Scout Enterprise Management Suite

Version 14.x

Administrationshandbuch zur Verwaltung einer Client-Infrastruktur mit der Scout Enterprise-Konsole

Stand 2017-06-16

0. Rechtliche Hinweise

Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH
Ludwig-Erhard-Allee 26
76131 Karlsruhe
+49 (0) 721 96451-0

1. Einleitung

1.1. Über die Scout Enterprise Management Suite

Mit der Scout Enterprise Management Suite verwalten Sie voll umfänglich Thin Clients oder PCs, die mit dem Betriebssystem eLux arbeiten. Zusätzlich können Sie Windows-basierende Clients mit grundlegenden Funktionen verwalten.

Die Scout Enterprise Management Suite besteht aus mehreren Komponenten. Die ersten sieben aufgeführten Komponenten sind Bestandteil der Standard-Installation,[1] können aber im Rahmen einer benutzerdefinierten Installation optional abgewählt werden.

Komponente	Beschreibung	Installation
Scout Enterprise-Server	Der Dienst steuert und verwaltet eLux-Clients sowie Windows-basierende Clients, die Scout Agent für Windows installiert haben.	`Scout Enterprise.exe`
Scout Enterprise-Konsole	Benutzeroberfläche zur Verwaltung von eLux-Clients sowie von Windows-basierenden Clients, die Scout Agent für Windows installiert haben Kommuniziert ausschließlich über die Datenbank mit dem Server In einer Scout Enterprise-Datenbank können mehrere Konsolen verwaltet werden.	`Scout Enterprise.exe`
Recovery-Service	TFTP-Dienst zur Realisierung einer PXE-Recovery-Umgebung für eLux-Clients	`Scout Enterprise.exe`
Scout Enterprise ELIAS	Mit dem Dialogprogramm eLux Image Administration Service (ELIAS) können individuelle Imagedefinitionsdateien (.idf) zum modularen Update der Firmware von eLux-Clients erstellt werden.	`Scout Enterprise.exe`
Scout Enterprise-Reportgenerator	Tool zum Erstellen von frei definierbaren Reports über die aktuell in der Scout Enterprise-Datenbank enthaltenen Geräte, Anwendungen und OUs	`Scout Enterprise.exe`

[1] ab Scout Enterprise Management Suite Version 15.0 kommen Dashboard und die Web API dazu

Komponente	Beschreibung	Installation
Scout Enterprise PUMA	Package Update Management Agent Der Dienst bietet die vollautomatische Aktualisierung ausgewählter eLux-Pakete über www.myelux.com in den eLux-Container auf dem Webserver.	`Scout Enterprise.exe`
Scout Enterprise Statistikservice (nur für SQL Server-Datenbank)	Dienst zur Auswertung von Client-Statusinformationen und von dynamischen Geräteinformationen	`Scout Enterprise.exe`
Scout Enterprise-Dashboard[1] (nur für SQL Server-Datenbank)	Webbasierte Konsole zur Verwaltung von eLux-Clients sowie von Windows-basierenden Clients, die Scout Agent für Windows installiert haben	`Scout Enterprise.exe`
Web API[2] (nur für SQL Server-Datenbank)	Programmierbare Anwendungsschnittstelle zur Verwaltung von eLux-Clients sowie von Windows-basierenden Clients, die Scout Agent für Windows installiert haben	`Scout Enterprise.exe`
Scout Enterprise Mirror App	Dialogprogramm zum Spiegeln von eLux-Clients ohne Verwendung der Scout Enterprise-Konsole (berücksichtigt die Scout Enterprise-Administratorrechte)	gesondert
Scout Agent für Windows	Dienst mit Benutzerschnittstelle für Windows-basierende Clients zur Verwaltung durch Scout Enterprise Management Suite	gesondert
Scout Enterprise Command Interface	Kommandozeilen-Tool für Scout Enterprise-Befehle	`Scout Enterprise.exe`
Scout Enterprise-Konfigurationsdateieditor	Dialogprogramm zum Bearbeiten von Konfigurationsdateien, die aus der Scout Enterprise-Konsole exportiert wurden	`Scout Enterprise.exe`
Scout Enterprise-Datenbankverbindungseditor	Tool zum Bearbeiten der Datenbankverbindungseinstellungen des Scout Enterprise-Servers und der Scout Enterprise-Konsole	`Scout Enterprise.exe`

Das vorliegende Handbuch beschreibt die Konfiguration, Steuerung und Verwaltung der Clients durch die Scout Enterprise-Konsole sowie den Statistikservice. Das Handbuch umfasst auch das Spiegeln mit der Scout Enterprise Mirror App.

[1] bis Scout Enterprise Management Suite Version 14.9 separate Installation erforderlich
[2] ab Scout Enterprise Management Suite Version 15.0

Für folgende Komponenten stehen eigene Handbücher zur Verfügung:

- Scout Enterprise ELIAS
- Scout Enterprise-Reportgenerator
- Scout Enterprise PUMA
- Scout Enterprise Command Interface
- Scout Enterprise-Konfigurationseditor
- Scout Enterprise-Dashboard

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

Hinweis
Damit Sie Ihre eigenen Image-Dateien zusammenstellen können, benötigen Sie zusätzlich zur Scout Enterprise Management Suite-Installation einen eLux-Container. Der eLux-Container ist ein Webserver-Container, der Software-Pakete und IDF-Dateien enthält. Mit Scout Enterprise ELIAS können Sie dann individuelle Image-Dateien für das Firmware-Update Ihrer Clients zusammenstellen. Die Installation des eLux-Containers erfolgt über das `AllPackages`-Bundle einer eLux-Version und der enthaltenen `setup.exe`-Datei.

1.2. Kommunikation zwischen Thin Client und Scout Enterprise-Server

Während ein Client-Gerät hochfährt, verbindet es sich zu seinem Scout Enterprise-Server und prüft, ob Aktualisierungen vorliegen. Diese Prüfung bezieht sich in der Regel auf alle Konfigurationseinstellungen des Clients: Gerätekonfiguration, Anwendungsdefinition, Erweiterte Dateieinträge und Dateiübertragung. Für weitere Informationen zur Ermittlung und Übertragung der Konfigurationsinformationen siehe Konfigurationsmethode.

Für den weiteren Ablauf der Kommunikation gibt es drei Varianten:

- Client erreicht den Scout Enterprise Server. Der Scout Enterprise-Server hat keine aktualisierte Konfiguration. Thin Client bootet weiter mit den bisher vorhandenen Einstellungen.
- Client erreicht den Scout Enterprise-Server. Der Scout Enterprise-Server meldet Neuigkeiten und überträgt diese an den Thin Client. Daraufhin erfolgt eventuell ein Neustart des Clients mit der neuen Konfiguration.
- Client erreicht Scout Enterprise Server wegen Netzwerk- oder anderer Probleme nicht. Dies führt zunächst zu einem Timeout (konfigurierbar in den Erweiterten Netzwerkeinstellungen). Der Thin Client arbeitet weiter mit den zuletzt gespeicherten Einstellungen.
  Je nach Handshake-Konfiguration wiederholt der Client den Verbindungsversuch, um die Konfiguration zu synchronisieren. Für weitere Informationen siehe Optimierung durch Handshake.

Die Aktualisierung kann sich auf die Gerätekonfiguration, Anwendungsdefinition, konfigurierte Dateiübertragung und Erweiterte Dateieinträge beziehen.

Während des Betriebs eines Thin Clients werden keine Daten zwischen Scout Enterprise-Server und Thin Client ausgetauscht. Beim Ausschalten eines Thin Client meldet der Thin Client seinen Status an Scout Enterprise.

Ausnahme: VPN-Verbindungen

1.3. 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
EBKGUI	Oberfläche des eLux Builder Kit (Komponente der Scout Enterprise-Software)
EPM	eLux package module (`.epm`, Software-Paket)
FPM	Feature package module (`.fpm`, Teil eines Software-Paketes)
FQDN	Fully qualified domain name
GB	Gigabyte
IDF	Image Definition File (`.idf`)
IIS	Microsoft Internet Information Services
MB	Megabyte
OU	Organizational unit Organisationseinheit oder Gruppe innerhalb der Organisationsstruktur
VPN	Virtual Private Network

1.4. Tastenkombinationen

Tasten	Markiertes Element	Beschreibung
STRG+UMSCHALT+EINFG	Individuelle Organisationseinheit	Öffnet die **Erweiterten Einstellungen** der markierten OU
	Anwendungen	Öffnet den Dialog **Anwendungseigenschaften** zum Definieren einer neuen Anwendung
	Geräte	Öffnet den Dialog **Informationen** zum Erstellen eines neuen Gerätes an der markierten Position und verlangt eine MAC-Adresse
STRG+UMSCHALT+ENTF	Individuelle Organisationseinheit	Löscht die markierte Organisationseinheit
	Individuelle Anwendung	Löscht die markierte Anwendung
	Individuelles Gerät	Löscht das markierte Gerät
F2	Individuelle Organisationseinheit	Umbenennen der markierten Organisationseinheit
	Individuelles Gerät	Umbenennen des markierten Gerätes
	Individuelle Anwendung	Umbenennen der markierten Anwendung
F5	_	Aktualisiert die Konfiguration aller Geräte
STRG+F	_	Aktiviert das Suchfeld für die schnelle Suche
STRG+UMSCHALT+F	_	Öffnet das Fenster Suchen für die erweiterte Suche
STRG+X	Individuelles Gerät	Schneidet das markierte Gerät aus
STRG+V	**Geräte** oder individuelles Gerät	Gerät aus der Zwischenablage an der markierten Position einfügen
STRG+A	Individuelle Anwendung oder Gerät im **Listen**-Fenster	Markiert alle Anwendungen/Geräte im **Listen**-Fenster
STRG+E	Individuelles Gerät	Führt einen Setupvergleich durch
STRG+P	_	Öffnet den Druckdialog, um die Geräteliste zu drucken

2. Installation

2.1. Systemvoraussetzungen

Hinweis
Wir empfehlen, die Scout Enterprise Management Suite auf einem Windows Server-System zu betreiben. Die Nutzung auf einer Windows-Workstation ist nur ohne Scout Enterprise-Dashboard möglich.

Mindestanforderungen für den Scout Enterprise-Server

- Festplattenspeicher 600 MB (ohne Software-Container)
- Microsoft Windows Server 2008 R2, 2012, 2012 R2 oder
  Microsoft Windows Server 2016 (erfordert Scout Enterprise Management Suite Version 14.9 oder höher) oder
  Microsoft Windows 7, Windows 8, Windows 10

  jeweils mit den von Microsoft zum Zeitpunkt der Installation zur Verfügung gestellten Software-Aktualisierungen
- Microsoft .NET Framework Version 3.5 und
  Microsoft .NET Framework Version 4.5.1 oder höher
- Passender ODBC Treiber
- Für die Installation der 64-Bit-Version (ab Scout Enterprise Management Suite V14.0.0) ist der Microsoft SQL Server Native Client 11.0 auf dem Scout Enterprise Server erforderlich. Die entsprechende `.msi`-Datei (Dateiname: `sqlncli.msi`) können Sie einzeln oder als Bestandteil eines Microsoft SQL Server Feature Packs von Microsoft herunterladen. Nach Installation des Microsoft SQL Server Native Client wird der Treiber in den ODBC-Datenquellen angezeigt.
- Administratorrechte für das System, auf dem Scout Enterprise läuft
- Administratorrechte für die Verbindung zu einem TCP/IP-Netzwerk

Anforderungen an das Datenbanksystem

- Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016
- oder für kleinere Installationen
  - bis Scout Enterprise Management Suite 14.6.1: die in Windows enthaltene JET Database Engine (.mdb)
  - ab Scout Enterprise Management Suite 14.7.0: die in der Scout Enterprise-Installationsdatei enthaltene MS SQL Server Express LocalDB als integriertes Datenbank-Managementsystem basierend auf SQL

Mindestanforderungen für den Container

- FTP- oder HTTP-Server mit Schreibzugriff, lokal installiert oder über Netzlaufwerk
- Der Platzbedarf ist abhängig von der Anzahl der vorgehaltenen Betriebssystem-Versionen. Für die Installation des RP5-Container (Version eLux RP5.5 LTSR) empfehlen wir beispielsweise mindestens 1 GB freien Speicherplatz.

