynamisch Port-Nummern zwischen 1024 und 5000 zuweist und erlauben Sie die Kommunikation von 1433 zu *ANY*.

Für weitere Informationen siehe IP-Ports.

Der Firewall-Dienst muss gestartet sein.

5.3. SQL Server-Datenbanken vorbereiten

Prüfen Sie, ob folgende Voraussetzungen erfüllt sind:

- Die Scout Server-Maschinen müssen über passende ODBC-Treiber zur Anbindung an die SQL-Datenbank verfügen. Für weitere Informationen siehe "Systemvoraussetzungen" auf Seite 6.
- Wir empfehlen, die erforderlichen Datenbanken (mit beliebigem Dateinamen) vor der Installation der Scout Enterprise Management Suite in Microsoft SQL Server anzulegen.[2]

  Hinweis
  Die Tabellen werden automatisch durch die Scout-Installationsroutine erstellt.

  Für weitere Informationen siehe "Datenbankunterstützung" auf Seite 10.

[1] vorausgesetzt, Sie verwenden die Standard-Ports
[2] Alternativ können die Scout-Datenbanken während der Installation in Microsoft SQL Server erstellt werden, entsprechende Rechte vorausgesetzt.

- SQL- oder AD-Benutzer (**SQL-Server\Instanz> / Sicherheit / Anmeldungen**) mit relevanten SQL Server-Berechtigungen für alle eingesetzten Datenbanken

  Für weitere Informationen siehe "SQL Server-Benutzer und Anwendungsrollen " auf Seite 14.

- Der Browser-Dienst auf dem SQL-Server muss gestartet sein.

5.4. Berechtigungen und Zertifikate

Berechtigung für die Scout Enterprise Management Suite-Installation

- AD-Administrator-Konto, Mitglied in der Gruppe der lokalen Administratoren auf dem Zielserver
- Das Konto muss über das lokale Benutzerrecht **Anmelden als Dienst (Log on as a service)** verfügen, wenn Sie LocalDB verwenden.

Für weitere Informationen zur Authentifizierung an der LocalDB siehe SQL LocalDB.

Für Informationen zur Authentifizierung am SQL-Server siehe Authentifizierung am SQL-Server.

Hinweis
Das Konto des installierenden Administrators ist das erste Konto, das nach dem Aktivieren der Administratorenverwaltung in der Scout Console aktiv ist.

Berechtigungen für den Webserver

Auf dem Webserver werden in einem oder mehreren eLux-Containern eLux Software-Pakte und Images bereitgestellt.

- Webserver (IIS)-Rolle oder entsprechende Berechtigung für den eingesetzten Webserver
- Administratorrechte auf das Root-Verzeichnis für den installierenden Administrator
- Schreibzugriff auf das eLux-Container-Verzeichnis für alle Benutzer, die Images in ELIAS bearbeiten dürfen

Berechtigungen für Scout Board

Die Anmeldung über Active Directory wird bereits im Technical Preview unterstützt. Die Administratorrechte werden so angewendet wie in der Scout Console unter **Sicherheit > Administratorenverwaltung** definiert.

SSL-Zertifikate für Scout Keep Alive-Service und Scout Board

Die Kommunikation zwischen eLux und dem Scout Keep Alive-Service[1] erfolgt über HTTPS. Während der Installation wird ein gültiges SSL-Zertifikat abgefragt oder alternativ ein Self-signed-Zertifikat angeboten(standardmäßig an Port 22124). Für weitere Informationen siehe "Zertifikat für Scout Keep Alive-Service" auf Seite 63.

Für eine sichere (HTTPS)-Verbindung zum Scout Board-Interface benötigen Sie ebenfalls ein gültiges SSL-Zertifikat. Für weitere Informationen siehe Scout Board installieren.

---

[1] ab Scout 15 2209. Frühere Versionen: Scout Statistikservice

eLux-Zertifikate für Software-Pakete

Wenn Sie die Signaturen der eLux Software-Pakete mit ELIAS überprüfen möchten, benötigen Sie die relevanten Zertifikate:

- Downloaden Sie die Zertifikate von unserem Portal myelux.com unter **eLux Software Packages**.

5.5. Software herunterladen

Laden Sie vor Beginn der Installation die `.zip`-Dateien zur Installation der gewünschten Software herunter:

- Scout Enterprise Management Suite
- ELIAS 18 zum Erstellen individueller Firmware-Images
- eLux-Software-Pakete für die gewünschte Betriebssystemversion
- USB-Stick-Image zur Recovery-Installation für einzelne Geräte für die gewünschte Betriebssystemversion
- …

1. Melden Sie sich auf unserem Portal myelux.com an.
2. Wählen Sie im Menü **Downloads** die gewünschte Software:

Option	Beschreibung / Option	Download
eLux	eLux Software Packages Neueste Betriebssystemversion als LTSR[1] oder CR[2]	■ Bundle: Mit `AllPackages-x` können Sie einen Container mit allen Software-Paketen einer eLux-Version in einem Schritt installieren[3] oder in ELIAS 18 importieren. ■ Einzelne Pakete: Für eine eLux-Version werden alle verfügbaren Software-Pakete unter **Release Packages** zum Download angeboten.
eLux	eLux USB Stick Images Fertige Images für die neueste eLux-Version zur Installation von USB	■ <eLux CR version> Recovery Stick ■ <eLux LTSR version> Recovery Stick enthält die Citrix Workspace app und den VMware Horizon-Client zur Verbindung gegen ein Backend
eLux	eLux Portable eLux auf USB, basierend auf aktueller eLux RP-Version	eLux Portable (keine Installation erforderlich)

[1] Long Term Service Release
[2] Current Release
[3] enthält die Installationsdatei `eLuxContainer.exe`

Option	Beschreibung / Option	Download
Scout	Scout Enterprise Management Suite Neueste LTSR- und CR-Version	■ <Scout CR-Version> ■ <Scout LTSR-Version> enthält die Installationsdatei `ScoutInstaller.exe`
	ELIAS Neueste ELIAS 18-Version zum Erstellen und Verwalten eigener Images Die Scout Enterprise Management Suite enthält alternativ die klassische ELIAS-Version.	■ ELIAS 18 <aktuelle Version> für Windows ■ ELIAS 18 <aktuelle Version> für Linux
	Scout Agent for Windows zur Verwaltung von Windows-Geräten	Neueste Version
Scout Cloud Gateway	Gateway zur Anbindung Ihrer Geräte über das Internet (neueste Version)	■ Vorlage für eine virtuelle Maschine (`.ova`) oder ■ Debian-Paket
Tools	StickWizz (auch in eLux USB Stick Images enthalten)	Neueste Version
	eLux Builder Kit (eLux SDK VM) Entwicklungsumgebung	Bitte bei sales(at)unicon.com erfragen
	Win2eLux Migration von Windows zu eLux	■ Win2eLux for 64-bit Windows ■ Win2eLux for 32-bit Windows

Für weitere Informationen siehe Long Term Service Releases und Current Releases im Whitepaper **Release-Optionen, Lebenszyklen und Kompatibilität**.

3. Um die gewünschte Datei herunterzuladen, klicken Sie jeweils auf den Dateinamen oder die Versionsnummer.

   Die Software wird in Form von `.zip`-Dateien heruntergeladen.

4. Entpacken Sie die `.zip`-Dateien.

5. Stellen Sie die Installationsdateien, beispielsweise `ScoutInstaller.exe` auf einer lokalen Festplatte bereit.
6. Um einen Recovery-Stick zu erstellen, stecken Sie einen leeren USB-Stick auf einen USB-Anschluss. Starten Sie die Anwendung `StickWizz.exe` aus dem `zip`-Archiv und schreiben Sie das Image auf den Stick. Für weitere Informationen siehe USB-Recovery-Stick erstellen in der Kurzanleitung **eLux Recovery-Verfahren**.

6. Installation: Scout Enterprise Management Suite

Die Scout Enterprise Management Suite enthält alle Komponenten, die zur Verwaltung einer Client-Infrastruktur erforderlich oder nützlich sind, insbesondere den Scout Server und die Scout Console.

Wenn Sie individuelle Firmware-Images erstellen möchten, installieren Sie zusätzlich **eine** der folgenden Software-Komponenten:

- ELIAS 18

  Hier importieren Sie später die Software-Pakete einer eLux-Version, die für die Firmware der Clients zur Auswahl stehen.
  Für weitere Informationen siehe Installation: ELIAS 18.

  oder

- Bei Verwendung des klassischen ELIAS, der in der Scout Enterprise Management Suite enthalten ist:[1]

  eLux-Container mit den Software-Paketen einer eLux-Version, zur Installation auf einem Webserver
  Für weitere Informationen siehe Installation: eLux-Container.

6.1. Funktionsumfang der Scout Enterprise Management Suite

Mit der Scout Enterprise Management Suite verwalten Sie voll umfänglich Cloud-Geräte, Hybrid Clients, mobile Geräte, PCs, und andere x86-Geräte, die mit dem Betriebssystem eLux arbeiten. Zusätzlich können Sie Windows-basierende Geräte mit grundlegenden Funktionen verwalten.

Die Scout Enterprise Management Suite besteht aus mehreren Komponenten. Die meisten Komponenten sind Bestandteil der Standard-Installation, können aber im Rahmen einer benutzerdefinierten Installation optional abgewählt werden.

Komponente	Beschreibung	Installation
Scout Server	Der Dienst steuert und verwaltet eLux-Geräte sowie Windows-basierende Geräte, die Scout Agent für Windows installiert haben.	`ScoutInstaller.exe`

[1] Wählen Sie die Benutzer-definierten Installation und aktivieren ELIAS als Komponente.

Komponente	Beschreibung	Installation
Scout Console	Benutzeroberfläche zur Verwaltung von eLux-Geräten sowie von Windows-basierenden Geräten, die Scout Agent für Windows installiert haben Kommuniziert ausschließlich über die Datenbank mit dem Server In einer Scout-Datenbank können mehrere Konsolen verwaltet werden.	`ScoutInstaller.exe`
Scout Board	Web-basierte Benutzeroberfläche zur Verwaltung von eLux-Geräten sowie von Windows-basierenden Geräten, die Scout Agent für Windows installiert haben	`ScoutInstaller.exe`
Recovery-Service	TFTP-Dienst zur Realisierung einer PXE-Recovery-Umgebung für eLux-Geräte	`ScoutInstaller.exe`
ELIAS[1]	Mit dem "klassischen" Dialogprogramm eLux Image Administration Service (ELIAS) können individuelle Imagedefinitionsdateien (`.idf`) zum modularen Update der Firmware von eLux-Geräten erstellt werden. Der klassische ELIAS wird von ELIAS 18 abgelöst.	`ScoutInstaller.exe`
ELIAS 18	Neue Web-basierte und Plattform-unabhängige ELIAS-Anwendung zur Erstellung individueller Imagedefinitionsdateien (`.idf`)	gesondert (`EliasInstaller.exe`)
Scout Reportgenerator	Tool zum Erstellen von frei definierbaren Reports über die aktuell in der Scout-Datenbank enthaltenen Geräte, Anwendungen und OUs Aufruf über die Scout Console	`ScoutInstaller.exe`
Scout Keep Alive-Service[2]	Windows-Dienst zur Verarbeitung von Keep Alive-Paketen von eLux-Geräten	`ScoutInstaller.exe`

[1]Der klassische ELIAS ist nicht in der Standard-Installation enthalten. Um die Komponente zu installieren, wählen Sie **Benutzerdefiniert**.
[2]Ersetzt ab Scout 15 2209 den Scout Statistikservice

Komponente	Beschreibung	Installation
Web API (nur für SQL Server-Datenbank)	Programmierbare Anwendungsschnittstelle zur Verwaltung von eLux-Geräten sowie von Windows-basierenden Geräten, die Scout Agent für Windows installiert haben	`ScoutInstaller.exe`
Scout Command Interface	Kommandozeilen-Tool für Scout - Befehle	`ScoutInstaller.exe`
Scout Datenbankverbindungseditor	Tool zum Bearbeiten der Datenbankverbindungseinstellungen des Scout Servers und der Scout Console	`ScoutInstaller.exe`

Weitere Produkte

Scout Cloud Gateway	Cloud-Gateway mit VPN-Backend zur komfortablen Anbindung von Geräten aus dem Internet an eine Scout-Infrastruktur	gesondert
Scout Agent für Windows	Dienst mit Benutzerschnittstelle für Windows-basierende Geräte zur Verwaltung durch die Scout Enterprise Management Suite	gesondert

Die Funktionalität wird in folgenden Handbüchern beschrieben:

- Scout Enterprise Management Suite:
  Konfiguration, Steuerung und Verwaltung der Endgeräte durch die Scout Console
- Scout Board
- Scout Cloud Gateway
- ELIAS (der "klassische" ELIAS)
- ELIAS 18
- Scout Reportgenerator
- Scout Command Interface

Recovery-Verfahren für eLux-Geräte werden in einer Kurzanleitung beschrieben.