Für weitere Informationen siehe Container installieren.

Support-Fristen und Kompatibilitäts-Matrix finden Sie im Downloadbereich auf unserem Portal www.myelux.com.

2.2. Systembeschränkungen

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

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

2.3. Datenbankunterstützung

Scout Enterprise erfordert eine Datenbanksoftware, entweder Microsoft SQL Server oder für kleinere Umgebungen Microsoft SQL Server Express LocalDB (ab Scout Enterprise Management Suite Version 14.7.0) bzw. Microsoft JET Database (bis Scout Enterprise Management Suite Version 14.6.1).

Microsoft SQL Server

Zur Nutzung von SQL-Datenbanken kann Microsoft SQL Server (Version mit verfügbarem Produktsupport) eingesetzt werden. Die Scout Enterprise-Datenbank (mit beliebigem Dateinamen) muss vor der Installation von Scout Enterprise in SQL Server angelegt werden. Der Speicherplatzbedarf für die Scout Enterprise-Datenbank beträgt pro 1.000 Geräte ca. 50 MB.

Wenn im Rahmen der Scout Enterprise-Installation der Scout Enterprise-Statistikservice installiert werden soll (vollständige Installation), muss zusätzlich die Scout Enterprise-Statistikdatenbank über Microsoft SQL Server erzeugt werden.

Für die Verwendung des gesondert zu installierenden Scout Enterprise-Dashboard wird eine dritte Datenbank benötigt, die ebenfalls vor der Installation des Scout Enterprise-Dashboard über Microsoft SQL Server angelegt werden muss.

Die Erzeugung der Tabellen innerhalb der jeweiligen Datenbank erfolgt durch den Installationsprozess der Scout Enterprise Management Suite bzw. des Scout Enterprise-Dashboard.[1]

Übersicht der Datenbanken:

- Scout Enterprise
  Geräte-Konfigurationen, Geräte-Bestandsdaten (statisch), Server-Einstellungen, Administratoren-/ Konsolen- /Lizenzverwaltung, Transaktionsprotokollierung
- Scout Enterprise Statistik
  Geräte-Informationen (dynamisch, Historie)
- Scout Enterprise-Dashboard
  Dashboard-Einstellungen, Transaktionsprotokollierung

Microsoft SQL Server Express LocalDB

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

Hinweis
Auf Basis von SQL Server Express LocalDB oder Microsoft JET Database ist die Nutzung des Scout Enterprise-Statistikservice (Übermittlung der 'keep alive' messages und der statistischen Geräteinformationen) und des Scout Enterprise-Dashboard (Web-Konsole) nicht möglich.

[1] Bis Scout Enterprise 14.9 wird das Dashboard separat installiert.

Die Scout Enterprise-Datenbank wird automatisch während der Installation erstellt:

- Bis Scout Enterprise Version 14.6.1: In den Microsoft Server-Betriebssystemen ist Microsoft JET Datenbase bereits enthalten. Scout Enterprise erstellt während der Installation auf Wunsch die Datenbank vom Typ `.mdb`. Der Dateiname ist frei wählbar.
- Ab Scout Enterprise Management Suite Version 14.7.0: In der Scout Enterprise-Installationsdatei ist Microsoft SQL Server Express LocalDB bereits enthalten. Scout Enterprise erstellt während der Installation auf Wunsch die Datenbank vom Typ `LocalDB`. Der Datenbankname ist System-intern vorgegeben.

Microsoft JET Database konvertieren

Eine bereits genutzte Microsoft JET Database (`.mdb`) kann konvertiert und als **Microsoft SQL Server Express LocalDB** weitergenutzt werden.

1. Aktualisieren Sie Ihre bestehende Scout Enterprise-Installation zunächst auf Scout Enterprise Management Suite Version 14.6.1 unter Verwendung Ihrer mdb-Datenbank.

   Beim Neustart des Scout Enterprise Serverdienstes wird die Datenbank auf die Version 14.6.1 konvertiert.

2. Installieren Sie anschließend eine neuere Version der Scout Enterprise Management Suite mit derselben Datenbank.

   Beim Neustart des Scout Enterprise Serverdienstes wird die Datenbank automatisch in eine SQL 2014 LocalDB-Datenbank konvertiert.

Mehrere Datenbankverbindungen

Mit dem Datenbank-Verbindungseditor können Sie mehrere Datenbankverbindungen für die Scout Enterprise-Konsole 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.

Datenbankbereinigung

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

2.3.1. SQL LocalDB

– ab Scout Enterprise Management Suite 14.7.0 –

Die Nutzung der integrierten Datenbank als Minimalversion des Microsoft SQL Server zur Verwaltung kleinerer Thin 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 Enterprise-Installationsdatei enthalten.

Bei Aktualisierung einer bestehenden Installation auf Scout Enterprise 14.7.0 oder neuer erfolgt die Konvertierung von Microsoft JET Database auf Microsoft SQL Server Express LocalDB automatisch während der Installation des Updates. Voraussetzung ist, dass die Datenbank zuvor mit Scout Enterprise-Version 14.6.1 geöffnet wird.

Während der Installation muss zur Nutzung der Datenbank unter Microsoft SQL Server Express LocalDB ein Scout -Windowsbenutzer 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.

LocalDB vor der Installation von Updates sichern

Bevor Sie eine bestehende Scout Enterprise-Installation mit SQL Server Express LocalDB aktualisieren, können Sie die LocalDB folgendermaßen 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 Enterprise-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 Enterprise-Installation verwenden Sie die Management Studio-Funktion **Restore** zum Wiederherstellen der Datenbank.

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

- Der Betrieb der Scout Enterprise-Konsole ist ausschließlich in Verbindung mit dem Scout Enterprise-Serverdienst und der LocalDB-Datenbank auf einem Serversystem möglich. Dedizierte Scout Enterprise-Konsolen mit Remote-Zugriff auf die LocalDB-Datenbank werden nicht unterstützt.
- Die Nutzung des **Statistik**-Dienstes (Übermittlung der 'keep alive' messages und der statistischen Geräteinformationen) und des Scout Enterprise **Dashboard** (Web-Konsole) sind nicht möglich.

- Das Kommando **Konfigurationslauf** zur Vorbereitung der Client-Konfigurationsinformationen steht nicht zur Verfügung.
- Die Funktion **Datenbankbereinigung** zum Löschen veralteter Daten steht erst ab Scout Enterprise Management Suite Version 14.9 zur Verfügung.

2.3.2. Authentifizierung für SQL-Server

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

Der anzugebende SQL- oder Windows-Benutzer muss Mitglied der festen Datenbankrolle db_owner am SQL-Server sein, um die relevanten Konfigurations- und Wartungsaktivitäten an der Datenbank ausführen zu können.

Modus	Beschreibung
Windows-Authentifizierung	'Trusted connection', die Benutzer-Identität wird von Windows bestätigt. Der Scout Enterprise-Dienst muss mit einem Benutzerkonto ausgeführt werden, das die entsprechenden Berechtigungen am SQL-Server (Mitglied von db_owner) besitzt. Die Anmeldedaten des Dienste-Kontos können im Dialog der Scout Enterprise-Installation eingegeben werden.
SQL Server-Authentifizierung	Benutzername und -kennwort eines SQL Server-Kontos werden verwendet. Der SQL-Benutzer muss die entsprechenden Berechtigungen am SQL-Server (Mitglied von db_owner) besitzen. Die Anmeldedaten des SQL-Benutzers können im Dialog der Scout Enterprise-Installation eingegeben werden.

2.3.3. Anwendungsrollen für SQL-Server definieren

Um die Berechtigungen der Konsole für den Zugriff auf die SQL Server-Tabellen zu beschränken, ist es möglich, eine SQL-Anwendungsrolle zu definieren. In der Scout Enterprise-Datenbank muss der Name der Anwendungsrolle in der Tabelle **System** hinterlegt werden. Name und Passwort können entweder verschlüsselt oder unverschlüsselt hinterlegt werden.

1. Fügen Sie für Namen und Passwort jeweils eine Zeile hinzu:

Verschlüsselt	Unverschlüsselt
`ParamName=RName` und `ParamVal=<Name der Rolle>`	`ParamName=RName2` und `ParamVal=<Name der Rolle>`
`ParamName=RPass` und `ParamVal=<Kennwort der Rolle>`	`ParamName=RPass2` und `ParamVal=<Kennwort der Rolle>`

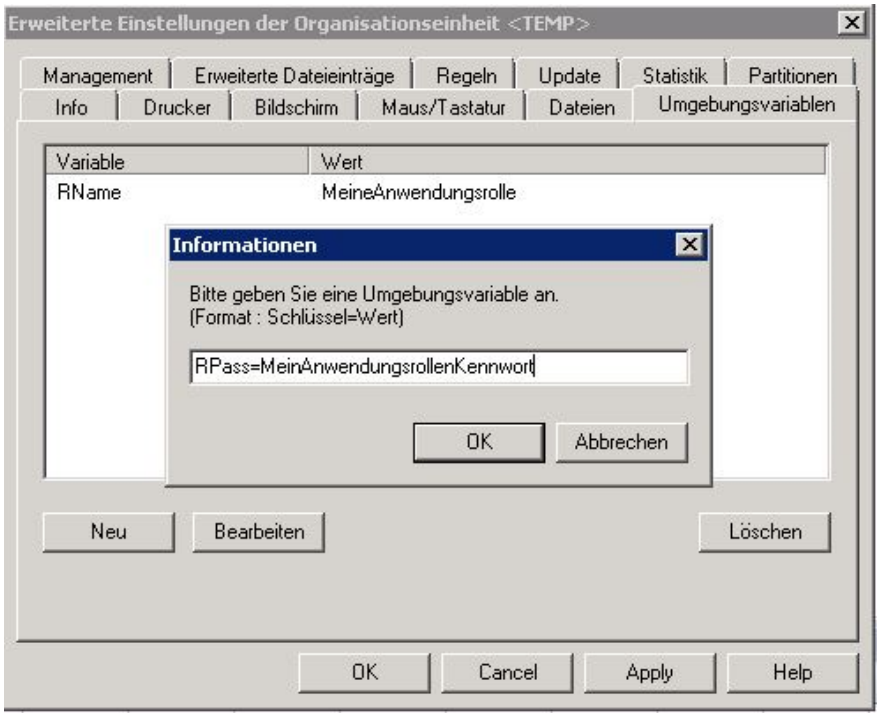
2. Wenn Sie die Daten der Anwendungsrolle verschlüsselt angeben, so müssen Sie Namen und Password für die Rolle verschlüsseln. Für weitere Informationen siehe Werte für SQL-Anwendungsrolle verschlüsseln.

Beim Starten der Scout Enterprise-Konsole werden die Felder ausgelesen und die Anwendungsrolle gesetzt.

2.3.4. Werte für SQL-Anwendungsrolle verschlüsseln

Wenn Sie eine SQL-Anwendungsrolle mit verschlüsselten Werten verwenden möchten, müssen Sie Name und Passwort verschlüsseln.

1. Legen Sie in der Scout Enterprise-Konsole eine temporäre OU an, beispielsweise mit Namen `TEMP`.
2. Öffnen Sie das Kontextmenü der `TEMP`-OU und wählen Sie **Erweiterte Einstellungen > Umgebungsvariablen**.
3. Fügen Sie zwei neue Variablen für Name und Passwort hinzu, und erfassen Sie die Werte der Anwendungsrolle.



4. Nach dem Erfassen der Variablen klicken Sie mit der rechten Maustaste auf die Variablen und wählen im Kontextmenü **Wert verschlüsseln**.
5. Markieren Sie die Variablen und klicken Sie auf **Bearbeiten**. Kopieren Sie anschließend den verschlüsselten Wert in den Zwischenspeicher und setzen ihn in Ihrer SQL-Tabelle ein.
6. Löschen Sie die temporäre OU.

2.3.5. Scout Enterprise-Servercluster

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

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

FailureLoadBalancing

Wenn der Client bei einem Kontaktversuch auf den zuletzt verfügbaren Scout Enterprise-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 Enterprise-Server verbinden kann.

ManagerLoadBalancing

Durch den zusätzlichen Parameter

`ManagerLoadBalancer=`

in der Datei `/setup/terminal.ini` kann den Geräten ein Scout Enterprise-Server als bevorzugter Server für den Verbindungsversuch vorgegeben werden.

Der Eintrag des Parameters erfolgt über die Scout Enterprise-Konsolenfunktion **Erweiterte Dateieinträge** und kann für alle Geräte, für eine OU oder für ein einzelnes Gerät gesetzt werden.

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

Als `ManagerLoadBalancer` wird ein am DNS-Server gesondert zu setzender DNS-Eintrag verwendet, der auf den entsprechenden Scout Enterprise-Server verweist. Damit kann über den DNS-Eintrag die Zuordnung von Geräten zu einem bestimmten Scout Enterprise-Server ohne Änderung der Geräte-Konfigurationseinstellungen erfolgen und auch wieder geändert werden.

Die Auswertung des Parameters `ManagerLoadBalancer` erfolgt durch die Geräte bei jedem Client-Neustart.

Schematischer Ablauf:

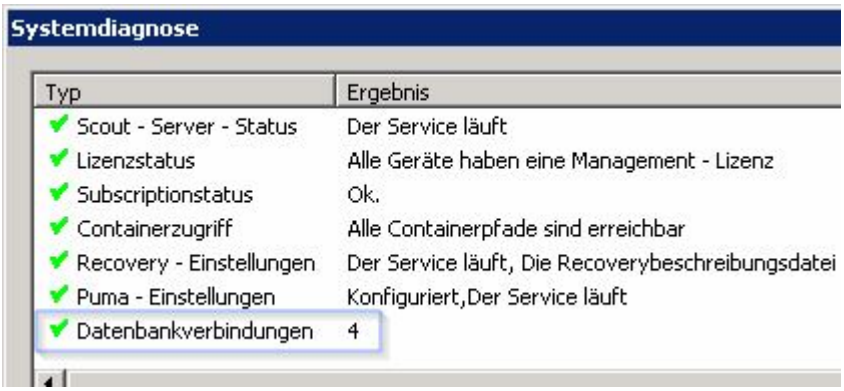
- Thin Client-Neustart
- Auflösung des DNS-Eintrages `ManagerLoadBalancer`
- Verbindung zum ermittelten Scout Enterprise-Server

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

2.3.6. Anzahl der ODBC-Verbindungen

Die Anzahl der ODBC-Verbindungen zwischen Scout Enterprise-Server und der Scout Enterprise-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 Enterprise-Konsole **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 Enterprise-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 Enterprise-Installation zu entsprechen. Dafür setzen Sie folgenden Parametereintrag in der Konfigurationsdatei `eluxd.ini` des Scout Enterprise-Servers:

Datei	`%sys-temdrive%\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.

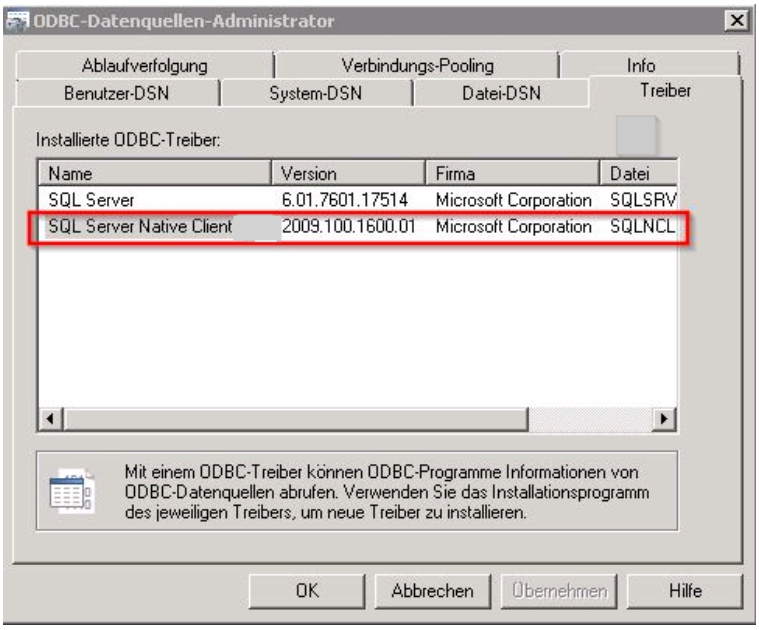
Für weitere Informationen zum Bearbeiten von `INI`-Dateien, siehe Erweiterte Dateieinträge.

2.3.7. SQL-Server Datenbankspiegelung

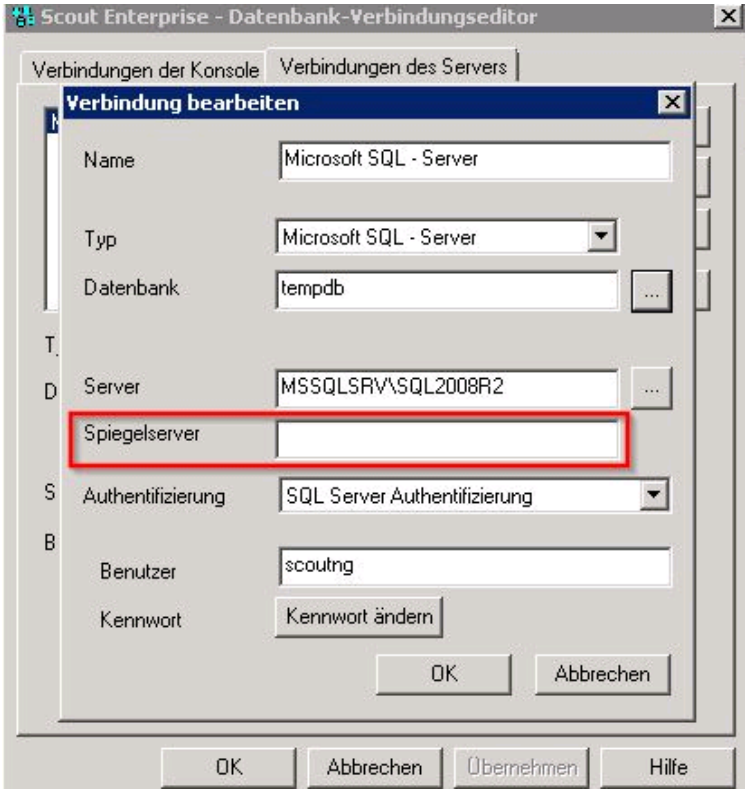
In Scout Enterprise Version 14.0.0 bis 14.5.0 wird der Failover-Mechanismus der Microsoft SQL Server-Datenbankspiegelung unterstützt.

Um die Unterstützung der SQL Datenbankspiegelung zu aktivieren,müssen Sie zunächst den Microsoft SQL Server Native Clients auf dem Scout Enterprise Server installieren.
Die entsprechende `MSI`-Datei `sqlncli.msi` kann gesondert oder als Bestandteil eines Microsoft SQL Server Feature Packs von Microsoft heruntergeladen werden.

Nach erfolgreicher Installation des Microsoft SQL Server Native Clients ist der Treiber in den ODBC-Datenquellen zu sehen:



Im Scout Enterprise Datenbank-Verbindungseditor können Sie daraufhin den Spiegelserver konfigurieren:



Hinweis
Wenn der Microsoft SQL Server Native Client auf dem Scout Enterprise Server nicht installiert ist, wird das Feld **Spiegelserver** im Dialog des Scout-Enterprise Datenbank-Verbindungseditors nicht angezeigt.

Nach erfolgreicher Konfiguration des Scout Enterprise Servers zur Nutzung eines Spiegelservers sind alle relevanten Scout Enterprise-Komponenten in der Lage, den Failover-Mechanismus der Microsoft SQL Server-Datenbankspiegelung zu unterstützen. Zu beachten ist hierbei, dass die User Credentials des Benutzers, der für den Zugriff auf die Datenbanken verwendet wird, für alle betroffenen SQL Server-Instanzen identisch sein müssen - dies betrifft auch den Security Identifier (SID). Details zur Einrichtung der Microsoft SQL Server-Datenbankspiegelung entnehmen Sie bitte der entsprechenden Microsoft-Dokumentation.

2.4. Scout Enterprise Management Suite installieren

Voraussetzung
Bei Verwendung von Microsoft SQL Server: Die Datenbanken für Scout Enterprise und Scout Enterprise Statistik müssen vor Beginn der Installation in Microsoft SQL Server vorhanden sein. Die Tabellen werden während der Installation vom System erzeugt. Für weitere Informationen siehe Datenbankunterstützung.

1. Laden Sie die aktuelle Scout Enterprise-Version von www.myelux.com herunter und entpacken Sie die `ZIP`-Datei.

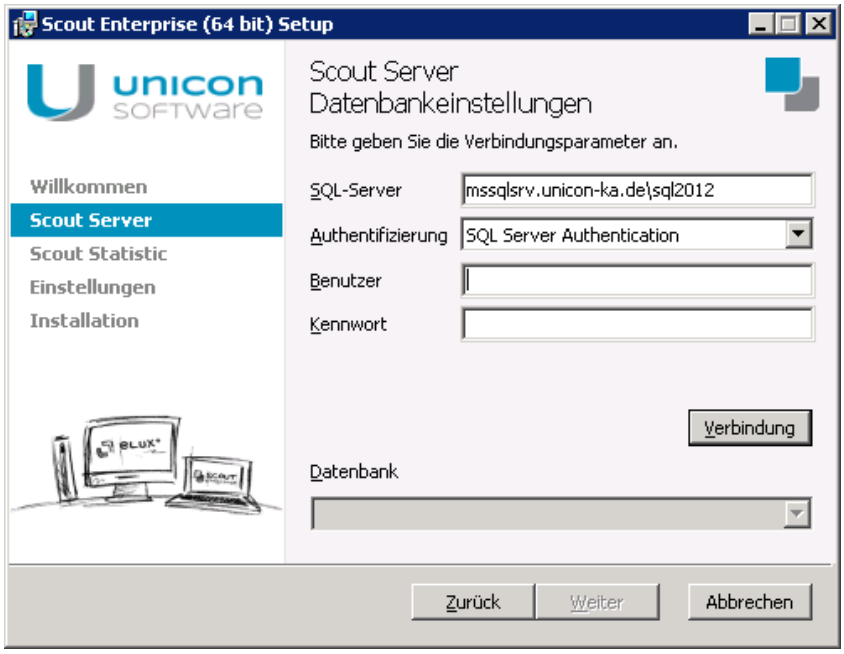
   Hinweis
   Führen Sie das Setup von der lokalen Festplatte aus, also nicht von einem USB-Stick, CD-Laufwerk oder Netzlaufwerk.

2. Führen Sie die Datei `Scout Enterprise.exe`[1] als Administrator aus.
3. Wählen Sie die Installationssprache aus. Wählen Sie dann den gewünschten Typ der Datenbank (`MS SQL Server` oder `MS SQL LocalDB`). Für weitere Informationen siehe Datenbankunterstützung.
   Klicken Sie auf **Install**.
4. Lesen Sie die Lizenzvereinbarung und stimmen Sie zu.
5. Wenn Sie einzelne Komponenten von der Installation ausschließen möchten oder das Installationsverzeichnis ändern möchten, klicken Sie auf **Benutzerdefiniert**. Nach dem Ändern der relevanten Optionen klicken Sie auf **Weiter**.

   Für die Standard-Installation klicken Sie auf **Installieren**.
6. Wenn Sie Microsoft SQL LocalDB verwenden, geben Sie den relevanten Windows-Benutzer und das Kennwort an. Für weitere Informationen siehe SQL LocalD.
7. Wenn Sie Microsoft SQL Server verwenden, geben Sie die Daten zur Verbindung mit der bereits vorhandenen **Scout Enterprise**-Datenbank ein:
   - *<SQL-Server\Instanz>*
   - `SQL Server-Authentifizierung` oder `Windows-Authentifizierung`

     Für weitere Informationen siehe Authentifizierungsmodus.
   - *<SQL-Benutzer>*
   - *<Kennwort>*

[1] bis Scout Enterprise Management Suite Version 14.6: `setup.exe`



Klicken Sie auf **Verbindung** und wählen anschließend Ihre **Scout Enterprise**-Datenbank aus dem Listenfeld.