Hinweis
Damit Sie Ihre eigenen Image-Dateien zusammenstellen können, benötigen Sie zusätzlich zur Scout Enterprise Management Suite-Installation eine ELIAS 18-Installation. Bei Einsatz des klassischen ELIAS benötigen Sie einen eLux-Container, der die Software-Pakete enthält, siehe eLux-Container installieren.

6.2. Scout Enterprise Management Suite installieren

Hinweis
Lesen Sie vor der Installation die Kapitel Systemvoraussetzungen und Vorbereitung der Installation.

Mit der Installationsroutine der Scout Enterprise Management Suite können Sie eine Standard-Installation durchführen, die alle Komponenten bis auf den klassischen ELIAS enthält. ELIAS 18 installieren Sie separat.

Alternativ verwenden Sie die benutzerdefinierte Variante und wählen die zu installierenden Komponenten. Hier können Sie den klassischen ELIAS hinzufügen. Für weitere Informationen zum Installationsumfang siehe "Funktionsumfang der Scout Enterprise Management Suite" auf Seite 32.

Hinweis
Führen Sie die Installation von einem lokalen Laufwerk aus, also nicht von einem USB-Stick, CD-Laufwerk oder Netzlaufwerk.

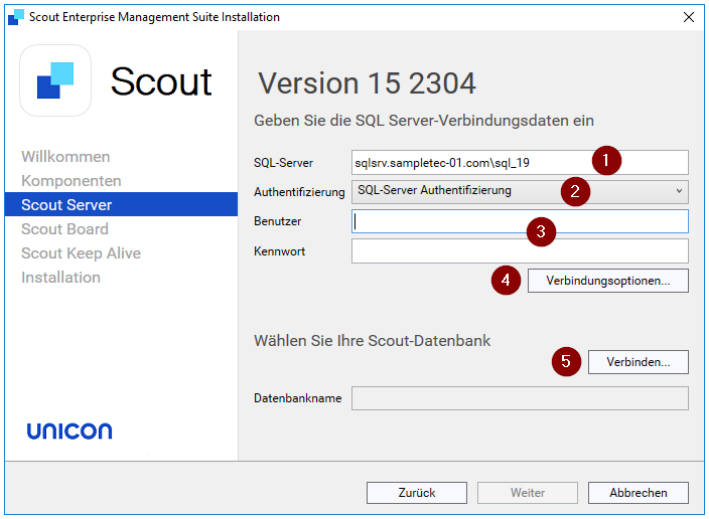
Hinweis
Anti-Viren-Programme können die Installation beeinflussen. Deaktivieren Sie Anti-Virus-Programme vor der Installation.

1. Führen Sie die Datei `ScoutInstaller.exe` als Administrator aus.
2. Wählen Sie die Sprache für die Installation. Lesen Sie anschließend die Lizenzvereinbarung und stimmen Sie zu.
3. Wählen Sie den Datenbanktyp, den Sie einsetzen:
   - `Microsoft SQL Server`
   - `Microsoft SQL LocalDB`

   Für weitere Informationen siehe Datenbankunterstützung.
4. Wählen Sie den Installationstyp. Die Option `Dienstleister` ist nur für Managed Service Provider (MSP) relevant, die Scout als Dienstleister anbieten möchten und über ein MSP-Konto auf unserem Portal myelux.com verfügen. Für weitere Informationen siehe die Kurzanleitung **Scout für MSPs**.
5. Wählen Sie den Installationsumfang. Um einzelne Komponenten für die Installation auszuwählen oder das Installationsverzeichnis zu ändern, wählen Sie `Benutzerdefiniert`. Für die Standard-Installation wählen Sie `Standard`.
6. Geben Sie die Datenbank-Verbindungsdaten für Ihre **Scout-Datenbank** ein.

   Wenn Sie Microsoft SQL LocalDB verwenden, geben Sie den relevanten Windows-Benutzer und das Kennwort an. Für weitere Informationen siehe SQL LocalDB.

   Wenn Sie Microsoft SQL Server verwenden, geben Sie die Verbindungsdaten für die SQL Server-Maschine ein:



1	*<SQL Server-Maschine\Instanz>* Beispiel: `sqlsrv.sampletec-01.com\sql_19`
2	`SQL Server-Authentifizierung` oder `Windows-Authentifizierung` Für weitere Informationen siehe Authentifizierung am SQL-Server.
3	SQL-oder Windows-Benutzername und -Kennwort für Zugriff auf die Datenbank
4	Verbindungsoptionen für den SQL Server: • Für AlwaysOn Cluster: Schnelleres Wiederverbinden nach Failover • Verschlüsselte ODBC-Verbindung verwenden • Server-Zertifikat vertrauen (standardmäßig aktiv)
5	Klicken, um Verbindung zum Datenbank-Server herzustellen

Nachdem Sie auf **Verbinden...** geklickt haben, wählen Sie Ihre **Scout**-Datenbank aus dem Listenfeld.

Hinweis
Um die Datenbanken auf dem angegebenen SQL Server anzuzeigen, muss der SQL Server-Browser-Dienst aktiv sein.

*Neben **Datenbankname** wird die ausgewählte Datenbank angezeigt.*

7. Bearbeiten Sie im nächsten Dialog die Optionen für **Scout Board**.[1]

   Geben Sie die Portnummer für den Scout Board-Dienst an und den Computernamen (FQDN) der Maschine, auf der die Datenbankschicht laufen soll. Für weitere Informationen siehe Scout Board installieren im **Scout Board**-Handbuch.

8. Bearbeiten Sie im nächsten Dialog die Optionen für den **Scout Keep Alive-Service**.[2]

   Geben Sie den TCP-Port an.

[1] optionale Komponente, ab Scout 15 2209
[2] optionale Komponente, ab Scout 15 2209

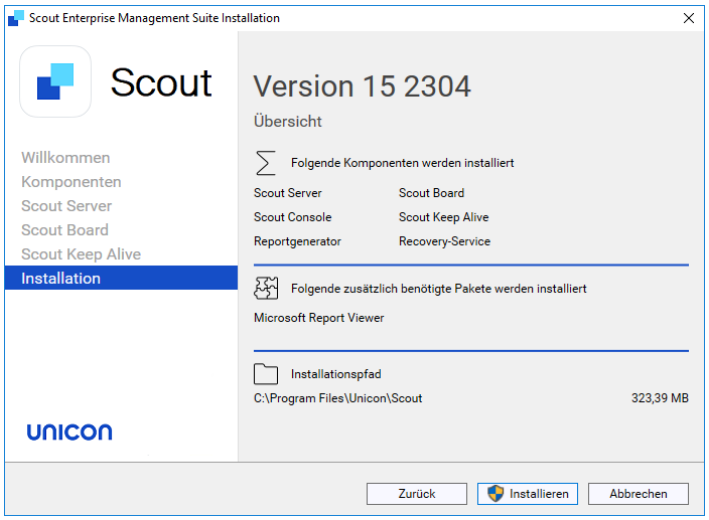
Mit **HTTPS** wird eine sichere Verbindung zum Interface verwendet. Geben Sie ein gültiges SSL-Zertifikat an. Alternativ erstellen Sie direkt aus dem Dialog heraus ein Selfsigned-Zertifikat und kehren anschließend zur Installation der Scout Enterprise Management Suite zurück.

Hinweis

Mit aktualisieren Sie den Inhalt des Listenfeldes und können dann Ihr neu erstelltes Zertifikat auswählen.
Vorhandene Zertifikate werden mit dem zugewiesenen **Friendly name** angezeigt oder, wenn nicht vorhanden bzw. mehrfach vergeben, mit ihrer Seriennummer.

---

9. Überprüfen Sie im letzten Schritt die Übersicht aller Komponenten, die installiert werden sollen. Um die Installation zu starten, klicken Sie auf **Installieren**.



Notwendige Software-Komponenten, die nicht auf dem Zielsystem installiert sind wie Visual C++ Redistributable oder Microsoft Report Viewer werden vom System installiert.

Nach der Installation finden Sie Verknüpfungen für die Scout Console und für das Scout Board auf dem Desktop. In der Scout-Gruppe der Windows Apps-Ansicht finden Sie zusätzlich alle installierten Komponenten wie den Scout Datenbankverbindungseditor.

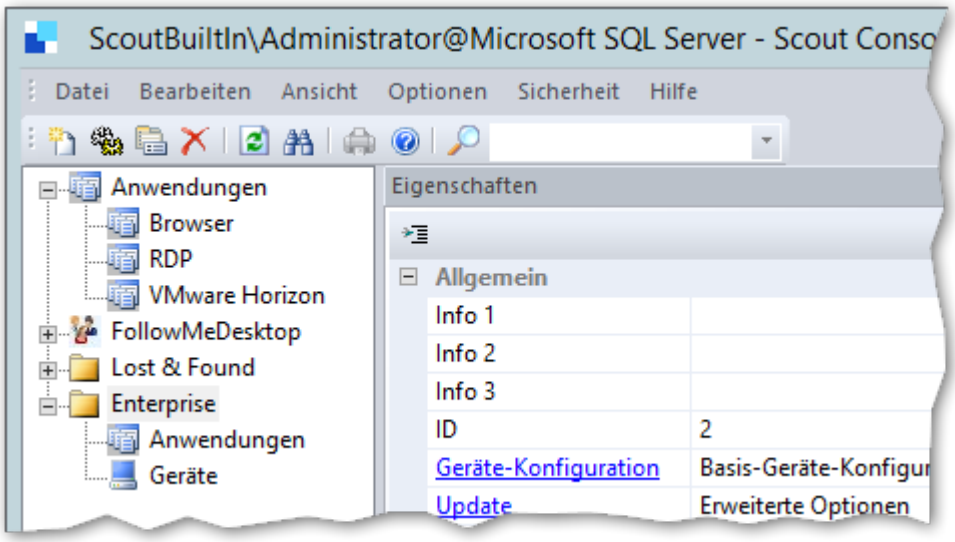
6.3. Nach der Erstinstallation

Die neu installierte Scout Enterprise Management Suite kann ohne Lizenzen für maximal 5 Clients und maximal 3 Monate für Evaluierungszwecke ohne funktionale Einschränkungen verwendet werden. Nach diesem Zeitraum oder für mehr als 5 Clients sind Lizenzen erforderlich.

Nach der Installation mit leerer Scout-Datenbank haben Sie folgende Situation:

- Für die Scout Console steht standardmäßig das Konto `Administrator` mit Kennwort `elux` zur Verfügung.
  - Ändern Sie das Kennwort sofort, um unberechtigten Zugriff zu verhindern:
    - Konsolen-Kennwort ändern oder
    - Administratorenverwaltung aktivieren
- Auf der obersten Ebene sind drei Anwendungen zur Verbindung gegen ein Backend vordefiniert: **RDP**, **VMware Horizon** und der **Firefox**-Browser.
  - Um eine der Anwendungen zu verwenden, passen Sie die Eigenschaften der Anwendungsdefinition an und stellen den Clients die relevante Software über ein IDF zur Verfügung. Für weitere Informationen siehe Anwendungsdefinition.
- In der Scout Console ist bereits die oberste Organisationseinheit (OU) mit Namen **Enterprise** angelegt.
  - Fügen Sie unterhalb davon weitere OUs gemäß Ihrer logischen Unternehmensstruktur hinzu. Für weitere Informationen siehe Organisationsstruktur.

Hinweis: Die Links oben beziehen sich auf das **Scout**-Handbuch.



6.4. Unbeaufsichtigte Installation

Hinweis
Die folgenden Informationen beziehen sich auf die Installation der Scout Enterprise Management Suite Version 15 2302 und höher. Sie beinhalten die Installation von Scout Board und Scout Keep Alive-Service. Informationen zu älteren Versionen[1] finden Sie im Archiv der Download-Seite PDF-Downloads.

Scout Enterprise Management Suite unbeaufsichtigt installieren

- Führen Sie die Datei `ScoutInstaller.exe` mit einem oder mehreren Parametern aus:
  `"ScoutInstaller.exe" /s /v"<Parameter>" /v"<Parameter>"`
  Sie können beliebig viele Parameter anfügen, siehe Tabelle unten.

Befehlszeile für unbeaufsichtigte Installation erstellen lassen

Mit Hilfe einer einmaligen manuellen Installation, die den gewünschten Kriterien entspricht, erstellen Sie eine Batch-Datei für weitere unbeaufsichtigte Installationen.

1. Führen Sie eine manuelle Installation der Scout Enterprise Management Suite mit den gewünschten Komponenten und Optionen durch.
2. Öffnen Sie die während der Installation erstellte Protokolldatei mit einem Texteditor:
   `%LOCALAPPDATA%\Temp\Scout_Enterprise_Management_Suite_<Zeitstempel>.log`
3. Kopieren Sie unter `Silent install command line` die Befehlszeile, die durch die manuelle Installation erzeugt wurde.
4. Erstellen Sie eine Batchdatei, die die kopierte Befehlszeile enthält.

   Kennwörter wurden entfernt und müssen manuell angegeben werden.
5. Ersetzen Sie die Zeichenfolgen `<SET_PASSWORD>` für die Datenbank-Kennwörter durch die jeweiligen Kennwörter im Klartext.
   Wenn Sie verschlüsselte Kennwörter verwenden möchten, fügen Sie an die Parameternamen die Zeichenfolge `_CRYPTED` an, siehe unten.

Liste der Parameter

Die folgenden Tabellen geben einen Überblick über die vorhandenen Parameter und deren mögliche Werte.
Auf der linken Seite werden **Standardwerte fett** dargestellt.

[1] mit Scout Statistikservice und Scout Dashboard

Hinweis
Um Kennwörter zu verschlüsseln, können Sie Umgebungsvariablen verwenden. Für weitere Informationen siehe Werte verschlüsseln.

Parameter für /v

Parameter	Beschreibung
UCPROP_DBTYPE=**2**	`2` - Microsoft SQL Server `5` - Microsoft SQL LocalDB
UCPROP_DBNAME=*Scout*	Name der Scout-Datenbank
UCPROP_DBSERVER=`sqlsrv.sampletec-01.com\sql_12`	Datenbank-Server (und Instanz) der Scout-Datenbank
DB_SCOUT_DB_AUTHENTICATION=`Windows Authentication`	`Windows Authentication` `SQL Server Authentication`
UCPROP_DBUSER=`Scout-Admin`	Nur bei SQL Server-Authentifizierung: SQL-Benutzername für Scout-Datenbank
UCPROP_DBPASSWORD_CRYPTED=*u[D``Gqu[w_*	Nur bei SQL Server-Authentifizierung: Verschlüsseltes Kennwort für Scout-Datenbank, siehe `eluxd.ini`
UCPROP_DBPASSWORD=*My_Password*	Nur bei SQL Server-Authentifizierung: Unverschlüsseltes Kennwort für Scout-Datenbank
UCPROP_SERVICEUSER	Nur bei Windows-Authentifizierung: Windows-Benutzername
UCPROP_SERVICEPASSWORD_CRYPTED	Nur bei Windows-Authentifizierung: Verschlüsseltes Windows-Kennwort
UCPROP_TRUSTSERVERCERTIFICATE=**1**	Dem Datenbank-Server-Zerifikat vertrauen
UCPROP_ENCRYPT=**0**	`0` - Unverschlüsselte ODBC-Verbindung `1` - Verschlüsselte ODBC-Verbindung
UCPROP_MULTISUBNETFAILOVER=**0**	`0` - Standard `1` - Schnelleres Wiederverbinden nach Failover (AlwaysOn Cluster)
UCPROP_DBCREATE=**0**	`0` - Scout-Datenbank wird nicht neu erstellt `1` - Scout-Datenbank wird neu erstellt

Parameter	Beschreibung
UCPROP_LANGUAGE=`1`	Anzeige-Sprache `0` - Deutsch `1` - Englisch Wenn der Parameter nicht gesetzt ist, wird die im Betriebssystem eingestellte Sprache verwendet.
RUNSCOUTSERVICE=**true**	`true` - Die Scout-Dienste werden während der Installation gestartet `false` - Die Scout-Dienste werden nicht gestartet
Voreinstellungen für die Geräte (Basis-Geräte-Konfiguration)	
UCPROP_DESKTOP_LANGUAGE=`en_US`	Anzeige-Sprache für den Desktop
UCPROP_KEYBOARD_LANGUAGE=`en`	Tastatursprache
UCPROP_TIMEZONE=`US/Eastern`	Zeitzone
Komponenten	

ADDLOCAL=
`Server,Console,Report`
	Nur die angegebenen Scout-Komponenten werden installiert.
	`CommonFeature`
	`Server`
	`Console`
	`Recovery`
	`Elias`
	`Report`

INSTALL_SCOUT_FEATURE=**1**	`0` - Scout-Komponenten werden nicht installiert `1` - Scout-Komponenten werden installiert (wie in ADDLOCAL definiert)
INSTALL_SCOUTBOARD_FEATURE=**1**	`0` - Scout Board wird nicht installiert `1` - Scout Board wird installiert
INSTALL_SCOUTKEEPALIVE_FEATURE=**1**	`0` - Scout Keep Alive-Service wird nicht installiert `1` - Scout Keep Alive-Service wird installiert
Scout Board	
UCPROP_SCOUTBOARD_HOST=`scout.sampletec-01.com`	Computername (FQDN) der Maschine, auf der die Datenbankschicht laufen soll
UCPROP_SCOUTBOARD_PORT=`22160`	Port-Nummer für den Scout Board-Dienst

UCPROP_SCOUTBOARD_DBLAYER_ADDRESS=`tcp://scout.sampletec-01.com:22150`	Adresse der Scout Board-Datenbankschicht
UCPROP_SCOUTBOARD_DBLAYER_ADDRESS_PUBLISH=`scout.sampletec-01.com:22151`	Öffentliche Adresse der Scout Board-Datenbankschicht

Scout Keep Alive-Service

UCPROP_SCOUTKEEPALIVE_DBSERVER=`sqlsrv.sampletec-01.com`	Datenbank-Server (und Instanz) für die Keepalive-Daten Diese werden normalerweise in der Scout-Datenbank, können aber auch in einer eigenen Datenbank gespeichert werden.
UCPROP_SCOUTKEEPALIVE_DBUSER	
UCPROP_SCOUTKEEPALIVE_DBNAME=`Scout`	
UCPROP_SCOUTKEEPALIVE_DBPASSWORD	
UCPROP_SCOUTKEEPALIVE_AUTHENTICATION=`Windows`	`Windows` `SQL Server`
UCPROP_SCOUTKEEPALIVE_SERVICEUSER	
UCPROP_SCOUTKEEPALIVE_SERVICEPASSWORD	
UCPROP_SCOUTKEEPALIVE_TRUSTSERVERCERTIFICATE=**1**	
UCPROP_SCOUTKEEPALIVE_ENCRYPT=**0**	
UCPROP_SCOUTKEEPALIVE_MULTISUBNETFAILOVER=**0**	
UCPROP_SCOUTKEEPALIVE_CERTIFICATES=CREATESELFSIGN	Zertifikatname oder automatisch erstelltes Self-signed-Zertifikat
UCPROP_SCOUTKEEPALIVE_PORT-T=22124	Port-Nummer für den Scout Keep Alive-Service

Weitere Parameter

/s	Die Installation wird unbeaufsichtigt durchgeführt (silent).
/uninstall	Die Scout Enterprise Management Suite wird deinstalliert.
/l "%PUBLIC%\Documents\UniCon\scoutlog.txt"	Die Protokolldatei wird auf die angegebene Datei umgeleitet.

Beispiel für eine unbeaufsichtigte Installation

```
ScoutInstaller.exe /s /v"UCPROP_DBTYPE=2" /v"UCPROP_DBNAME=Scout"
/v"UCPROP_DBSERVER=sqlsrv.sampletec-01.com\sql_12"
/v"DB_SCOUT_DB_AUTHENTICATION=SQL Server Authentication"
/v"UCPROP_DBUSER=Scout-Admin"
/v"UCPROP_DBPASSWORD_CRYPTED=u[D``Gqu[w_" /v"UCPROP_DESKTOP_LANGUAGE=de"
/v"INSTALL_SCOUTBOARD_FEATURE=1"
/v"UCPROP_SCOUTBOARD_HOST=scout.sampletec-01.com"
/v"UCPROP_SCOUTBOARD_PORT=22160"
/v"UCPROP_SCOUTBOARD_DBLAYER_ADDRESS=tcp:/scout.sampletec-01.com:22150"
/v"UCPROP_SCOUTBOARD_DBLAYER_ADDRESS_PUBLISH=tcp://scout.sampletec-
01.com:22151"
/v"ADDLOCAL=CommonFeature,Server,Console,Recovery,Report"
/v"INSTALL_SCOUTKEEPALIVE_FEATURE=0"
/v"INSTALLDIR=C:\Program Files\Unicon\Scout"
```

Hinweis
Indem Sie eine beaufsichtigte Installation mit den relevanten Parametern durchführen, wird die Datei `eluxd.ini` im Scout Server-Verzeichnis angelegt. Diese Datei enthält Scout-Werte, die Sie verwenden können.

Unbeaufsichtigte Deinstallation durchführen

- Verwenden Sie folgenden Befehl:
  `"ScoutInstaller.exe" /s /uninstall`

6.5. Auf neuere Version aktualisieren

Eine bestehende Scout Enterprise Management Suite-Installation kann in wenigen Schritten auf eine neuere Version aktualisiert werden.

1. Führen Sie ein vollständiges Datenbank-Backup für Ihre Scout-Datenbanken durch.

   Für weitere Informationen zur Sicherung einer LocalDB siehe SQL LocalDB vor der Installation von Updates sichern.

2. Laden Sie die aktuelle Version der Scout Enterprise Management Suite als `.zip`-Datei von unserem Portal myelux.com herunter.
3. Entpacken Sie die `.zip`-Datei und stellen Sie die Installationsdatei auf einer lokalen Festplatte bereit.
4. Führen Sie die Datei `ScoutInstaller.exe` als Administrator aus.
5. Folgen Sie den Anweisungen des Installations-Assistenten. Geben Sie Ihre vorhandenen Scout-Datenbanken an.

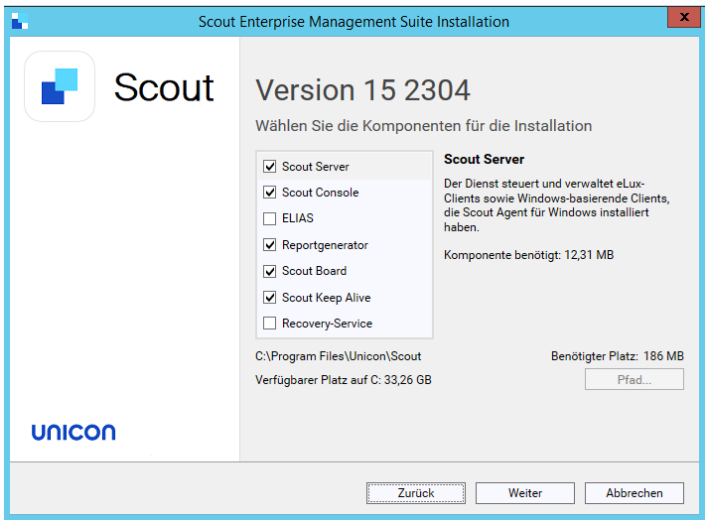
Abhängig vom Funktionszuwachs können beim Update auf eine neue Version längere Laufzeiten bei der Konvertierung der Scout-Datenbank entstehen.

> **Achtung** Um auf Scout 15 2204 oder eine höhere Version zu aktualisieren, muss die Absprungbasis für ein Update Scout 15.2.0 oder höher sein. Ältere Datenbanken können nicht konvertiert werden und werden vom Installer nicht akzeptiert.

6.6. Scout Enterprise Management Suite-Installation ändern

Programm-Komponenenten nachinstallieren oder installierte Komponenten de-installieren

1. Verwenden Sie die Systemsteuerung (Apps und Features) oder führen Sie die Installationsdatei `ScoutInstaller.exe` als Administrator aus.
2. Wählen Sie im Installations-Dialog die Option **Ändern**. Die installierten Komponenten werden mit einem Haken angezeigt.



3. Aktivieren Sie die Komponenten, die Sie installieren möchten oder deaktivieren Sie die Komponenten, die Sie deinstallieren möchten.

Hinweis
Wenn Sie eine der installierten Komponenten deaktivieren, wird diese Komponente deinstalliert.

Installation reparieren

1. Verwenden Sie die Systemsteuerung (Apps und Features) oder führen Sie die Installationsdatei `ScoutInstaller.exe` als Administrator aus.
2. Wählen Sie im Installations-Dialog die Option **Reparieren**.

Die Scout Enterprise Management Suite wird auf fehlende Dateien, Verknüpfungen und Registry-Einstellungen überprüft und ggf. repariert.

6.7. Scout Enterprise Management Suite deinstallieren

1. Verwenden Sie die Systemsteuerung (Apps und Features) oder führen Sie die Installationsdatei `ScoutInstaller.exe` als Administrator aus.
2. Wählen Sie im Installations-Dialog die Option **Deinstallieren**.