Überprüfen oder bearbeiten Sie im nächsten Dialog die Daten zur Verbindung mit der bereits vorhandenen Scout Enterprise **Statistik**-Datenbank. Klicken Sie auf **Verbindung** und wählen anschließend Ihre **Statistik**-Datenbank aus.

Geben Sie zur Installation des Scout Enterprise-Statistikservice den TCP-Port und das Zertifikat des Statistikservices an.

Achtung

Ein gültiges Zertifikat mit dem Zweck Serverauthentifizierung ist Voraussetzung für die Übermittlung der 'keep alive' messages und der statistischen Geräteinformationen von den Geräten über HTTPS an den Scout Enterprise-Statistikservice. Optional kann die Installation des Scout Enterprise-Statistikservice über die benutzerdefinierte Installation abgewählt werden.

8. Geben Sie eine erste Organisationseinheit (OU) ein.
9. Geben Sie Sprache, Tastaturbelegung und Zeitzone an.
10. Wenn gewünscht, definieren Sie Anwendungen. Anwendungen können auch später definiert werden. Für weitere Informationen siehe Anwendungsdefinition.
11. Starten Sie die Installation.

Nach erfolgreicher Installation steht standardmäßig das Konto `Administrator` *mit Kennwort* `elux` *zur Verfügung.*

Hinweis

Ändern Sie das Kennwort sofort, um unberechtigten Zugriff zu verhindern:

- Konsolen-Kennwort ändern oder
- Administratorenverwaltung aktivieren

2.5. Unbeaufsichtigte Installation

Scout Enterprise unbeaufsichtigt installieren

- Führen Sie die Datei `Scout Enterprise.exe`[1] mit den folgenden Parametern aus:
  `"Scout Enterprise.exe" /s /v"/qn"`

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

.

Optionen	Beschreibung
/v"UCPROP_DBTYPE=*2*"	5=Microsoft SQL LocalDB 2= Microsoft SQL-Server
/v"UCPROP_DBNAME=*Scout*"	Scout Enterprise-Datenbank
/v"UCPROP_DBSERVER=*your-server.your-domain.de\your_instance*"	Datenbank-Server der Scout Enterprise-Datenbank
/v"UCPROP_DBUSER=*Scout-Admin*"	Datenbank-Benutzer (nur bei SQL Server-Authentifizierung)
/v"UCPROP_DBPASSWORD_CRYPTED=*u[D``Gqu[w_*"	siehe `eluxd.ini`
/v"UCPROP_OUNAME=*your-OU*"	Anzulegende OU
/v"UCPROP_DESKTOP_LANGUAGE=*de_DE*"	Spracheinstellung für den Client-Desktop
/v"UCPROP_KEYBOARD_LANGUAGE=*de*"	Spracheinstellung für die Client-Tastatur
/v"UCPROP_LANGUAGE=*de*"	Spracheinstellung für die Scout Enterprise-Konsole beim ersten Aufruf de=deutsch en=englisch Wenn der Parameter nicht gesetzt ist, wird die im Betriebssystem eingestellte Sprache verwendet.
/v"UCPROP_DBNAME_STATISTIC=*Scout_Statistik*"	Scout Enterprise Statistik-Datenbank

[1] bis Scout Enterprise Management Suite Version 14.6: `setup.exe`

Optionen	Beschreibung
/v"UCPROP_DBSERVER_STATISTIC=*your-server.your-domain.de\your_instance*"	Datenbank-Server der Scout Enterprise Statistik-Datenbank
/v"UCPROP_DBUSER_STATISTIC=*Scout-Admin*"	Datenbank-Benutzer (nur bei SQL Server-Authentifizierung)
/v"UCPROP_DBPASSWORD_CRYPTED_STATISTIC=*u[D``Gqu[w_*"	siehe eluxd.ini
/v"UCPROP_STATISTIC_SERVER_PORT=*22124*"	TCP-Port des Scout Enterprise-Statistikservice
/v"UCPROP_STATISTIC_CERTIFICATES=\"*MyCert_ServAuth*\""	Zertifikat des Scout Enterprise-Statistikservice
/v"ADDLOCAL=*Komponente 1,Komponente 2*" Beispiel: `/v"ADDLOCAL=Console,Server,Report"`	Optionaler Parameter zur Installation von bestimmten Komponenten. Nur die angegebenen Komponenten werden installiert.

Beispiel:

```
"Scout Enterprise.exe" /s /v"/qn" /v"/lv c:\temp\SetupLog.log"
/v"UCPROP_DBTYPE=2" /v"UCPROP_DBNAME=Scout" /v"UCPROP_DBSERVER=your-server.your-domain.de\instance_sql2012" /v"UCPROP_DBUSER=Scout-Admin"
/v"UCPROP_DBPASSWORD_CRYPTED=u[D``Gqu[w_" /v"UCPROP_OUNAME=MyOU"
/v"UCPROP_DESKTOP_LANGUAGE=de_DE" /v"UCPROP_KEYBOARD_LANGUAGE=de"
/v"UCPROP_DBNAME_STATISTIC=Scout_Statistik" /v"UCPROP_DBSERVER_
STATISTIC=your-server.your-domain.de\instance_sql2012" /v"UCPROP_
DBUSER_STATISTIC=Scout-Admin" /v"UCPROP_DBPASSWORD_CRYPTED_STATISTIC=u
[D``Gqu[w_" /v"UCPROP_STATISTIC_SERVER_PORT=22124" /v"UCPROP_STATISTIC_
CERTIFICATES=\"MyCert_ServAuth\"" /v"ADDLOCAL-
L=Console,Server,Report,Elias,ScoutStatistic"
```

Installierbare Scout Enterprise-Komponenten[1]

Server
Console
Recovery
Elias
Report
Puma
ScoutStatistic

[1] bis Scout Enterprise Management Suite Version 14.6 wurden für eine 32 Bit-Installation folgende abweichende Komponentennamen verwendet: Server32, Console32, Recovery32, Elias32, Report32, Puma32.

Unbeaufsichtigte Deinstallation durchführen

- Verwenden Sie folgenden Befehl:
  `"Scout Enterprise.exe" /x /s /v"/qn"`

2.6. Update auf neue Scout Enterprise-Version

Um Ihr System auf eine neuere Scout Enterprise-Version zu aktualisieren, laden Sie die relevante `ZIP`-Datei von unserem Portal www.myelux.com herunter. Entpacken und installieren Sie die neue Version unter Angabe Ihrer vorhandenen Datenbank.

Abhängig vom Funkionszuwachs können beim Update auf eine neue Version längere Laufzeiten bei der Konvertierung der Scout Enterprise-Datenbank entstehen. Falls dies zutrifft, enthalten die entsprechenden Release Notes auf www.myelux.com detaillierte Informationen.

2.7. Scout Enterprise Management Suite deinstallieren

- Verwenden Sie die Systemsteuerung, um Scout Enterprise zu deinstallieren.

Oder:

1. Führen Sie die Datei `Scout Enterprise.exe`[1] als Administrator aus.
2. Wählen Sie **Programm entfernen**.

[1] bis Scout Enterprise Management Suite Version 14.6: `setup.exe`

2.8. Verschlüsselung

Die Verschlüsselung zwischen Scout Enterprise Server und den eLux Clients erfolgt über das proprietäre Scout Enterprise Management-Protokoll auf TCP/IP-Basis unter Verwendung des gesicherten Ports 22123 mit AES-256-Verschlüsselung. Auf den Clients muss eLux RP eingesetzt werden.

Wenn Sie eine Firewall verwenden, muss der Port 22123 freigeschaltet werden.

2.9. Pfade

Programmverzeichnis

Scout Enterprise wird ab der Version 14.0 in das Verzeichnis

`%PROGRAMFILES%\Unicon\Scout`

installiert. Ältere Versionen wurden nach

`%PROGRAMFILES%\Unicon\ScoutNG` installiert.

Verzeichnis für Serverdateien

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

`%PUBLIC%\Documents\UniCon`

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

Verzeichnis für Benutzer-Dateien

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

`%USERPROFILE%\Documents\UniCon\`

Hinweis
Die Pfade können je nach Windows-Version variieren.

2.10. Zertifikate

Verschiedene Anwendungen und Funktionen erfordern die Bereitstellung von Zertifikaten.

- Die Dateierweiterung muss `.pem` (Base64) oder `.crt` (DER) sein.
- Die Übertragung von Zertifikaten zum Client erfolgt über die Funktion Dateien in der Scout Enterprise-Konsole.
- Die Zertifikate werden lokal am Client im Zertifikatsstore `/setup/cacerts/` oder einem Unterverzeichnis gespeichert. Die folgende Tabelle gibt einen Überblick:

Funktion	Komponente	Verzeichnis
Benutzeranmeldung	ADS (UserAuth)	/setup/cacerts/login
Benutzeranmeldung	ADS+Smartcard (UserAuth)	/setup/cacerts/login
SSL-Verschlüsselung	Firefox	/setup/cacerts/firefox
SSL-Verschlüsselung	Chromium	/setup/cacerts/browser
SSL-Verschlüsselung	Citrix (ICA client)	/setup/cacerts/ und /setup/cacerts/intcerts
SSL-Verschlüsselung	VMware Horizon View client	/setup/cacerts/
Netzwerkanmeldung	WPA-/X-Supplikant (xsupplicant) X509/Radius SCEP (Zertifikatsüberwachung)	/setup/cacerts/ /setup/cacerts/scep
VPN-Client/ OpenVPN	vpnsystem	/setup/openvpn
VPN-Client / Cisco AnyConnect	vpnsystem	/setup/cacerts/ca und /setup/cacerts/client
Firmware-Update mit Zertifikatsprüfung	BaseOS	/setup/cacerts
RDP-Client	eLuxRDP	/setup/cacerts

Hinweis

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

2.11. Lizenzierung

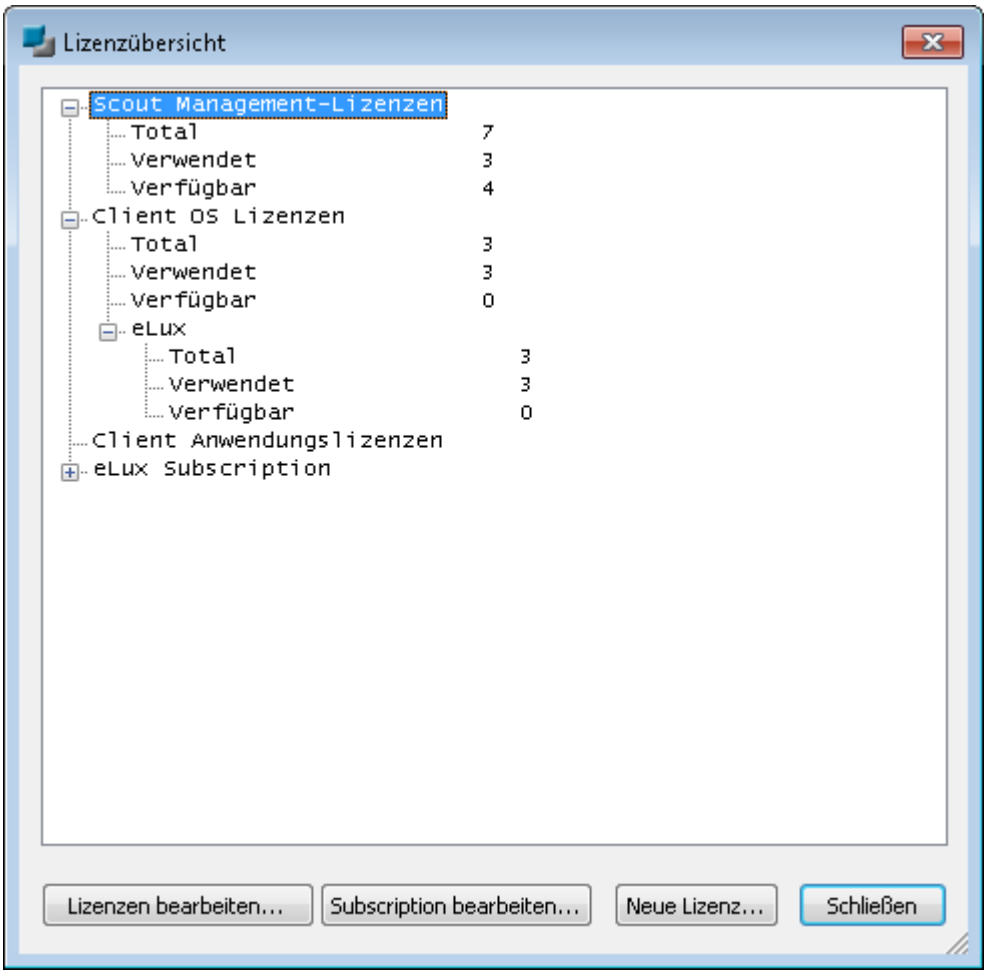
Neben der Betriebssystem-Lizenz benötigt ein Client eine Scout Enterprise Management-Lizenz, damit er über die Scout Enterprise Management Suite verwaltet werden kann. Detaillierte Informationen zu unserem Lizenzmodell finden Sie in unserem White Paper Lizenzmodell und Subscription.