7. Installation: eLux-Container

Hinweis
Wenn Sie den Web-basierten ELIAS 18 einsetzen, entfällt die Container-Installation. In ELIAS 18 importieren Sie einfach die relevanten Software-Pakete oder das `AllPackages`-Bundle. Für weitere Informationen siehe Software-Pakete importieren im **ELIAS 18**-Handbuch.

Der eLux-Container ist eine Zusammenstellung von Software-Paketen, die für die Client-Firmware (IDF) zur Auswahl stehen. Der Administrator wählt eine Untermenge aus dem Paketpool und definiert damit die Imagedefinitionsdatei zur Installation der Pakete am Client.

Die Software-Pakete können mit Hilfe der Container-Installation auf einem Web- oder FTP-Server bereitgestellt werden (klassischer ELIAS) oder über den ELIAS18-Web-Service in einer MongoDB (lokal oder in Kombination mit IIS).

Für die eLux Hauptversionen ist jeweils ein eigener Container vorgesehen. Aktuelle eLux RP 6 / 64-Bit-Versionen werden unter `...\eluxng\UC_RP6_X64` installiert.

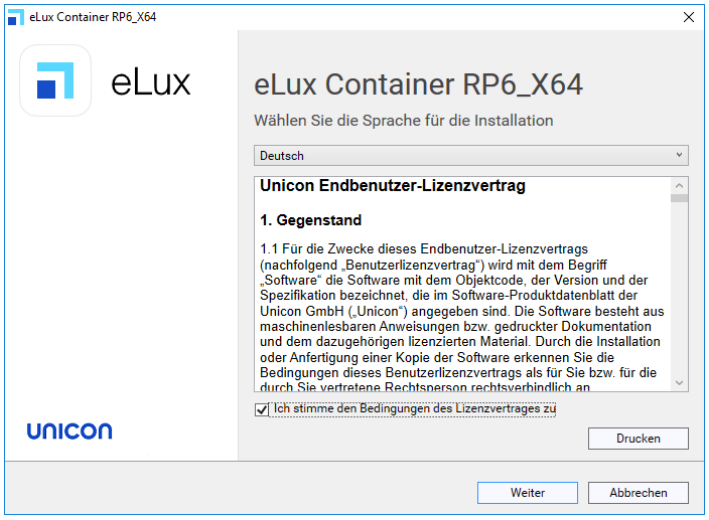
7.1. Container installieren

- nur bei Verwendung des klassischen ELIAS -

Die folgende Anleitung beschreibt die Installation eines Containers inklusive aller Software-Pakete, die für die gewählte Betriebssystem-Variante auf unserem Portal zur Verfügung stehen.

Hinweis
Lesen Sie vor der Installation die Kapitel Systemvoraussetzungen und "Vorbereitung der Installation" auf Seite 20.

1. Führen Sie die Datei `eLuxContainer.exe`[1] als Administrator von einem lokalen Laufwerk aus.



[1] Entpacktes Allpackages-Archiv

2. Wählen Sie die Sprache für die Installation. Lesen Sie anschließend die Lizenzvereinbarung und stimmen Sie zu.
3. Wählen Sie den Typ des Servers, den Sie als Quell-Server für die Firmware-Updates einsetzen:
   - `HTTP`
   - `FTP`
4. Geben Sie die Zugriffsdaten für den HTTP- oder FTP-Server an:

Option	Beschreibung	Beispiel
Root-Verzeichnis	Stammverzeichnis des Servers, lokal oder auf einem Netzlaufwerk	`W:\inetpub\wwwroot` `C:\Programme\inetpub\ftproot`
URL	vollständiger URL für den Zugriff auf den Server	`http://update.sampletec-01.com` `ftp://update.sampletec-01.com`

5. Wenn Sie FTP verwenden, geben Sie zusätzlich die Anmeldedaten ein:

Option	Beispiel
Benutzername	`anonymous`
Kennwort	`elux@sampletec-01.com`

Der letzte Dialog zeigt den benötigten Festplattenspeicher an.

6. Starten Sie die Installation.

   Auf dem Web- oder FTP-Server wird das Verzeichnis `UC_RP6_X64` als eLux RP 6-Container erstellt. Die Datei `container.ini` und die Software-Pakete (`.epm`, `.fpm` und Signatur-Dateien) werden im Container verfügbar gemacht. Sie können jetzt in ELIAS eine Image-Datei erstellen.

7. Wenn die Scout Enterprise Management Suite bereits installiert ist, stellen Sie die Verbindung der Scout Console zum eLux-Container in ELIAS her: Wählen Sie in der Scout Console **Optionen > ELIAS-Einstellungen...** und wählen Sie den Pfad zu dem soeben erstellten Container auf dem Web-/FTP-Server.

7.2. Auf neuere Version aktualisieren

- nur bei Verwendung des klassischen ELIAS -

Eine Anpassung des eLuxContainers kann erforderlich werden, wenn eine neue Betriebssystem-Version oder Fixes angeboten werden, oder wenn neue Versionen der Client-Anwendungen verfügbar sind.

Auf neuere Haupt- oder Nebenversion aktualisieren

Neue Haupt- oder Nebenversionen von eLux werden im Rahmen von Releases auf unserem Portal angeboten.

- Führen Sie eine Container-Installation mit dem neuesten `Allpackages`-Bundle durch.

Wenn Sie auf eine neue Hauptversion aktualisieren, wird ein neuer Container (Beispiel: `UC_RP6_X64`) erstellt, in den die Software-Pakete der neuen eLux-Version installiert werden.
Wenn Sie auf eine neue Nebenversion aktualisieren, wird der vorhandene Container durch die neuen Software-Pakete ergänzt. Die vorhandenen Software-Pakete bleiben erhalten.

Einzelne Software-Pakete aktualisieren

1. Laden Sie das gewünschte Paket als `.zip`-Datei von unserem Portal aus dem relevanten Container herunter.

   Aus den **Details** *der Pakete im Container geht die relevante Funktionserweiterung des Paketes und die Historie hervor.*

2. Importieren Sie die `.zip`-Datei in Ihren eLux-Container. Verwenden Sie dazu die ELIAS-Funktion **Container > Paket importieren**. Für weitere Informationen siehe Pakete in einen Container importieren im ELIAS-Handbuch.

7.3. eLux-Container deinstallieren

- nur bei Verwendung des klassischen ELIAS -

1. Verwenden Sie die Systemsteuerung oder führen Sie die Installationsdatei `eLuxContainer.exe` als Administrator aus.
2. Wählen Sie im Installations-Dialog die Option **Deinstallieren** und klicken Sie auf **Weiter**.

8. Installation: ELIAS 18

Hinweis
In ELIAS 18 verwalten Sie die eLux-Software-Pakete für Ihre Firmware-Images. Die ELIAS 18-Installation ersetzt die Container-Installation und den klassischen ELIAS aus früheren Versionen.

ELIAS 18 ist ein Webdienst, der stand-alone betrieben werden kann oder in Kombination mit Microsoft IIS.[1] ELIAS 18 kann unter Windows oder unter Linux betrieben werden.

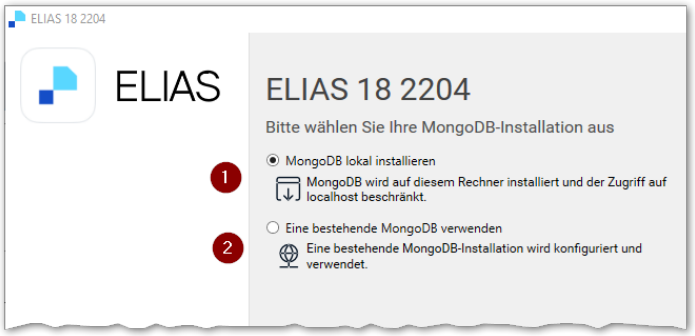
ELIAS 18 ist Plattform-unabhängig und bietet mehr Funktionalität und Komfort als der klassische ELIAS. Für weitere Informationen siehe Überblick im **ELIAS 18**-Handbuch.

8.1. ELIAS 18 installieren / Windows

Hinweis
Lesen Sie vor der Installation die Kapitel:

- "Systemvoraussetzungen" auf Seite 6 und
- Vorbereitung der Installation

1. Führen Sie die Datei `EliasInstaller.exe` als Administrator aus.
2. Wählen Sie die Sprache für die Installation. Lesen Sie anschließend die Lizenzvereinbarung und stimmen Sie zu.
3. Wählen Sie, ob Sie MongoDB lokal installieren oder eine vorhandene MongoDB-Installation verwenden möchten.



1	Die Datenbank ist nur auf dem lokalen Computer verfügbar.
2	Um eine vorhandene MongoDB-Installation zu nutzen, geben Sie im nächsten Schritt die MongoDB-Verbindungsdaten an.

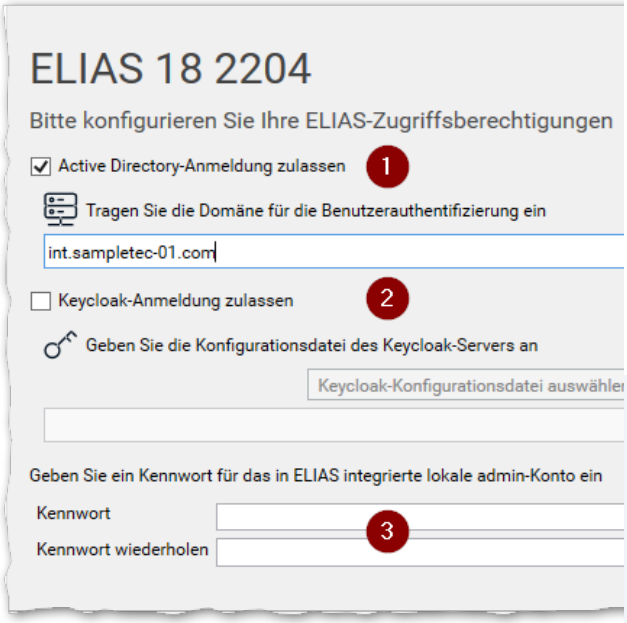
Beachten Sie für eine **vorhandene** MongoDB-Installation:

[1] Andere Webserver können eingesetzt werden, jedoch ohne Unterstützung für die Konfiguration.

- Wenn Ihre Administratoren von mehreren Webservern auf die gleiche MongoDB-Installation zugreifen sollen, verwenden Sie unterschiedliche Datenbanken innerhalb der MongoDB-Installation.
- Geben Sie die MongoDB-Serveradresse mit Port und die Anmeldedaten an. Je nach Konfiguration Ihrer MongoDB-Installation geben Sie zusätzliche Optionen an, beispielsweise um auf ein bestimmtes Replicaset mit Timeout zu verbinden. MongoDB erstellt aus allen Angaben eine URL zur Verbindung auf die Datenbank. Für weitere Informationen siehe https://docs.mongodb.com/manual/reference/connection-string/

Hinweis
Ab ELIAS 18 2104 werden alle Container in einer Datenbank gespeichert. Dadurch können später zusätzliche Container unabhängig vom Datenbank-Benutzer erstellt werden. Das Datenbank-Präfix entfällt.

4. Geben Sie im nächsten Schritt einen Namen für Ihre ELIAS-Datenbank ein.
5. Legen Sie danach Ihre ELIAS-Zugriffsregelung fest:

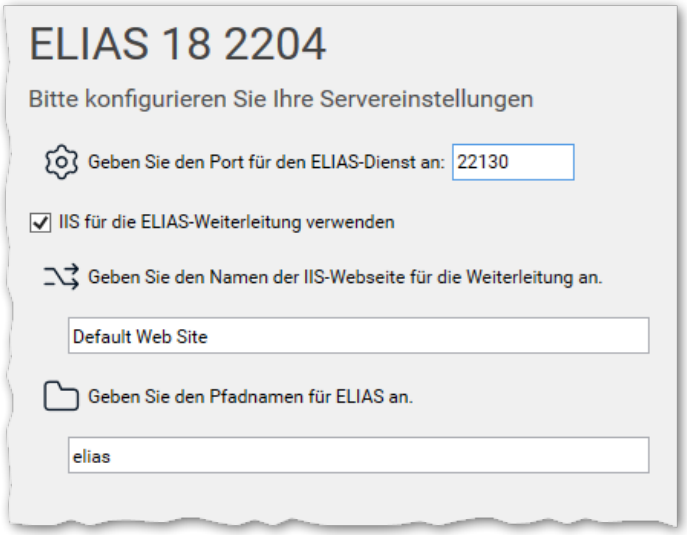


1	AD-Domäne für Benutzer-Authentifizierung über Active Directory Beispiel: `int.sampletec-01.com` Die Domänen-Benutzer müssen in einer speziellen AD-Gruppe registriert sein. Für weitere Informationen siehe Zugriffsverwaltung über AD im **ELIAS 18**-Handbuch.
2	Konfigurationsdatei des Keycloak-Servers für Keycloak-Anmeldung[1] Beispiel: `C:\install\ELIAS\keycloak.json` Für weitere Informationen siehe Zugriffsverwaltung über Keycloak im **ELIAS 18**-Handbuch.
3	Kennwort für den lokalen **admin**-Account

Beachten Sie, dass sich die Felder **Domäne** und **Kennwort** auf zwei verschiedene Anmeldearten beziehen. Für weitere Informationen siehe Zugriffsverwaltung und Anmeldung im **ELIAS 18**-Handbuch.

[1]Wenn Sie die Keycloak-Konfigurationsdatei nach der Installation einfügen, starten Sie anschließend den ELIAS-Dienst neu.

6. Konfigurieren Sie die Webserver-Einstellungen:



   Wenn Sie kein IIS auf Ihrem System haben, wird der ELIAS-Webdienst standardmäßig auf Port 80 installiert.

   Wenn IIS auf dem System installiert ist, aktivieren Sie die Option **IIS für ELIAS-Weiterleitung verwenden**. In diesem Fall wird ELIAS auf Port 22130 installiert, um Konflikte mit dem Webserver-Port 80 zu vermeiden. Um ELIAS über die Standard-Ports 80/443 zu erreichen, wird der Dienst mit Hilfe des Reverse-Proxy-Verfahrens und des angegebenen Unterverzeichnisses registriert.
   Geben Sie den Webseitennamen und einen Pfadnamen für ELIAS an.

   Für die Nutzung von HTTPS muss ein externer Webserver wie IIS verwendet werden. Die Bindung der Webseite auf Port 443 muss definiert sein.

   Hinweis
   Um Ihre Clients für Firmware-Updates zu konfigurieren, geben Sie den hier definierten Pfadnamen im **Firmware**-Register der Client-Geräte-Konfiguration in der Scout Console an.

7. Bestätigen oder ändern Sie den Installationspfad.
8. Um die Installation zu starten, klicken Sie auf **Installieren**.

*Nach der Installation finden Sie ein **ELIAS**-Symbol auf dem Desktop, das die URL Ihrer ELIAS 18-Installation enthält. Doppelklicken Sie, um ELIAS im Standard-Browser zu öffnen.*

Cross-Origin-Requests

Nach der ELIAS 18-Installation ist Cross-Origin Resource Sharing (CORS) aus Sicherheitsgründen nur aus dem Netzwerk des Installations-Servers (FQDN) erlaubt. Dieser wird während der Installation unter **allowedOrigins** eingetragen. Administratoren außerhalb dieses Netzwerks können nicht auf die Installation zugreifen.

- Um die Zugriffsmöglichkeiten zu erweitern, fügen Sie weitere Server mit ihrem FQDN in der Konfigurationsdatei `config.json` unter **allowedOrigins** hinzu. Ports werden nach dem

Servernamen mit Doppelpunkt angehängt. Trennen Sie mehrere Einträge durch Kommata.

Mit Hilfe des Wildcard-Zeichens ***** können Sie auch globalen Zugriff konfigurieren. Dies empfehlen wir jedoch aus Sicherheitsgründen nicht. Beispiel: `"allowedOrigins": ["*"],`

8.2. ELIAS 18 installieren / Linux

- Die folgende Anleitung bezieht sich auf ELIAS 18 2209 oder höher -

ELIAS 18 kann auch in einer Linux-Umgebung betrieben werden. Dazu steht ein Debian-Paket (`.deb`) zur Verfügung, das mit Ubuntu 20.04 getestet wurde.

Voraussetzung
Eine MongoDB-Datenbank muss entweder lokal oder remote verfügbar sein. Die Datenbank benötigt ausreichenden Festplattenspeicher für die Container-Verwaltung, siehe auch "Systemvoraussetzungen" auf Seite 6.

1. Laden Sie von unserem Portal myelux.com unter **Downloads > Scout > ELIAS** das Debian-Paket **ELIAS 18** *<Version>* **für Linux** herunter.
2. Installieren Sie das Debian-Paket mit Hilfe entsprechender Paketverwaltungswerkzeuge (Debian/Ubuntu).

   Beispiel: `sudo apt install ./elias-paket.deb`

   Die Dateien werden nach `/opt/unicon/elias` *installiert.*
3. Um die Anbindung an MongoDB und den Webdienst zu konfigurieren (Backend-Konfiguration), bearbeiten Sie die Datei `/opt/unicon/elias/server.json`:[1]

Option	Beschreibung	Standard/Beispiel
"server"	MongoDB-Servername (als FQDN oder IP-Adresse) Für eine lokale Installation verwenden Sie `"localhost"`. Fügen Sie die Port-Nummer nach einem Doppelpunkt an den Servernamen an.	`"localhost:27017"`
"mongoUser"	MongoDB-Benutzername Wenn Sie keine Anmeldedaten verwenden, setzen Sie eine leere Zeichenfolge.	`""`

[1] Diese Datei bleibt lokal.

Option	Beschreibung	Standard/Beispiel
"mongoPassword"	MongoDB-Kennwort Wenn Sie keine Anmeldedaten verwenden, setzen Sie eine leere Zeichenfolge.	`""`
"mongoPasswordEncrypted"	Verschlüsseltes MongoDB-Kennwort	false
"mongoOptions"	optional: Zusätzliche MongoDB-Optionen	
"adminPassword"	Verschlüsseltes Kennwort für den lokalen **admin**-Account Um Kennwörter zu verschlüsseln, verwenden Sie das **bcrypt**-Verfahren mit 13 Runden.	`"elias"`
"adGroup"	AD-Gruppe, in der AD-Benutzer für die Anmeldung Mitglied sein müssen Für weitere Informationen über die Anmeldearten siehe Zugriffsverwaltung und Anmeldung im **ELIAS 18**-Handbuch.	`"ELIAS"`
"logLevel"	Protokollstufe (debug | info | warn | error)	`"debug"`
"port"	Port, der von der ELIAS-API verwendet wird	`"22130"`
"iisWebsite"	Webseitenname für IIS-Weiterleitung, wird unter Linux nicht verwendet	–

Hinweis
Um ELIAS mit Zugriffsverwaltung über Keycloak zu konfigurieren, siehe Zugriffsverwaltung über Keycloak im **ELIAS 18**-Handbuch.

4. Um das Frontend zu konfigurieren, bearbeiten Sie die Datei `/opt/unicon/elias/config.json`:

Option	Beschreibung	Standard/Beispiel
"pollingInterval"	Intervall in Millisekunden für das Pollen der API durch die Oberfläche	`3000`

Option	Beschreibung	Standard/Beispiel
"api"	Hostname des Gerätes, auf dem ELIAS läuft (FQDN oder IP-Adresse)	"*<Hostname>*"
"domain"	AD-Domäne für Benutzer-Authentifizierung Die Domänenbenutzer müssen in einer speziellen AD-Gruppe registriert sein. Wenn Sie eine leere Zeichenfolge setzen, ist nur der lokale **admin**-Account verfügbar.	""
"redirectPath"	Pfad, der zur API weiterleitet (beispielsweise, wenn Apache eingesetzt wird) Muss auf `api` enden	"`api`"

Hinweis
Dieser Pfad muss auch in der Scout Console im **Firmware**-Register der Client-Geräte-Konfiguration angegeben werden.

"protocol"	"http" oder "https"	"`http`"
"apiVersions"	Muss auf `["1.0"]` gesetzt werden	`["1.0"]`
"base.database"	Name für Ihre ELIAS-Datenbank In dieser Datenbank werden alle Container gespeichert.[1]	"`ELIAS-Database`"
"port"	Port, auf dem die ELIAS-Webseite von außen erreichbar ist	"`8080`"
"allowedOrigins"	Liste von URLs, über die die ELIAS-Webseite erreichbar sein soll (durch Komma getrennt) Beispiel: "`http://`*<Hostname oder IP-Adresse>*`:8080`"	

5. Starten Sie den ELIAS-Service neu.

   Beispiel: `sudo systemctl restart scout-enterprise-elias`

Reverse-Proxy für Webserver

Aus Performance- oder Sicherheitsgründen können Sie einen einfachen Reverse-Proxy konfigurieren, der die SSL-Verschlüsselung und -Entschlüsselung übernimmt. Eine Konfiguration für **Apache** könnte aussehen wie folgt:

[1] ab ELIAS 18 2104

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName elias.dev.sampletec-01.com
    ProxyPreserveHost Off
    ProxyRequests off
    SSLProxyEngine On
    <Proxy *>
        Require all granted
    </Proxy>
    ProxyPass / http://localhost:22130/
    ProxyPassReverse / http://localhost:22130/

# Insert your certificate file names:
SSLCertificateFile /etc/ssl/private/ca-certificate.crt.pem
SSLCertificateKeyFile /etc/ssl/private/ca-certificate.key.pem

SSLEngine on

# Intermediate configuration, tweak to your needs:
SSLProtocol             all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-
ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-
CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
SSLHonorCipherOrder     off
SSLSessionTickets       off

SSLOptions +StrictRequire

# Add vhost name to log entries:
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"" vhost_combined
LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost_common

</VirtualHost>
</IfModule>
```

Passen Sie die Daten wie Servername und Zertifikatsdateien an Ihre Konfiguration an.

Wir empfehlen außerdem, eine zweite Konfigurationsdatei zu erstellen, um die Kommunikation, die über Port 80 unverschlüsselt ankommt, auf Port 443 umzuleiten. Beispiel:

```
<VirtualHost *:80>
RewriteEngine on
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
```

Passen Sie die Daten wieder an Ihre Konfiguration an.

Damit die Konfigurationsdateien ausgeführt werden, gehen Sie folgendermaßen vor:

1. Kopieren Sie Ihre **.conf**-Dateien nach `/etc/apache2/sites-available`
2. Machen Sie sie verfügbar in `/etc/apache2/sites-enabled`
   beispielsweise mit `a2ensite <filename>.conf`
   oder per Symlink, beispielsweise `ln -s sites-available/<filename>.conf sites-enabled/<filename>.conf`
3. Starten Sie den Webserver neu:
   `systemctl reload apache2`

8.3. ELIAS 18 starten

Hinweis
Die ELIAS 18-Installation wurde erfolgreich durchgeführt. Für weitere Informationen siehe Installation: ELIAS 18 im **Installations**-Handbuch.

Die URL, mit der Sie ELIAS in Ihrem Web-Browser aufrufen, bezieht sich auf den installierten ELIAS-Webdienst.

Ohne IIS:

- Geben Sie im Web-Browser folgende URL ein:
  `http://<Hostname>:<Port-Nummer>` oder
  `https://<Hostname>:<Port-Nummer>`

  `<Hostname>` bezieht sich auf den Computernamen oder die IP-Adresse des Computers, auf dem ELIAS installiert ist.

  `<Port-Nummer>` bezieht sich auf den Port, den Sie für den ELIAS-Webdienst angegeben haben.

Mit IIS-Weiterleitung:

- Geben Sie im Web-Browser folgende URL ein:
  `http://<Hostname>/path` oder
  `https://<Hostname>/path`

  `<Hostname>` bezieht sich auf den Computernamen oder die IP-Adresse des Computers, auf dem ELIAS installiert ist bzw. auf Ihren Webserver.

  `<Pfad>` ist der angegebene ELIAS-Pfadname unter Ihrer Webseite (`elias` im Beispiel oben)

Hinweis
Auf dem Computer, auf dem ELIAS installiert ist, finden Sie ein ELIAS-Desktop-Symbol.

Für den Zugriff aus anderen Netzwerken, siehe Installation: ELIAS 18 im **Installations**-Handbuch.

8.4. Auf neuere ELIAS-Version aktualisieren

Eine bestehende ELIAS 18-Installation kann in wenigen Schritten auf eine neuere Version aktualisiert werden.

Hinweis
Ab ELIAS 18 2104 werden alle Container in einer Datenbank gespeichert. Wenn Sie mehrere Container in einer älteren ELIAS 18-Installation verwalten, werden bei der Update-Installation die entsprechenden Datenbanken zu einer Datenbank zusammengeführt.

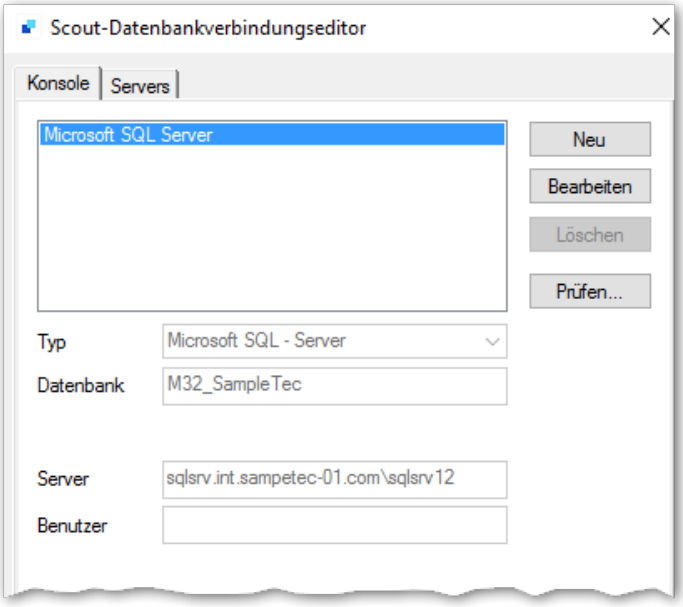
1. Laden Sie die aktuelle ELIAS 18-Version als `.zip`-Datei von unserem Portal myelux.com herunter (**Download > Scout > ELIAS**).

2. Entpacken Sie die `.zip`-Datei und stellen Sie die Installationsdatei auf einer lokalen Festplatte bereit.
3. Führen Sie die Datei `EliasInstaller.exe` als Administrator aus und folgen Sie den Anweisungen des Installations-Assistenten.

9. Datenbank-Verbindungen

Die Scout-Datenbank wird bei der Installation der Scout Enterprise Management Suite angegeben. Nach der Installation können die Datenbankverbindungen überprüft und bearbeitet werden.

Für den Scout Server und die Scout Console können Sie eine oder mehrere Verbindungen zur Scout-Datenbank mit Hilfe des **Scout-Datenbankverbindungseditors** definieren. Den Datenbankverbindungseditor finden Sie als eigenständiges Programm in der Scout-Gruppe der Windows Apps-Ansicht.



10. Zertifikate

Verschiedene Anwendungen und Funktionen erfordern die Bereitstellung von Zertifikaten.
Für (Root-)Zertifikate auf der Client-Seite gilt folgendes:

- Wenn nicht anders angegeben, müssen die Zertifikate Base64-kodiert (ASCII) sein mit Dateierweiterung `.crt`.
- Um die Zertifikate auf die Geräte zu übertragen, verwenden Sie die Scout-Funktion **Konfigurierte Dateiübertragung**. Für weitere Informationen siehe Konfigurierte Dateiübertragung im **Scout**-Handbuch.
- Die Zertifikate werden lokal am Client im Zertifikatsstore `/setup/cacerts/` oder einem Unterverzeichnis gespeichert.

Die folgende Tabelle gibt einen Überblick:

Funktion	Komponente	Verzeichnis
Smartcard-Benutzeranmeldung Die Zertifikate werden in der Scout Console unter **Sicherheit > Benutzerauthentifizierung > Zertifikate** angegeben	Benutzerauthentifizierung / AD+Smartcard	/setup/cacerts/login
Sichere Verbindung (TLS)	Firefox	/setup/cacerts/browser[1]
Sichere Verbindung (TLS)	Chromium	/setup/cacerts/browser
Sichere Verbindung (TLS)	Builtin-Browser Kiosk-Modus	/setup/cacerts/browser
Sichere Verbindung (TLS)	Citrix Workspace app	/setup/cacerts/ und /setup/cacerts/intcerts
Sichere Verbindung (TLS)	VMware Horizon client	/setup/cacerts/
Sichere Verbindung (TLS)	eLuxRDP	/setup/cacerts
Netzwerkanmeldung	WLAN drivers / WPA-Supplikant (802.1X) X509/Radius Network Access Control / SCEP	/setup/cacerts/ /setup/cacerts/scep
VPN / OpenVPN	BaseOS	/setup/openvpn

[1] In früheren Versionen wurde auch `/setup/cacerts/firefox` verwendet.

Funktion	Komponente	Verzeichnis
VPN / Cisco AnyConnect	Cisco AnyConnect	/setup/cacerts/[1] und /setup/cacerts/client
Firmware-Update mit Zertifikatsprüfung	BaseOS	/setup/cacerts

Hinweis
StoreFront kann über eine Citrix-Verbindung oder über einen Browser aufgerufen werden.

[1] eLux-Versionen < eLux RP 6 2302 benötigen das Zertifikat in `/setup/cacerts/ca`

10.1. Zertifikat für Scout Keep Alive-Service

Die Kommunikation zwischen eLux und dem Scout Keep Alive-Service erfolgt über HTTPS. Daher wird zur Installation des Scout Keep Alive-Service ein gültiges Zertifikat mit dem Zweck Serverauthentifizierung benötigt und standardmäßig an den Port 22124 gebunden.

Sobald ein Zertifikat seine Gültigkeit verliert, muss ein neues Zertifikat an den Port gebunden werden, damit der Scout Keep Alive-Service weiter funktioniert. Verwenden Sie hierzu das `netsh.exe`-Tool der Windows-Kommandozeile auf dem System, auf dem der Scout Keep Alive-Service installiert ist.

Hinweis
Wenn der Computer über mehr als eine Netzwerkkarte verfügt, muss die Zertifkatsbindung für alle IP-Adressen durchgeführt werden.

Anzeigen der aktuellen SSL-Zertifikatsbindungen

1. Rufen Sie die Kommandozeile auf.
2. Geben Sie folgendes Kommando ein:

```
netsh.exe http show sslcert
```

Alle Ports, die eine Zertifikatsbindung haben, werden mit den relevanten Informationen gelistet.

SSL-Zertifikat aus Port löschen

1. Rufen Sie die Kommandozeile auf.
2. Verwenden Sie das `netsh.exe`-Tool, wie in folgendem Beispiel gezeigt:
   `netsh.exe http delete sslcert ipport=<IP-Adresse des Computers>:22124`

Anzeigen der Thumbprints (Fingerabdrücke) von Zertifikaten

Hinweis
Der Thumbprint oder Fingerabdruck entspricht dem certificate hash value.

1. Rufen Sie die Powershell auf.
   Beachten Sie, dass der Befehl nicht in der normalen Kommandozeilenschnittstelle (cmd) unterstützt wird.
2. Geben Sie in Abhängigkeit des Zertifikatspeichers folgenden Befehl ein:
   `dir cert:\LocalMachine\My`

Für die in der Microsoft Management Console unter Local Computer\Personal vorhandenen Zertifikate mit und ohne Bindung werden die Thumbprints angezeigt.

Neues SSL-Zertifikat an Port binden

1. Rufen Sie die Kommandozeile auf.
2. Verwenden Sie das `netsh.exe`-Tool mit folgendem Befehl:
   `netsh.exe http add sslcert ipport=0.0.0.0:22124 certhash=<Thumbprint Ihres Zertifikates> appid={957ba029-e2a1-4a13-b426-645a5e3802e2}`

   Der `ipport`-Parameter gibt die IP-Adresse und die Port-Nummer an.

   Der `certhash`-Parameter gibt den Thumbprint (Fingerabdruck) des Zertifikats an.

   Der `appid`-Parameter ist die ID des Scout Keep Alive-Service und darf nicht geändert werden.

11. Management-Protokoll

Die Kommunikation zwischen Scout Server und den eLux Clients kann über Port 22123 oder Port 22125 erfolgen.

Wenn Sie eine Firewall verwenden, muss der entsprechende Port freigeschaltet werden.

11.1. Zertifikat-basiertes Management-Protokoll

Das Management-Protokoll zur Kommunikation zwischen Scout Server und eLux-Geräten verwendet die Ende-zu-Ende-Verschlüsselung über TLS 1.2.

Ab Scout 15 2107 werden nur noch Geräte mit **eLux RP 6.2 oder neueren eLux-Versionen** unterstützt. Für weitere Informationen siehe Kompatibilität Client-Plattform und Scout Enterprise Management Suite im Whitepaper **Releases, Lebenszyklen und Kompatibilität**.

Die Zertifikat-basierte Verschlüsselung des Management-Protokolls erfolgt über ein vom Scout-Dienst automatisch erzeugtes Self-signed-Zertifikat. Alternativ können Sie ein CA-Zertifikat verwenden, das Sie am Scout Server konfigurieren.

Für die verschlüsselte Kommunikation mit dem Scout Server wird Port 22125 verwendet.[1]

Folgende Voraussetzungen müssen für die Kommunikation über TLS 1.2 erfüllt sein:

- Die Vertrauensstufe muss auf den Geräten mit der Option **TlsVerifyOption** eingestellt werden. Standardmäßig ist die Vertrauensstufe auf `0` gesetzt und die Zertifikatsprüfung ausgeschaltet.

  Für weitere Informationen siehe Clients für Zertifikat-basierte Kommunikation konfigurieren.

- Wenn Sie ein von einer CA erstelltes Zertifikat einsetzen (statt self-signed), muss das Zertifikat in Form einer `pfx`-oder `pem`-Datei am Scout Server hinterlegt und konfiguriert werden. Das Zertifikat darf nicht Kennwort-geschützt sein. Die Clients müssen mit den zugehörigen Root-Zertifikaten ausgestattet werden.

  Für weitere Informationen siehe ." Scout Server für Kommunikation über CA-Zertifikate konfigurieren" auf Seite 68.

Hinweis
Die Kommunikation über TLS können Sie in der Protokolldatei für den Scout Serverdienst `eluxd.log` überprüfen.

---

[1] Bis Scout 15 2107 konnten Geräte mit älteren eLux-Versionen über Port 22123 mit AES-256-Verschlüsselung genutzt werden.

11.2. Geräte für Zertifikat-basierte Kommunikation konfigurieren

Die Zertifikat-basierte Verschlüsselung des Management-Protokolls zur Kommunikation zwischen Scout Server und eLux-Client erfordert die Prüfung der relevanten Zertifikate (Chain of trust). Standardmäßig wird die Verschlüsselung über ein Self-signed-Zertifikat durchgeführt, das automatisch vom Scout Server erstellt wird.

> **Achtung** Wenn Sie ein Zertifikat einsetzen, das von einer CA erstellt wurde (CA-Zertifikat), müssen Sie auch die zugehörigen Root-Zertifikate an die Clients übertragen. Wenn das Root-Zertifikat nicht vorhanden ist und die Zertifikatsprüfung eingeschaltet ist, kann das Gerät vom Scout Server nicht erreicht werden.
> Sie können beide Schritte, das Einschalten der Zertifikatsprüfung und die Übertragung der Zertifikate, in einem Zug durchführen.

> **Achtung** Auch der Scout Server muss entsprechend konfiguriert werden und das Zertifikat lokal bereitstellen.

1. Um die Zertifikatsprüfung einzuschalten, konfigurieren Sie die Vertrauensstufe für die relevanten Geräte mit der Option **TlsVerifyOption**.

   Verwenden Sie hierzu die Funktion **Erweiterte Dateieinträge** der Scout Console:

Datei	`/setup/terminal.ini`
Abschnitt	`Security`
Eintrag	`TlsVerifyOption`
Wert	`0` ausgeschaltet `1` eingeschaltet `3` eingeschaltet mit zusätzlicher Überprüfung auf Übereinstimmung des Scout Servernamens mit dem Subject Common Name (CN) oder Subject Alternative Name (SAN) im Zertifikat

   Für weitere Informationen siehe Erweiterte Dateieinträge im **Scout**-Handbuch.

2. Wenn Sie ein CA-Zertifikat einsetzen, übertragen Sie alle zugehörigen Root/Intermediate-Zertifikate Ihrer CA an die Clients in das Verzeichnis `/setup/cacerts/scoutsrv`. Dort sucht das System nach den benötigten Zertifikaten, sobald die Zertifikatsprüfung eingeschaltet ist (Chain of trust).

   Für weitere Informationen siehe Konfigurierte Dateiübertragung im **Scout**-Handbuch.

3. Wenn Sie ein CA-Zertifikat einsetzen, konfigurieren Sie im nächsten Schritt den Scout Server. Für weitere Informationen siehe " Scout Server für Kommunikation über CA-Zertifikate konfigurieren" auf Seite 68.

4. Starten Sie die Geräte neu.

Hinweis
Nachdem die Datei `terminal.ini` auf dem Gerät durch einen Neustart aktualisiert wurde, kann ein weiterer Geräte-Neustart erforderlich sein, um die neue Einstellung zu aktivieren.

Sobald bei einem Gerät die Vertrauensstufe 1 oder 3 aktiviert wurde, kann das Gerät nur noch über gültige Zertifikate mit seinem Scout Server kommunizieren. Bei Vertrauensstufe 3 wird zusätzlich der Gerätename überprüft.

11.3. Scout Server für Kommunikation über CA-Zertifikate konfigurieren

Hinweis
Diese Konfiguration ist nur dann notwendig, wenn Sie ein Zertifikat einsetzen, das von einer CA erstellt wurde.

1. Speichern Sie die Zertifikats-Datei lokal am Scout Server.
2. Öffnen Sie auf der Server-Maschine im Dateisystem unter `%PUBLIC%\Documents\Unicon\Scout\Server\` die Datei `eluxd.ini` zur Bearbeitung.

   Setzen Sie folgende Einträge:

Abschnitt	Eintrag	Beschreibung
`ELUXD`	`UseSelfsignedCertificate=0`	erfordert die Verwendung eines Zertifikats, das von einer CA erstellt wurde Verwenden Sie ein Zertifikat, das nicht durch ein zusätzliches Kennwort geschützt ist. Wenn Sie diese Option setzen, müssen Sie die nächsten Werte definieren. Default: `1`
`ELUXD`	`CertificateFile=`*Path to certificate file*	Pfad zum Speicherort der Zertifikatsdatei Beispiel: `C:\Users\Public\Documents\Unicon\Scout\Server\sampletec-01.pfx`
`ELUXD`	`CertificateKeyFile=`*Path to private key file*	Muss nur angegeben werden, wenn die Zertifikatsdatei nicht im `pfx`-Format vorliegt

3. Starten Sie den Scout-Dienst neu.

4. Stellen Sie sicher, dass die Zertifikatsprüfung eingeschaltet ist und die notwendigen Root/Intermediate-Zertifikate Ihrer CA auf den Geräten vorhanden sind (Chain of trust). Für weitere Informationen siehe Clients für Zertifikat-basierte Kommunikation konfigurieren.

Der Scout Server kommuniziert nur noch mit Clients, die dem CA-Zertifikat trauen.

12. Problembehandlung

Fehlermeldung / Problem	Ursache	Lösung
Scout Desktop-Symbole werden nicht korrekt angezeigt.	Desktop-Symbole werden von Windows gecacht. Dies kann dazu führen, dass nach einer Aktualisierung auf eine neue Scout-Version ein neues Symbol nicht korrekt angezeigt wird.	Setzen Sie den Windows Symbol-Cache zurück. Bitte konsultieren Sie die relevante Dokumentation.
Dateizugriffsfehler beim Prüfen des HTTP/FTP-Servers (Fehlernummer=404)	Mögliche Ursache sind fehlende MIME Type-Einträge für die verwendeten Dateierweiterungen am Webserver (siehe unten)	Ordnen Sie in den MIME-Type-Einstellungen des Webservers die Dateierweiterungen, die in eLux-Containern verwendet werden, den relevanten MIME-Typen zu. Bei der Installation von ELIAS 18 oder des eLux-Containers auf einem Microsoft Internet Information Server (IIS) werden die Zuordnungen automatisch durchgeführt.

Folgende MIME Type-Zuordnungen werden benötigt und mit dem Container installiert:

Erweiterung	MIME-Type
.dd	text/plain
.epm	text/plain
.fpm	text/plain
.gz	application/x-gzip
.idf	text/plain
.ini	text/plain
.rdf	text/plain
.sig	text/plain
.xz	application/x-xz

Folgende zusätzliche Zuordnungen können erforderlich sein:

Erweiterung	MIME-Typ	Beschreibung
.bin	application/octet-stream	BIOS-Update über Scout

Erweiterung	MIME-Typ	Beschreibung
.bup	text/plain	BIOS-Update über Scout
.cab	application/vnd.ms-cab-compressed	UEFI-Update über Scout
.mee	text/plain	Migration von eLux RP 5 auf eLux RP 6 mit Whitelist[1] Unterschiedliche Images je nach Hardware-Modell (für weitere Informationen siehe Problembehandlung)
.udf	text/plain	UEFI-Updates analog zu Firmware-Updates[2]

Mögliche Probleme bei der Installation mit Microsoft SQL Server

Fehlermeldung	Ursache	Lösung
Die Lizenzdatenbank kann nicht initialisiert werden.	Bei der Überprüfung der Datenbank-ID wurde ein Problem identifiziert.Die Wiederherstellung einer Datenbanksicherung wurde auf einem SQL Server durchgeführt, auf dem die Datenbank nicht existiert. Hinweis: Über eine eindeutige Datenbank-ID wird sichergestellt, dass eine Scout-Lizenzdatenbank nicht mehrfach verwendet werden kann.	Präventiv: Führen Sie die Wiederherstellung einer Datenbanksicherung nur auf dem SQL Server durch, auf dem die Datenbanksicherung erzeugt wurde und die Datenbank noch existiert. Im Fehlerfall: Kontaktieren Sie den Unicon-Support.Über die Schaltfläche **Datenbank reparieren** wird eine Prüfsumme angezeigt, mit der durch den Unicon-Support ein Validierungscode zur Reparatur der Lizenzdatenbank erzeugt werden kann.

Mögliche Probleme bei der Installation mit LocalDB

Fehlermeldung	Ursache	Lösung
Ihre Microsoft Jet Database Engine (MDB) Datenbank ist nicht aktuell	Microsoft Jet Database Engine wird von neueren Scout-Versionen nicht mehr unterstützt.	Verwenden Sie Microsoft SQL Server Express LocalDB.

[1] in aktuellen eLux-Versionen automatisch mit der Container-Installation
[2] ab Scout 15 2107 and eLux RP 6 2107

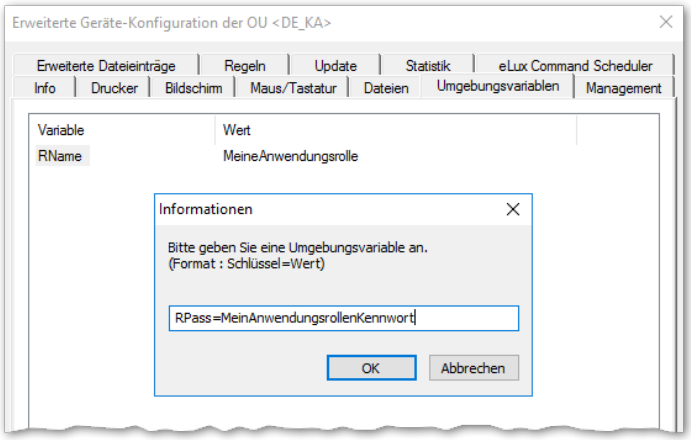
Fehlermeldung	Ursache	Lösung
Die Überprüfung des angegebenen Benutzers ist fehlgeschlagen	Der angegebene Benutzername oder das angegebene Kennwort sind falsch.	Stellen Sie sicher, dass der angegebene Benutzer vorhanden ist.Wir empfehlen ein technisches Benutzerkonto für den Zugriff auf die LocalDB zu verwenden.
Der Benutzer hat nicht das Recht sich als Dienst anzumelden	Das Konto muss über das lokale Benutzerrecht **Anmelden als Dienst (Log on as a service)** verfügen.	Verwenden Sie ein technisches Benutzerkonto für den Zugriff auf die LocalDB, das über das Recht **Anmelden als Dienst (Log on as a service)** verfügt.
Der Benutzer hat nicht das Recht, sich als Administrator anzumelden	Der Benutzer muss Mitglied der Administratorengruppe sein.	Überprüfen Sie die Rechte des verwendeten Kontos.

Für weitere Informationen siehe "SQL LocalDB" auf Seite 12.

13. Werte verschlüsseln

Zum Verschlüsseln beliebiger Werte empfehlen wir das Erfassen und Verschlüsseln von Variablen in einer temporären OU. Die verschlüsselten Werte werden anschließend über den Zwischenspeicher an ihre Zielposition kopiert.

1. Legen Sie in der Scout Console eine temporäre OU an, beispielsweise mit Namen `TEMP`.
2. Öffnen Sie das Kontextmenü der `TEMP`-OU und wählen Sie **Erweiterte Geräte-Konfiguration > Umgebungsvariablen**.
3. Fügen Sie eine neue Variable und ihren Wert hinzu.Bestätigen Sie mit **OK**.



*Die neue Variable und ihr Wert werden im Register **Umgebungsvariablen** angezeigt.*

4. Klicken Sie mit der rechten Maustaste auf die Variable und wählen im Kontextmenü **Wert verschlüsseln**.

   Der Wert der Variable wird verschlüsselt angezeigt.

5. Markieren Sie die Variable und klicken Sie auf **Bearbeiten**. Kopieren Sie anschließend den verschlüsselten Wert über Kontextmenü oder STRG-C in den Zwischenspeicher und setzen ihn an der Zielposition ein.
6. Löschen Sie die temporäre OU.

14. Anhang

14.1. Programm- und Datei-Verzeichnisse

Programmverzeichnis

Die Scout Enterprise Management Suite wird standardmäßig installiert nach

`%PROGRAMFILES%\Unicon\Scout`

ELIAS 18 wird gemäß Ihren Angaben während der Installation beispielsweise auf dem Webserver IIS installiert.

Der eLux-Container (nur bei Einsatz des klassischen ELIAS) wird auf dem Webserver installiert nach

`<Root-Verzeichnis>\eluxng`

Verzeichnis für Scout Serverdateien

Für Protokoll-, Konfigurations- und weitere Dateien verwendet Scout ein Unterverzeichnis von

`%PUBLIC%\Documents\Unicon`

- Öffnen Sie das Serverdateien-Verzeichnis im Windows Dateiexplorer mit Hilfe der Scout-Menüfunktion **Ansicht > Systemdiagnose > Serverdateien** (nur wenn Konsole und Server auf der gleichen Maschine installiert sind).