Lizenzübersicht

Der Scout Enterprise-Server fungiert auch als Lizenzserver und verwaltet folgende Lizenz-informationen

- Scout Enterprise Management -Lizenzen
- Client Betriebssystem-Lizenzen
- Client-Anwendungs-Lizenzen
- Subscription

Eine Übersicht über alle verwalteten Lizenzen erhalten Sie in der Scout Enterprise-Konsole unter **Optionen > Lizenzinformation...**



Lizenzen, die unter **Verfügbar** angegeben sind, sind noch nicht zugewiesen (oder wieder frei geworden). Sie werden automatisch neuen Clients zugewiesen, wenn diese noch nicht lizenziert sind und den Scout Enterprise-Manager kontaktieren.

Neue Lizenzen

Für neue Lizenzen müssen Sie, sofern es sich nicht um integrierte (builtin) Lizenzen handelt, im Product Activation Center unseres Portals **myelux.com** einen Aktivierungscode erzeugen. Dazu benötigen Sie den License Base Key auf Ihrem Lizenzzertifikat.

Im zweiten Schritt geben Sie die neuen Lizenzen in der Scout Enterprise-Konsole, unter **Lizenzübersicht > Neue Lizenz...** ein und aktivieren die neuen Lizenzen anschließend mit Hilfe des Aktivierungscodes.

Eine genaue Anleitung finden Sie unter Aktivierung der Lizenzen in unserem White Paper **Lizenzmodell und Subscription**.

2.12. Problembehandlung

Fehlermeldung	Ursache	Lösung
Dateizugriffsfehler beim Prüfen des HTTP/FTP-Servers (Fehlernummer=404)	Mögliche Ursache sind fehlende MIME Type-Einträge für die Dateiendungen `.idf`, `.epm`, `.fpm` und `.gz` als text/plain am Webserver	Fügen Sie dem Microsoft Internet Information Server (IIS) die Scout Enterprise MIME-Typen hinzu, indem Sie das VB-Skript `ScoutAddMimeToIIS.vbs` ausführen, siehe unten.

MIME-Typen in IIS über VB-Skript hinzufügen

1. Downloaden Sie von www.myelux.com unter **eLux Software Packages > eLux RP Container > Released packages >** *Neueste Version* **> Bundles > eLuxRP-*_AllPackages** die Datei `AllPackages.zip`.
2. Öffnen Sie die `zip`-Datei und den Ordner `Support`. Kopieren Sie die Datei `ScoutAddMimeTollS.vbs` nach `C:\temp`.
3. Führen Sie das VB-Skript mit Administratorrechten aus.

   *Die Meldung **Add Scout MIME types to Internet Information Server** wird angezeigt.*
4. Bestätigen Sie mit **OK**.

   *Die Meldung **Added MIME types successfully** wird angezeigt.*

Hinweis
Ggf. müssen Sie das VB-Skript in der Windows-Eingabeaufforderung in C:\TEMP mit dem Kommando `wscript ScoutAddMimeToIIS.vbs` ausführen.

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 Enterprise-Versionen nicht mehr unterstützt. Für die Konvertierung einer MDB-Datenbank auf LocalDB ist Scout Enterprise Version 14.6.1 erforderlich, bevor Sie auf eine neuere Version aktualisieren können.	Installieren Sie zunächst Scout Enterprise Version 14.6.1 (Download auf myelux.com) mit der MDB-Datenbank und starten Sie die Scout Enterprise-Konsole. Installieren Sie anschließend eine neuere Scout Enterprise-Version mit Ihrer Datenbank. Beim Starten der Scout Enterprise-Konsole wird die Konvertierung der Datenbank automatisch durchgeführt.
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.
Windows 2008 R2 Server oder **Windows 7 Professional**: Der Benutzer hat nicht das Recht, sich als Administrator anzumelden (obwohl der Benutzer zur Administratorengruppe gehört)	Bekannter Fehler im Betriebssystem: Die Abfrage, ob ein Benutzer zur Gruppe Administrator gehört, schlägt fehl.	Installieren Sie den Microsoft-Hotfix https://support.microsoft.com/de-de/kb/2830145

Für weitere Informationen siehe SQL LocalDB.

3. Oberfläche

3.1. Organisationsstruktur

Das Hauptfenster der Scout Enterprise-Konsole zeigt im oberen linken Bereich die hierarchisch organisierte Organisationsstruktur mit den verwalteten Geräten in einer Baumstruktur an. Bei der ersten Anmeldung sehen Sie die standardmäßig angelegten Organisationseinheiten **Lost&Found** und **Enterprise**.[1] Letztere dient als oberster Knoten Ihrer Organisationsstruktur.

Auf der obersten Ebene sind drei Anwendungen zur Verbindung gegen ein Backend vordefiniert:[2] **RDP**, **StoreFront** und **VMware Horizon**. Für weitere Informationen siehe Anwendungsdefinitionen.

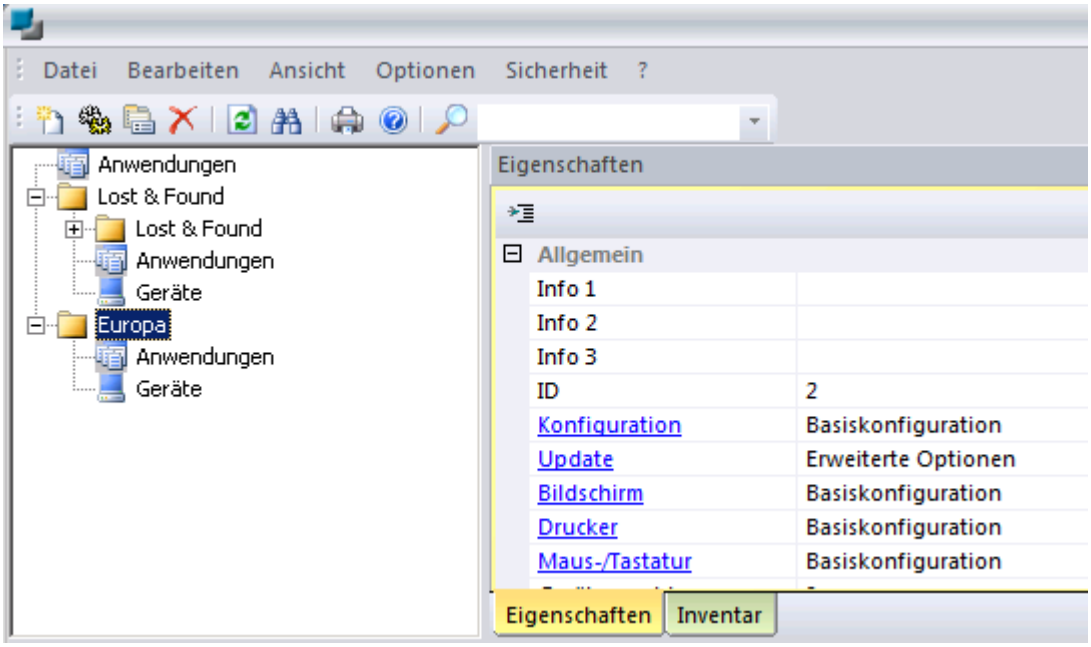
Zu jeder Organisationseinheit (im folgenden **OU**) können Sie Anwendungen, Geräte sowie weitere Organisationseinheiten hinzufügen. Jede OU kann untergeordnete OUs, Anwendungen und Geräte enthalten.

Standardmäßig gilt das Vererbungsprinzip: Anwendungen – genauer Anwendungsdefinitionen – werden auf untergeordnete OUs vererbt, und Konfigurationen werden nach unten bis auf die Geräte-Ebene vererbt.

Wenn einer OU ein neues Gerät hinzugefügt wird, erhält es automatisch die Anwendungsdefinitionen und Konfiguration dieser OU.

Einzelne Geräte und Anwendungsdefinitionen können per Drag&Drop oder Zwischenablage von einer OU zu einer anderen verschoben werden. Den Geräten werden dann automatisch die Eigenschaften der neuen Organisationseinheit zugewiesen (Voraussetzung: Vererbung ist eingeschaltet).

Für weitere Informationen siehe Geräte-Konfiguration/Konzept.



[1] ab Scout Enterprise Management Suite Version 15.0
[2] ab Scout Enterprise Management Suite Version 15.0

Für das in der Baumstruktur markierte Element werden im **Eigenschaften**-Fenster verschiedene Details angezeigt.

Neue OU hinzufügen

1. Öffnen Sie für die relevante OU das Kontextmenü und wählen Sie **Hinzufügen > Organisationseinheit...**

   *Der Dialog **Erweiterte Konfiguration** öffnet.*

2. Geben Sie einen aussagekräftigen Namen für die neue OU ein.
3. Wenn gewünscht, geben Sie weitere Informationen in die **Info**-Felder ein und bearbeiten Sie Felder in den anderen Registern.
4. Bestätigen Sie mit **Übernehmen** und **OK**.

Die neue OU wird in der Baumstruktur angezeigt und enthält die Ordner  Anwendungen und  Geräte.

3.2. Symbole

Symbol	Beschreibung
	Organisationseinheit (OU)
	Anwendungen
	Gerät, war noch nicht mit dem Scout Enterprise-Server verbunden (Beispiel: Geräte-Import)
	Gerät, eingeschaltet und betriebsbereit
	Gerät, ausgeschaltet oder nicht verfügbar
	Gerät, Desktop wird gerade initialisiert bzw. das Anmeldefenster ist geöffnet
	Gerät, Update läuft gerade
	Gerät, ohne gültige Lizenz zur Verwaltung mit Scout Enterprise

3.3. Fenster

Neben der Organisationsstruktur können Sie über das Menü **Ansicht > Fenster** weitere Fenster ein- oder ausblenden. Folgende Fenster stehen zur Verfügung:

Fenster	Beschreibung
Eigenschaften	Eigenschaften für markierte Anwendung, OU oder Gerät

Fenster	Beschreibung
Assets/Inventar (nur für Geräte)	Informationen zur Hardware
Dynamische Gerätegruppen	Zeigt alle definierten Dynamischen Gerätegruppen Für weitere Informationen siehe Dynamische Gerätegruppen
Unabhängige Konfigurationen	OUs und Geräte, die nicht die übergeordnete Instanz verwenden Für weitere Informationen siehe Vererbung unterbrechen – unabhängige Konfiguration
Konfigurationsvergleich	Gibt Unterschiede in den Konfigurationen von Geräten oder OUs an
OU Geräte/Anwendungen	Zeigt Geräte oder Anwendungen einer OU als Liste und ohne Symbole an Wenn Sie auf ein Gerät doppelklicken, wird das zugehörige Gerät in der Baumstruktur markiert. Diese Funktion kann deaktiviert werden, siehe unten.
Alle Geräte	Zeigt alle Geräte als Liste und ohne Symbole an Die Geräteinformationen werden nur dann von der Scout Enterprise-Datenbank geladen, wenn Sie auf die Schaltfläche **Aktualisieren** klicken. Damit wird das ungewollte Laden großer Datenmengen vermieden. Mehrere Geräte können mit STRG oder UMSCHALT markiert werden, um Kontextmenü-Funktionen wie Kommandos durchzuführen. Wenn Sie auf ein Gerät doppelklicken, wird das zugehörige Gerät in der Baumstruktur angezeigt. Diese Funktion kann deaktiviert werden, siehe unten. Um das Fenster zu durchsuchen, verwenden Sie das **Suchen**-Feld der Symbolleiste, geben eine Zeichenfolge ein und drücken UMSCHALT+RETURN. Drücken Sie UMSCHALT+F3, um zum nächsten Treffer zu springen. Für weitere Informationen siehe Nach Anwendungen, Geräten oder OUs suchen.

Spalten sortieren

- Klicken Sie auf den Spaltenkopf einer Spalte, um die Zeilen zu sortieren.

Eigenschaften ein-/ausblenden

- Klicken Sie auf die Schaltfläche , um die anzuzeigenden Eigenschaften zu konfigurieren. Alternativ verwenden Sie das Kontextmenü.

Zusätzliche Optionen im Eigenschaften-Fenster für Geräte und OUs

Markiertes Element	Option	Beschreibung
Gerät	**Konfiguration**	Doppelklick öffnet die relevante **Geräte-Konfiguration**
Gerät	**Image**	Doppelklick öffnet ELIAS mit der für das Gerät konfigurierten IDF-Datei im relevanten Container
Gerät	**Updatestatus**	Doppelklick oder **...** öffnet die **Update-Info** für das Gerät mit Informationen über die durchgeführten Updates. Für weitere Informationen siehe Update-Protokoll.
OU	**Konfiguration**	Doppelklick öffnet die relevante Geräte-Konfiguration
OU	**Update**	Doppelklick öffnet die relevanten **Update**-Einstellungen in der **Erweiterten Konfiguration** für diese OU.
OU	**Bildschirm**, **Drucker**, **Maus/Tastatur**	Doppelklick öffnet die relevante Konfiguration (**Geräte-Konfiguration** oder **Erweiterte Konfiguration**) für Bildschirm, Drucker bzw. Maus/Tastatur.
OU	ID	Zeigt die ID dieser OU. Zusätzlich zum Dezimalwert der ID können Sie den Hexadezimalwert einblenden. Dazu setzen Sie in der Registry folgenden Eintrag: Schlüssel: HKEY_CURRENT_USER\Software\UniCon\Scout\Settings Wertname: `DisplayHexOUID` Werttyp: `DWORD:32` Wert: `1`

Hinweis

Verwenden Sie die blau dargestellten Links, um schnell und zuverlässig zu den jeweils relevanten Dialogen für Konfiguration und Information zu gelangen!

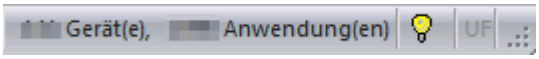
Funktion Doppelklick auf Gerät deaktivieren

Standardmäßig bewirkt ein Doppelklick auf ein Gerät innerhalb einer Geräteliste, dass das zugehörige Gerät in der Baumstruktur angezeigt und markiert wird. Dieses Verhalten kann deaktiviert werden:

- Setzten Sie folgende Registry-Einträge mit Werttyp `DWORD:32` und Wert: `1`:

  HKEY_CURRENT_USER\Software\UniCon\Scout\Settings
  DisableDoubleClick_OUDevices_View
  DisableDoubleClick_AllDevices_View
  DisableDoubleClick_DCG_View

3.4. Statusleiste



Die Statusleiste zeigt im rechten Bereich die Anzahl aller Geräte und Anwendungen.

Per Doppelklick auf das Lampensymbol zeigen Sie die Alarmmeldungen an (Fehler, Warnung, Info) wie beispielsweise **Scout Enterprise-Server wurde beendet** oder **Konnte Scout Serverprotokoll nicht schreiben**. Das Lampen-Symbol wird gelb angezeigt, sobald ein neuer Eintrag erzeugt wurde.

3.5. Nach Geräten, OUs oder Anwendungen suchen

Hinweis
Die Suche berücksichtigt die im **Suchen**-Dialog eingestellten Suchparameter.

Schnelle Suche in der Baumstruktur

1. Klicken Sie in die Baumstruktur, um den Fokus zu setzen.
2. Drücken Sie STRG+F oder klicken Sie in das **Suchen**-Feld der Symbolleiste.
3. Geben Sie den Namen einer Anwendung, eines Geräts oder einer OU ein.

   Je nach Einstellung genügen Wortteile.

4. Drücken Sie RETURN oder klicken Sie auf das Lupen-Symbol.

   Das erste zutreffende Objekt wird in der Baumansicht angezeigt und markiert.
5. Drücken Sie F3 oder klicken Sie auf das Lupen-Symbol, um zum nächsten Treffer zu springen.

Schnelle Suche im Fenster Alle Geräte

1. Klicken Sie in das Fenster **Alle Geräte**, um den Fokus zu setzen.
2. Drücken Sie STRG+F oder klicken Sie in das **Suchen**-Feld der Symbolleiste.
3. Geben Sie den Namen eines Geräts ein.

   Je nach Einstellung genügen Wortteile.
4. Drücken Sie RETURN oder klicken Sie auf das Lupen-Symbol.

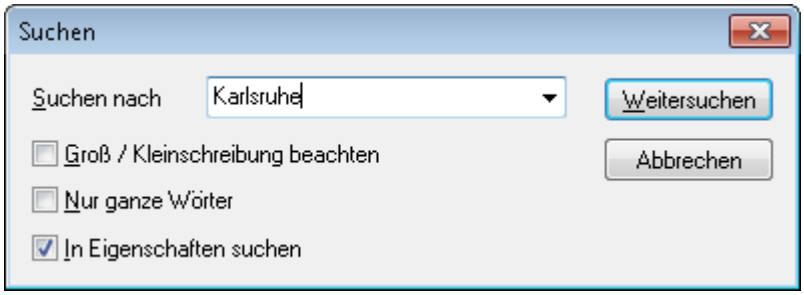
   *Das erste zutreffende Objekt wird im Fenster **Alle Geräte** angezeigt und markiert.*
5. Drücken Sie F3 oder oder klicken Sie auf das Lupen-Symbol, um zum nächsten Treffer zu springen.

Hinweis
Wenn der Fokus nicht im Fenster **Alle Geräte** ist, können Sie trotzdem dort suchen: Drücken Sie UMSCHALT+RETURN, um die Suche nach dem angegebenen Objekt auszulösen und UMSCHALT+F3, um zum nächsten Treffer zu springen.

Suche über Dialog und Einstellen der Suchparameter

1. Drücken Sie STRG+UMSCHALT+F oder wählen Sie **Bearbeiten > Suchen...**

   *Der **Suchen**-Dialog öffnet.*



2. Geben Sie den Namen einer Anwendung, eines Geräts oder einer OU ein.

   Je nach Einstellung genügen Wortteile.

3. Wenn gewünscht, passen Sie die Suchparameter an:

Option	Beschreibung
Groß-/Kleinschreibung beachten	Nur genaue Übereinstimmungen in der Groß-/Kleinschreibung werden gefunden
Nur ganze Wörter	Nur genaue Übereinstimmungen werden gefunden, keine Wortteile
In Eigenschaften suchen	Die Suche wird auch auf **Eigenschaften**- und **Inventar**-Felder angewendet. Beispielsweise können Sie nach einem Hersteller oder nach einer MAC-Adresse suchen.

> **Hinweis**
> Die Suchparameter bleiben nach der Suche aktiv und werden auch auf die Schnelle Suche angewendet.

   Das erste zutreffende Objekt wird in der Baumansicht angezeigt und markiert.

4. Klicken Sie auf **Weitersuchen** oder drücken Sie F3, um zum nächsten Treffer zu springen.

3.6. Elemente verschieben und kopieren

Geräte, OUs und Anwendungen können innerhalb der Organisationsstruktur von einer OU in eine andere OU verschoben werden. Wenn die Vererbung eingeschaltet ist, erhalten verschobene Geräte und OUs nach dem Verschieben die Eigenschaften der neuen übergeordneten OU.

Gerät, OU oder Anwendung verschieben

1. Machen Sie Quell- und Zielposition des relevanten Elements in der Baumstruktur sichtbar.

   Als Zielposition wählen Sie das Symbol der Ziel-OU oder einen gültigen Bereich unterhalb der Ziel-OU.

2. Ziehen Sie das Element per Drag&Drop von der Quellposition an die Zielposition.
   oder
   Verschieben Sie das Element per Kontextmenü oder STRG-X in den Zwischenspeicher und

fügen Sie es an der Zielposition per Kontextmenü oder STRG-V ein.

3. Bestätigen Sie mit **Ja**.

Das Element wird in die Ziel-OU verschoben.

Anwendung kopieren

Hinweis
Anwendungen in der Organisationsstruktur sind Anwendungsdefinitionen und beinhalten keine Software. Die Software muss zusätzlich über das IDF konfiguriert und zur Verfügung gestellt werden.

1. Machen Sie Quell- und Zielposition der relevanten Anwendung in der Baumstruktur sichtbar.

   Als Zielposition wählen Sie das Symbol der Ziel-OU oder den Zweig **Anwendungen** unterhalb der Ziel-OU.

2. Ziehen Sie die Anwendung per Drag&Drop mit gedrückter STRG-Taste von der Quellposition an die Zielposition
   oder
   Kopieren Sie ddie Anwendung per Kontextmenü oder STRG-C in den Zwischenspeicher und fügen Sie sie an der Zielposition per Kontextmenü oder STRG-V ein.

3. Bestätigen Sie mit **Ja**.

Die Anwendung wird in die Ziel-OU kopiert.

Hinweis
Anwendungen können auch von einem beliebigen Client-Gerät in eine Scout Enterprise-OU kopiert werden. Für weitere Informationen siehe Anwendungen von Client zu Scout Enterprise hochladen.

3.7. OU auf höchste Ebene verschieben

Hinweis
Diese Funktion kann nur auf eine OU angewendet werden.

- Öffnen Sie für die relevante OU das Kontextmenü und wählen Sie **Bearbeiten > Zu Basis-OU machen**.

Die OU wird zu einer Basis-OU gemacht und auf der obersten Ebene angezeigt. Konfiguration und Vererbung bleiben wie eingestellt. Wenn die Vererbung aktiv ist, sind die Einstellungen der Basis-Konfiguration gültig.

3.8. Geräteliste drucken

Hinweis
Die Druck-Funktion ist ab Scout Enterprise Management Suite Version 14.9 nicht mehr verfügbar. Verwenden Sie den Report-Generator, um Gerätelisten nach Ihren Kriterien zu erstellen.

1. Wählen Sie **Datei > Drucken**.
2. Wählen Sie im Dialog **Drucken** Drucker und Seitenformat aus und bestätigen mit **OK**.

4. Geräteverwaltung

Damit Scout Enterprise Client-Geräte mit eLux oder anderen Betriebssystemen verwalten kann, müssen die MAC-Adressen der Clients in Scout Enterprise registriert sein. Für das Registrieren und Einbinden der Clients gibt es verschiedene Vorgehensweisen:

- Automatische Geräteerfassung
- Discovery: Geräte über die IP-Adresse suchen
- Reverse Discovery

Neue Geräte müssen einer Organisationseinheit (OU) zugeordnet werden. Sie können konfigurieren, ob neue Geräte

- standardmäßig in eine hierfür festgelegte OU aufgenommen werden (**Standard-OU**)
- automatisch über den OU-Filter nach definierbaren Kriterien zugeordnet werden
- über die Reservierung von Geräteprofilen bereits vor der ersten Verbindung angelegt werden.

Wie mit neuen Geräten verfahren werden soll, legen Sie im wesentlichen in **Optionen > Erweiterte Konfiguration >** Geräte fest.

Hinweis
Da die Geräte in OUs hierarchisch organisiert sind, bieten die Dynamischen Gerätegruppen eine Möglichkeit, bestimmte Funktionen OU-unabhängig auf mehrere Geräte anzuwenden.