Verzeichnis für Benutzer-Dateien

Benutzerbezogene Dateien werden in einem Unterverzeichnis des lokalen Benutzer-Verzeichnisses gespeichert unter

`%USERPROFILE%\Documents\Unicon`

Diagnose-Dateien, die über die Konsole angefordert werden, werden gespeichert unter

`%USERPROFILE%\Documents\Unicon\Scout\Console\Diag`

Diagnosedateien, die über Scout Board angefordert werden, werden vom verwendeten Browser heruntergeladen und je nach Konfiguration im Download-Verzeichnis gespeichert.

Hinweis
Wenn Sie auf dem Scout Server Anti-Virus-Software einsetzen, empfehlen wir zur Vermeidung von Seiteneffekten, die angegebenen Verzeichnisse von der Virenprüfung auszuschließen.

14.2. eLux-Partitionen

Der Flash-Speicher eines Clients wird bei der eLux-Installation in drei bzw. vier Partitionen aufgeteilt. Jede Partition ist für einen dedizierten Zweck reserviert und wird nur beim Ausführen von Aufgaben angefasst, die mit der relevanten Partition zusammenhängen.

Alle Partitionen werden während einer Recovery-Installation erstellt.

Übersicht Partitionen

Partition	Voraussetzungen	Zweck	Wird neu erstellt durch	Sonstiges
System		Reserviert für die Firmware (Software-Pakete)	Scout **Update**-Kommando mit **System-Partition vor Update formatieren**	Größe bis eLux RP 6 2104 LTSR: 1,77 GB / 1,84 GB mit/ohne Verschlüsselung Größe ab eLux RP 6 2107: 2,35 GB / 2.41 GB mit/ohne Verschlüsselung
Boot	nur UEFI und USB	Boot-Sektion	-	
Setup		Geräte-Konfiguration Lokale Anwendungsdefinitionen	Kommando **Grundzustand**	Hat keine Auswirkungen auf die System-Partition mit installierter Firmware
Update	4 GB Flash-Speicher	Software-Auslieferung (vor Firmware-Update) via Scout-Kommando oder -Vormerkung Signaturprüfung für eLux Software-Pakete Geräte mit Update-Partition können als Dynamischer Proxy (Provider) für Firmware-Updates verwendet werden.	Scout **Auslieferung**-Kommando mit Option **Update-Partition vor Auslieferung bereinigen**	Die Größe der Update-Partition richtet sich nach dem vorhandenen Speicherplatz. Auf Geräten mit weniger als 4 GB Flash-Speicher wird keine Update-Partition erstellt.

Hinweis
In der Scout Console können System-, Setup- und Update-Partition mit ihrer jeweiligen Größe im **Eigenschaften**-Fenster eines Gerätes angezeigt werden.

Vergrößerte System-Partition ab eLux RP 6 2107

Wenn Sie eine Update-Installation oder eine Neu-Installation (Recovery) auf eLux RP 6 2107 oder höher durchführen, wird die System-Partition mit 2,35 GB / 2.41 GB (mit/ohne Verschlüsselung) statt

mit bisher knapp 2 GB erstellt. Dadurch entsteht mehr Platz für die Firmware und es können größere Images verwendet werden.

- **Update-Installation**

  Eine Update-Installation (Firmware-Update) erfolgt noch auf Basis der alten Partitionsgrößen. Die Image-Größe ist damit noch auf die alten Werte beschränkt. Danach steht die vergrößerte System-Partition zur Verfügung und Sie können Images installieren, die bis zu 2,35 GB / 2.41 GB groß sein dürfen. Um größere Images auf die soeben vergrößerte Partition der Geräte zu installieren, ist daher ein zweites Firmware-Update notwendig.

- **Recovery-Installation**

  Vorausgesetzt ein aktuelles Recovery-System ist vorhanden, kann mit einer PXE- oder USB-Recovery-Installation die System-Partition direkt während des Installationsvorganges auf die neue Größe partitioniert werden und im selben Vorgang ein größeres Image mit bis zu 2,35 GB / 2.41 GB geschrieben werden. Eine Neu-Installation oder Recovery-Installation erlaubt also die Vergrößerung und Nutzung der Partition in einem Schritt.

Downgrade

> **Achtung** Ein Downgrade von Geräten, die über die vergrößerte System-Partition verfügen (eLux RP 6 2107 oder höher) auf eine ältere Version, die nur die alte System-Partition mit knapp 2 GB unterstützt, ist ausschließlich auf die Version eLux RP 6 2104 LTSR möglich.

Wir empfehlen daher, ein Update auf eLux RP 6 2107 oder höher im ersten Schritt nur mit Testgeräten durchzuführen und die Funktionalität gründlich zu testen.

Für weitere Informationen siehe Update auf neues Partitions-Layout im **Scout**-Handbuch.

14.3. IP-Ports

eLux / notwendige Ports

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
	ICMP	**ping** muss zur Überprüfung des Gerätestatus der eLux-Geräte unterstützt werden		ein/aus
80	TCP	Firmware-Update via HTTP (und Proxy Port, falls genutzt)		ausgehend
443	TCP	Firmware-Update via HTTPS/TLS		ausgehend

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
5900	TCP	Spiegelung des eLux Desktop	Spiegelung deaktivieren (**Konfig**[1] > **Sicherheit**) oder `VNC server`-FPM im `X.Org`-Paket deinstallieren	eingehend
22123	TCP	Scout Server (Scout Manager / secure)		ein/aus
22125	TCP	Scout Server (Scout Manager / TLS 1.2)		ein/aus
22129	TCP	VPN		ausgehend

eLux / optionale Ports

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
	ESP	VPN (Datenphase)	`VPN System`-Paket deinstallieren	ein/aus
21	TCP	Update via FTP control port (dynamic data port)		ausgehend
22	TCP	SSH-Anwendungen		ausgehend
23	TCP	5250 Emulationen und Telnet-Sitzungen		ausgehend
53	TCP, UDP	DNS-Server		ausgehend
67	UDP	DHCP-Server	Lokale IP-Adresse konfigurieren (**Konfig > Netzwerk**)	ausgehend
68	UDP	DHCP Client (oder BootP Client)	Lokale IP-Adresse konfigurieren (**Konfig > Netzwerk**)	eingehend
69	UDP	TFTP-Server (wird nur während eines PXE-Recovery verwendet)		ausgehend
88	TCP, UDP	AD-Authentifizierung (Kerberos)		Outgoing

[1] Geräte-Konfiguration

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
111	TCP, UDP	TCP Portmapper - RPC nur zur internen Verwendung Funktioniert mit lockd (random) UDP Portmapper - Treiberzugang auf NFS-Servern Funktioniert mit NFSD-Laufwerkszugriff (Port 2049) und mountd (random)	`Network Drive Share`-Paket deinstallieren	ein/aus
123	UDP	Windows-Zeitserver (NTP)	Keinen Zeitserver konfigurieren (**Konfig > Desktop**)	ein/aus
139	TCP, UDP	SMB Laufwerkszuordnung (NetBIOS) und SMB Benutzerauthentifizierung (CIFS)	Pakete `Network Drive Share` und `User authentication modules` deinstallieren	ausgehend
161	UDP	SNMP	`SNMP Environment`-Paket deinstallieren	ein/aus
162	UDP	SNMPTRAP	`SNMP Environment`-Paket deinstallieren	ausgehend
177	UDP	XCMCP-Protokoll		ausgehend
389	TCP	AD-Authentifizierung mit Benutzervariablen		ausgehend
443	TCP	VPN (Verbindungsaufbau) via HTTPS/TLS	`VPN System`-Paket deinstallieren	ein/aus
464	TCP, UDP	AD-Authentifizierung (Kerberos) / Kennwort setzen		Outgoing
514	TCP	Shell, X11-Anwendungen		ausgehend
515	TCP	Drucken über LPD	`Print Environment (CUPS)`-Paket deinstallieren	ein/aus
631	TCP, UDP	CUPS (IPP) Druck-Client	`Print Environment (CUPS)`-Paket deinstallieren	ausgehend
636	TCP	LDAPS-Authentifizierung mit Benutzervariablen		ausgehend

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
6000	TCP	Remote X11 Anwendungen	Option **Konfig > Sicherheit > Remote X11 Clients zulassen** deaktiveren	eingehend
7100	TCP	Fontserver Zuordnung in eLux Systemsteuerung möglich (**Konfig > Bildschirm > Erweitert**)		ausgehend
8080	TCP	Firmware-Update über Dynamischen Proxy (Provider und Consumer)	Option **Konfig > Firmware > Proxy-Typ** auf `Kein` setzen	ein/aus
9100	TCP	Direktdruck auf parallelen Port Zuordnung in eLux Systemsteuerung (**Konfig > Drucker**)	Option **Konfig > Drucker > TCP Direktdruck** deaktivieren	eingehend
9101	TCP	Direktdruck auf USB Port Zuordnung in eLux Systemsteuerung (**Konfig > Drucker**)	Option **Konfig > Drucker > TCP Direktdruck** deaktivieren	eingehend
20000	UDP	Wake On LAN		ein/aus
22124	TCP	Scout Statistics		ausgehend

Scout Server

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
	ICMP	**ping** muss zur Überprüfung des Gerätestatus der eLux-Geräte unterstützt werden		ein/aus
1433	TCP	MS SQL Server		ausgehend
1434	UDP	MS SQL Server (Browserdienst)		ein/aus
22123	TCP	Clients (Scout Manager / secure)		ein/aus
22124	TCP	Scout Statistics		eingehend
22125	TCP	Clients (Scout Manager / TLS 1.2)		ein/aus

Scout Console

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
1433	TCP	MS SQL Server		ausgehend
1434	UDP	MS SQL Server (Browserdienst)		ausgehend
5900	TCP	Spiegelung des eLux Desktop	Spiegelung deaktivieren (**Konfig > Sicherheit**) oder `VNC server`-FPM im `X.Org`-Paket deinstallieren	ausgehend

Scout Cloud Gateway

Port	Typ	Beschreibung	Ein/Aus
22125	TCP	Clients (Scout Manager / TLS 1.2)	ein/aus
22129	TCP	VPN	eingehend

14.4. SNMP

SNMP (Simple Network Management Protocol) ist ein Netzwerkprotokoll zur Überwachung und Steuerung von Netzwerkgeräten.

eLux RP 6 wird SNMPv3 eingesetzt.

Hinweis
Das Kommandozeilenprogramm **snmpget** ist nicht Bestandteil des Software-Paketes. Verwenden Sie zum Abfragen der SNMP-Statusinformationen bitte eine Software von Drittanbietern.

14.4.1. SNMP konfigurieren

1. Downloaden Sie von unserem Portal myelux.com unter **eLux Software Packages** für Ihre eLux-Version unter **Add-On** das Paket **SNMP Environment** und übertragen Sie die Software auf die Geräte.
2. Wenn noch keine `/setup/snmp/snmpd.conf` vorhanden ist, übertragen Sie die Konfigurationsdatei `snmpd.conf` auf die Geräte nach `/setup/snmp/snmpd.conf`. Verwenden Sie dazu die Scout-Funktion Dateien.

   Oder:

   Konfigurieren Sie die Datei `terminal.ini` mit der Scout-Funktion Erweiterte Dateieinträge. Beispiel:

Datei	`/setup/terminal.ini`
Abschnitt	`SNMPD`
Eintrag	`rocommunity`
Wert	`secret`

3. Geben Sie optional weitere SNMPD Configuration Directives in der Datei `terminal.ini` im Abschnitt `SNMPD` an. Verwenden Sie dazu die Scout-Funktion Erweiterte Dateieinträge. Beispiele:

   ```
   syscontact=contact@sampletec.com
   syslocation=testcenter
   doDebugging=1
   ```

   Für weitere Informationen über SNMPD Configuration Directives siehe http://www.net-snmp.org.

Der Client wertet den Abschnitt `SNMPD` in der Datei `terminal.ini` aus und erstellt die Datei `/setup/snmp/snmpd.local.conf`. Eine vorhandene `/setup/snmp/snmpd.conf` wird dabei überschrieben.

Wenn die Konfigurationsdatei fehlt, wird die Datei `/setup/snmp/snmpd.local.conf` mit Standardwerten erstellt.

Hinweise zur Konfiguration von SNMP v3

- Setzen Sie bei der Definition des Benutzers(**createUser**) ein Kennwort mit mindestens 8 Zeichen.
- Definieren Sie als Authentifizierungsmethode entweder `authPriv` oder `authNoPriv`.

Hinweis
Für SNMP v2 können Sie die Authentifizierungsmethode `noAuthNoPriv` verwenden.

14.4.2. SNMPD und SNMP Konfigurations-Befehle

Die nachstehende Liste bezieht sich auf das eLux-Software-Paket **snmp**.
Zur Verwendung von SNMP unter eLux siehe SNMP.

Für weitere Informationen siehe http://www.net-snmp.org.

SNMPD Configuration Directives

Verwendung	Befehl
authtrapenable	1 | 2 (1 = enable, 2 = disable)
trapsink	host [community] [port]
trap2sink	host [community] [port]
informsink	host [community] [port]
trapsess	[snmpcmdargs] host
trapcommunity	community-string
agentuser	agentuser
agentgroup	groupid
agentaddress	SNMP bind address
syslocation	location
syscontact	contact-name
sysservices	NUMBER
interface	name type speed
com2sec	name source community
group	name v1|v2c|usm security
access	name context model level prefx read write notify
view	name type subtree [mask]
rwcommunity	community [default|hostname|network/bits] [oid]
rocommunity	community [default|hostname|network/bits] [oid]
rwuser	user [noauth|auth|priv] [oid]
rouser	user [noauth|auth|priv] [oid]
swap	min-avail
proc	process-name [max-num] [min-num]
procfix	process-name program [arguments...]

Verwendung	Befehl
pass	miboid command
pass_persist	miboid program
disk	path [minspace | minpercent%]
load	max1 [max5] [max15]
exec	[miboid] name program arguments
sh	[miboid] name program-or-script arguments
execfix	exec-or-sh-name program [arguments...]
file	file [maxsize]
dlmod	module-name module-path
proxy	[snmpcmd args] host oid [remoteoid]
createUser	username (MD5|SHA) passphrase [DES] [passphrase]
master	pecify 'agentx' for AgentX support
engineID	string
engineIDType	num
engineIDNic	string

SNMP Configuration Directives

Verwendung	Befehl
doDebugging	(1|0)
debugTokens	token[,token...]
logTimestamp	(1|yes|true|0|no|false)
mibdirs	[mib-dirs|+mib-dirs]
mibs	[mib-tokens|+mib-tokens]
mibfile	mibfile-to-read
showMibErrors	(1|yes|true|0|no|false)
strictCommentTerm	(1|yes|true|0|no|false)
mibAllowUnderline	(1|yes|true|0|no|false)
mibWarningLevel	integerValue
mibReplaceWithLatest	(1|yes|true|0|no|false)
printNumericEnums	1|yes|true|0|no|false)
printNumericOids	1|yes|true|0|no|false)
escapeQuotes	(1|yes|true|0|no|false)

Verwendung	Befehl
dontBreakdownOids	(1|yes|true|0|no|false)
quickPrinting	(1|yes|true|0|no|false)
numericTimeticks	(1|yes|true|0|no|false)
suffixPrinting	integerValue
extendedIndex	(1|yes|true|0|no|false)
printHexText	(1|yes|true|0|no|false)
dumpPacket	(1|yes|true|0|no|false)
reverseEncodeBER	(1|yes|true|0|no|false)
defaultPort	integerValue
defCommunity	string
noTokenWarnings	(1|yes|true|0|no|false)
noRangeCheck	(1|yes|true|0|no|false)
defSecurityName	string
defContext	string
defPassphrase	string
defAuthPassphrase	string
defPrivPassphrase	string
defVersion	1|2c|3
defAuthType	MD5|SHA
defPrivType	DES (currently the only possible value)
defSecurityLevel	noAuthNoPriv|authNoPriv|authPriv