4.1. Automatische Geräteerfassung

Beim ersten Bootvorgang sucht der Thin Client automatisch nach einem Scout Enterprise-Server. Der Client benötigt die IP-Adresse des Scout Enterprise-Servers.

Voraussetzungen für die automatische Geräteerfassung:

- Thin Client muss sich im Grundzustand befinden.
- Thin Client muss mit dem Netzwerk verbunden sein.
- Die Scout Enterprise IP-Adresse muss über einen der folgenden Server konfiguriert sein:
  - DHCP: Eine entsprechend konfigurierte DHCP-Option verweist auf die IP-Adresse/Namen des Scout Enterprise-Servers. Es können auch mehrere Scout Enterprise-Server und eine OU angegeben werden. Für weitere Informationen siehe DHCP-Konfiguration.

  oder

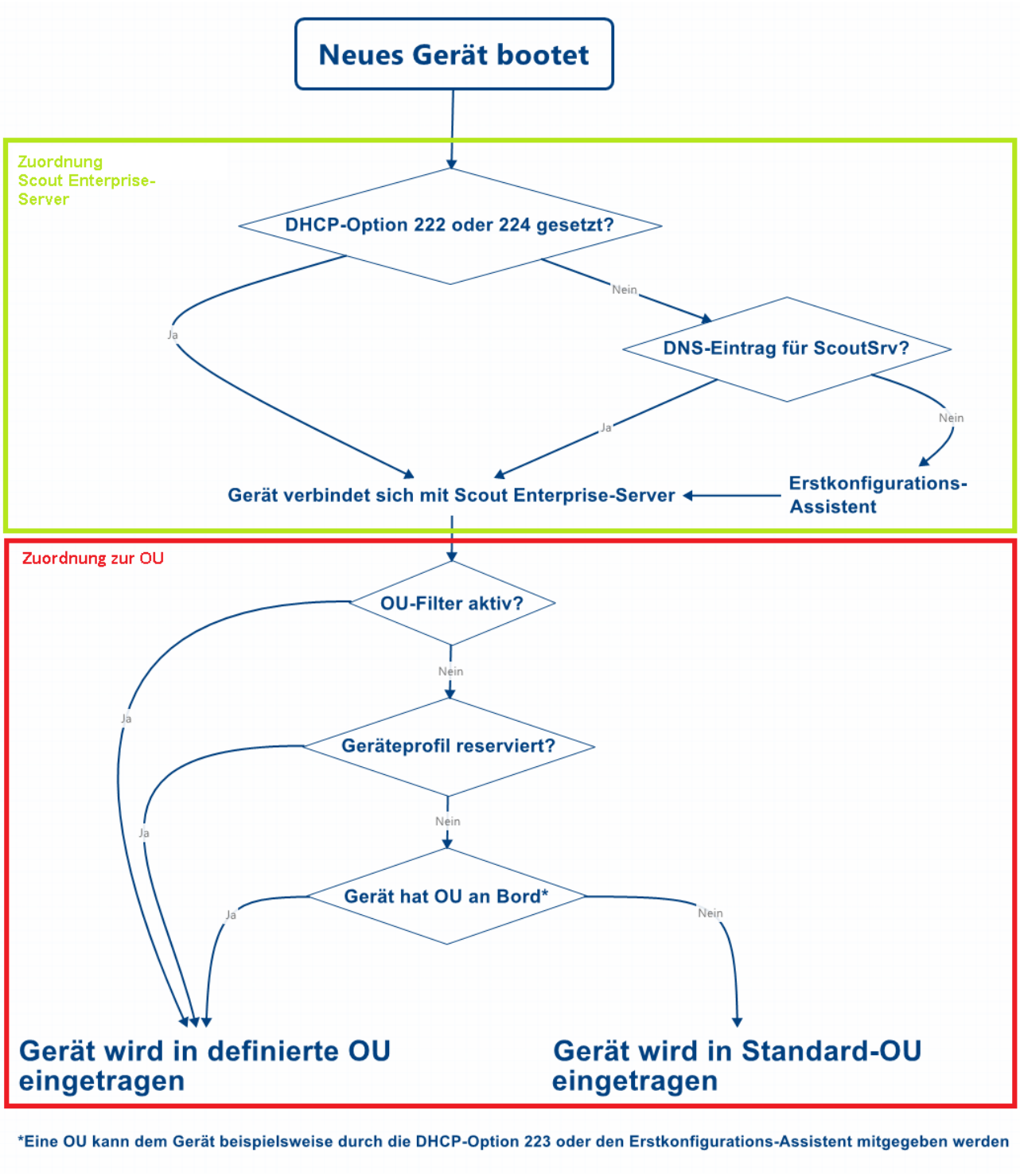
  - DNS: Der DNS-Server löst den Hostnamen des Scout Enterprise-Servers `ScoutSrv` (Groß-/ Kleinschreibung irrelevant) auf.

Wenn die IP-Adresse des Scout Enterprise-Servers weder über DNS noch über DHCP ermittelt werden kann, startet der Erstkonfigurations-Assistent und unterstützt den lokalen Benutzer bei der ersten Konfiguration.

Gerät automatisch erfassen:

1. Schalten Sie den Thin Client ein.

Wenn die Voraussetzungen zur automatischen Geräteerfassung erfüllt sind, kontaktiert der Client seinen Scout Enterprise-Server und trägt sich selbst in die definierte OU oder die Standard-OU ein. Dem Thin Client wird die Konfiguration seiner OU zugewiesen und er wird mit den neuen Einstellungen hochgefahren.



Das Ablaufdiagramm zeigt grob, wie ein neues Gerät einem Scout Enterprise-Server und einer OU zugeordnet wird. Details wie beispielsweise die Option **Nur bekannte Geräte akzeptieren** sind nicht berücksichtigt.

4.2. DHCP-Konfiguration

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 Enterprise-Servers (Option 222)
- Liste der Scout Enterprise-Server (Option 224)
- ID für die Ziel-OU am Scout Enterprise-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 2008.

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

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

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

Option	Wert
Name	Scout Enterprise-Serverliste
Datentyp	Zeichenkette
Code	224
Beschreibung	Servernamen/IP-Adressen, komma-getrennt

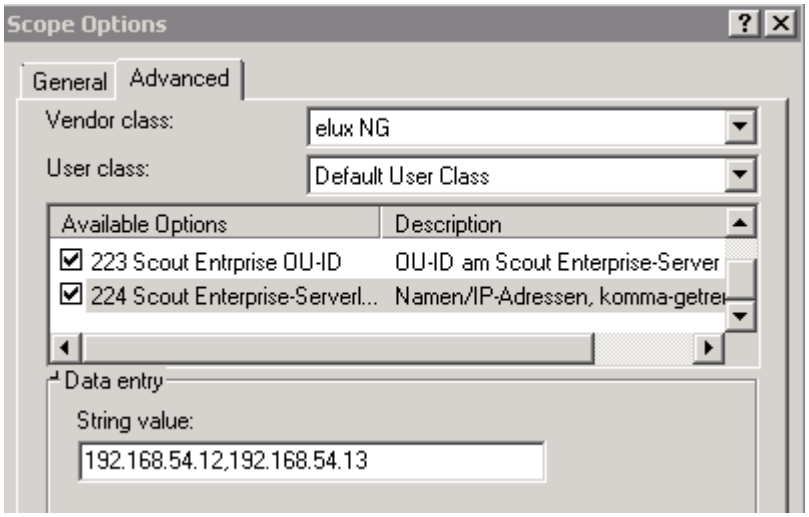
7. Wenn Sie neue Geräte über DHCP einer bestimmten OU zuordnen möchten, erstellen Sie mit **Hinzufügen** eine Option mit folgenden Angaben:

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

8. Um die Optionen zuzuordnen, markieren Sie für den relevanten DHCP-Server entweder die **Serveroptionen**, die **Bereichsoptionen** oder die **Reservierungen** und wählen dann **Vorgang > 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 Enterprise Server	*<Name oder IP-Adresse des Scout Enterprise-Servers>*
223 Scout Enterprise OU-ID	*<ID der Ziel-OU am Scout Enterprise-Server>*
224 Scout Enterprise Serverliste	*<Namen oder IP-Adressen der Scout Enterprise-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 **Vorgang > 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 Enterprise Server, Zeichenkette, 222
   - Scout Ernteprise-Serverliste, Zeichenkette, 224
   - Scout Enterprise 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 **Vorgang > Optionen konfigurieren... > Allgemein**. Aktivieren Sie die erstellten Optionen und geben Sie die entsprechenden Werte ein:

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

4.3. Geräte suchen (Discovery)

Auf der Basis von IP-Adressen können Sie Geräte im gesamten Netzwerk oder in bestimmten Subnetzen suchen. Gefundene Geräte werden automatisch in Scout Enterprise eingebunden und der angegebenen OU (**Zielgruppe**) zugeordnet. Die Geräte werden neu gestartet und erhalten die Konfiguration der Ziel-OU (Gerätekonfiguration, Anwendungsdefinition, erweiterte Dateieinträge, Dateiübertragung).

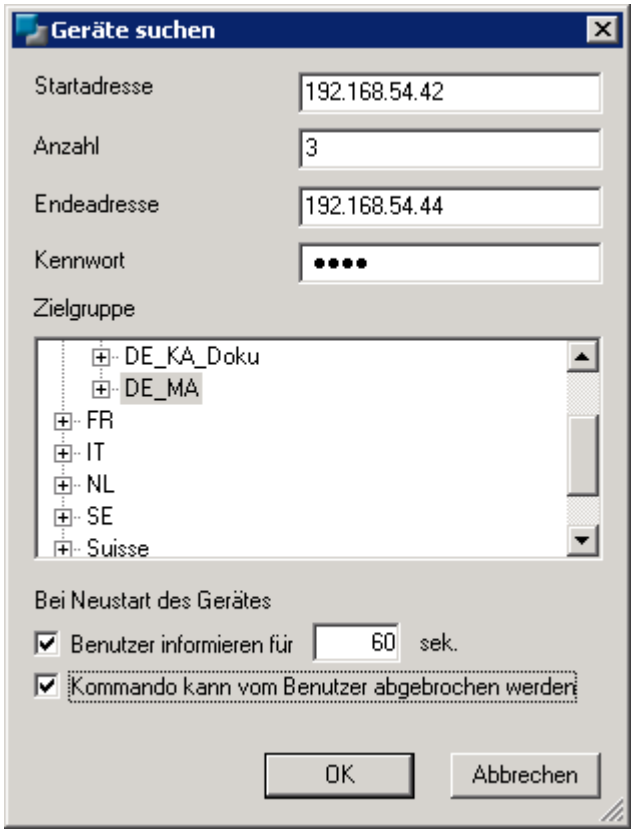
Hinweis
Wenn der OU-Filter aktiv ist, bestimmt dieser die Ziel-OU bzw. Ziel-OUs. Für weitere Informationen siehe Erweiterte Konfiguration/Geräte.

Voraussetzungen:

- Die Geräte sind eingeschaltet und mit dem Netzwerk verbunden.
- Die Geräte haben gültige IP-Adressen.
- Das Gerätekennwort ist bekannt.

Geräte suchen und erfassen

1. Stellen Sie sicher, dass die Ziel-OU korrekt konfiguriert ist.
2. Wählen Sie **Optionen > Geräte suchen**.



3. Bearbeiten Sie folgende Felder:

Startadresse	Erste IP-Adresse im Bereich
Zähler	Anzahl der IP-Adressen im Bereich (maximal 255)
Endadresse	Letzte IP-Adresse im Bereich
Kennwort	Gerätekennwort (Standard: `elux`) Das Gerätekennwort muss mit dem aktuell gültigen Geräte-Kennwort des jeweiligen Clients übereinstimmen.
Zielgruppe	Die OU, der die Geräte zugeordnet werden sollen Default ist die vordefinierte OU `Lost&Found` mit der Basis-konfiguration.
	Achtung Wenn das Feld **Zielgruppe** abgeblendet ist und `Deaktiviert` anzeigt, ist der OU-Filter aktiv und die zutreffenden Geräte werden nach den OU-Filterregeln zugeordnet.
Benutzer informieren	Der Benutzer wird durch eine Meldung über den anstehenden Geräte-Neustart informiert. Geben Sie in Sekunden an, wie lang die Meldung angezeigt werden soll.
Kommando kann vom Benutzer abge-brochen werden	Erlaubt dem Benutzer , den Neustart zu unterdrücken. Die Kon-figuration wird erst mit dem nächsten Neustart aktualisiert.

4. Bestätigen Sie mit **OK**.

Die gefundenen Geräte erhalten die IP-Adresse des verwaltenden Scout Enterprise-Servers. Sie werden der Ziel-OU zugeordnet und neu gestartet. Die Geräte übernehmen die Konfiguration ihrer neuen OU. Eventuelle lokale Konfigurationen werden dabei überschrieben. Ab sofort verbinden sich die Clients bei jedem Systemstart mit dem Scout Enterprise-Server und erhalten dann ggf. aktualisierte Konfigurationen und Anwendungsdefinitionen.

Wenn das Geräteprofil für die jeweiligen Clients bereits reserviert war, wird das vordefinierte Profil beim Discovery automatisch zugewiesen.

Die Reaktionszeit der Geräte und die maximale Suchzeit für die komplette Ausführung der Discovery-Funktion können Sie in **Optionen > Erweiterte Optionen > Geräte > Geräte suchen** anpassen.

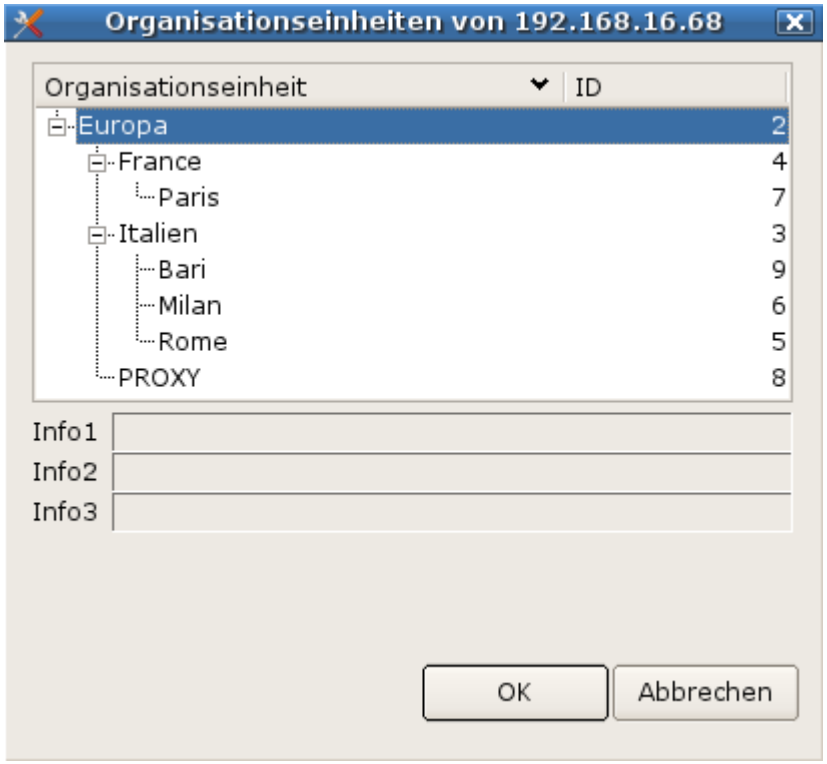
Hinweis
Bereits registrierte Geräte werden von der Discovery-Funktion nicht verändert, aber ihr Status wird durch die Verbindung aktualisiert.

4.4. Reverse Discovery ausführen

Die Reverse-Discovery-Funktion ist das Gegenstück zur Geräteerkennung über **Geräte suchen**: Reverse Discovery wird vom Client aus initiiert, der Client sucht den zuständigen Scout Enterprise-Server und kann einer OU zugeordnet werden.

1. Wählen Sie in der eLux-Systemsteuerung **Setup > Sicherheit**.
2. Geben Sie im Feld **Scout Enterprise** den Namen oder die IP-Adresse des Scout Enterprise-Servers an.
3. Klicken Sie auf die Schaltfläche **...**

   Ein Fenster mit allen OUs des Scout Enterprise-Servers öffnet.



4. Wählen Sie die relevante OU aus.
5. Bestätigen Sie mit **OK** und **Übernehmen**.

Nach dem Neustart wird der Client der entsprechenden OU zugeordnet. Der Hostname des Gerätes wird beim Eintrag in Scout Enterprise als Gerätename verwendet.

Wenn das Geräteprofil für den jeweiligen Client bereits reserviert war, wird das vordefinierte Profil beim Reverse Discovery automatisch zugewiesen.

4.5. Geräteprofil reservieren

Die Zuordnung von Geräten zu einer OU können Sie bereits vor dem ersten Kontakt der Geräte zum Scout Enterprise-Server definieren.

Indem Sie die Geräte vorab manuell in der Scout Enterprise-Konsole anlegen, reservieren Sie das Geräteprofil anhand der MAC-Adresse. Sobald eines der manuell angelegten Geräte bei der Erst-Inbetriebnahme Verbindung zum Scout Enterprise-Server aufnimmt, wird die bereits vorhandene MAC-Adresse erkannt und die Gerätekonfigurationsdaten der entsprechenden OU werden an das Gerät übermittelt.

Die Reservierung von Geräteprofilen kann bei den folgenden Verfahren der Geräteerfassung angewendet werden:

- Discovery
- Reverse Discovery
- DNS-Aliasname `ScoutSrv`
- DHCP-Option `222` für den Scout Enterprise-Server

Hinweis
Wenn ein OU-Filter aktiv ist, wird der OU-Filter höher priorisiert als die Reservierung eines Geräteprofils.

Geräteprofil reservieren

1. Wählen Sie die OU, der das Gerät zugeordnet werden soll, und blenden Sie die Struktur der OU ein.
2. Öffnen Sie das Kontextmenü für **Geräte** unterhalb der OU, und wählen Sie **Hinzufügen...**
3. Geben Sie die 12-stellige MAC-Adresse des Geräts (ohne Bindestriche) ein.

   *Wenn die MAC-Adresse gültig ist, öffnet der Dialog **Konfiguration**. Die Option **Übergeordnete Instanz verwenden** ist automatisch aktiv.*
4. Bestätigen Sie mit **OK**.

Für das Gerät mit der entsprechenden MAC-Adresse wird ein Profil reserviert. Die eigentliche Erfassung erfolgt bei der ersten Verbindung.

Hinweis
Der Geräte-Import resultiert ebenfalls in der Reservierung entsprechender Profile in der OU-Struktur.
Um eine größere Anzahl an Geräten anzulegen, empfehlen wir den Geräte-Import. Für weitere Informationen siehe Import/Export.

4.6. Sichere Geräteverwaltung mit Scout Enterprise

Für die Verbindung neuer Clients zur Scout Enterprise-Konsole können Sie die Sicherheitsstufe erhöhen: Clients, deren MAC-Adresse (Geräteprofil) bereits in der Scout Enterprise-Datenbank hinterlegt ist, werden vom Scout Enterprise-Server akzeptiert und können in die Scout Enterprise-Verwaltung integriert werden. Im Gegensatz dazu werden Clients mit unbekannter MAC-Adresse nicht akzeptiert und nicht in die Scout Enterprise-Verwaltung einbezogen. Diese Clients bekommen somit auch keine Lizenzen aus dem verfügbaren Lizenzpool zugewiesen.

Nur bekannten Clients die Verbindung mit Scout Enterprise erlauben:

1. Wählen Sie in der Scout Enterprise-Konsole **Optionen > Erweiterte Optionen > Geräte > Eintragung neuer Geräte**.
2. Aktivieren Sie die Option **Nur bekannte Geräte akzeptieren**.

Versucht ein unbekanntes Gerät den Scout Enterprise-Server zu kontaktieren, zeigt eine Fehlermeldung am Client an, dass keine Verbindung zum Scout Enterprise-Server möglich ist.

Hinweis
Ausschließlich anfragende Clients, die bereits durch einen Geräteimport oder ein Geräteprofil mit der MAC-Adresse in der Scout Enterprise Datenbank gespeichert sind, werden in die Scout Enterprise-Verwaltung aufgenommen.

4.7. OU-Filter

Der OU-Filter filtert Geräte auf bestimmte Kriterien und ordnet sie den angegebenen Organisationseinheiten zu. Neue Geräte können dadurch automatisch in die passende OU eingehängt werden. Die automatische Zuordnung erfolgt auch, wenn Geräte physikalisch umgezogen werden und sich dadurch die Filterkriterien ändern.

Den OU-Filter können Sie auf zwei Arten konfigurieren:

- Der Subnetz-Filter verwendet die Client-Netzwerkadresse als Filterkriterium.
- Der benutzerdefinierte Filter verwendet konfigurierte Asset-Informationen der Geräte als Filterkriterien

Sie können immer nur einen Filter aktivieren. Die gleichzeitige Verwendung beider Filter ist nicht möglich. In jedem Filter können Sie mehrere Filterregeln definieren und die Reihenfolge ihrer Abarbeitung festlegen.

Einmal definierte Filterregeln bleiben erhalten, bis sie explizit gelöscht werden. Deaktivieren Sie aktuell nicht benötigte Filterregeln, um sie zur späteren Verwendung aufzuheben.

Der OU-Filter hat eine höhere Priorität als

- die OU-Zuordnung von Geräten über die DHCP-Option 223
- die Gerätesuche (Discovery) via Scout Enterprise-Konsole
- die OU-Auswahl im First Configuration Wizard lokal am Client
- die in **Erweiterte Optionen > Geräte** festgelegte Standard-OU.

Für einzelne Geräte kann der OU-Filter ignoriert werden (**Erweiterte Einstellungen > Management**).

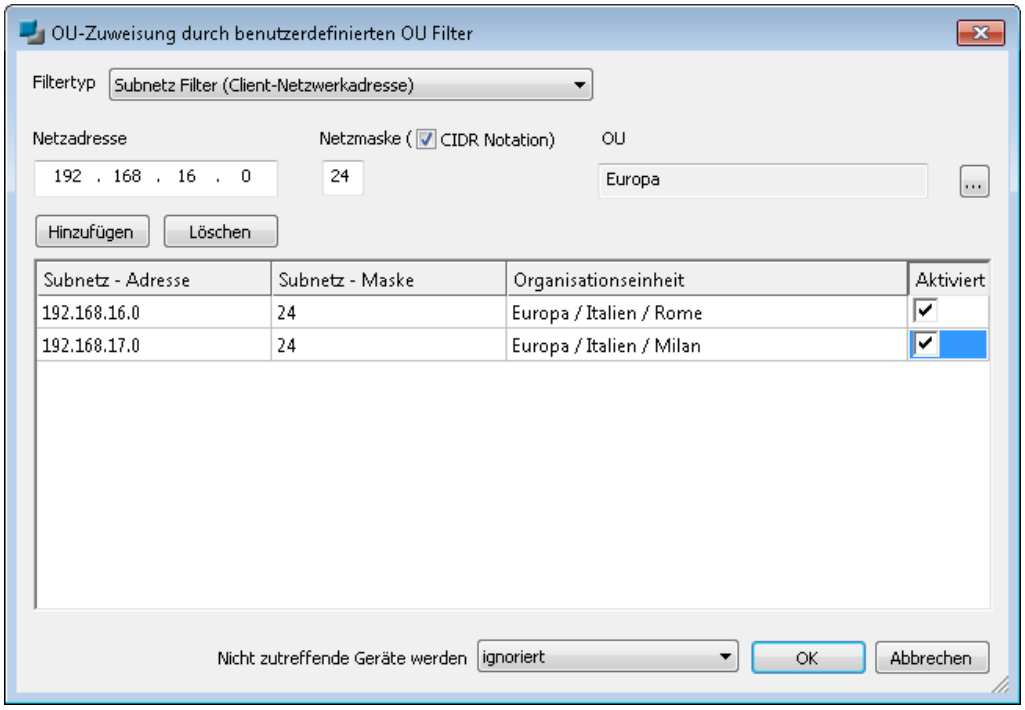
OU-Filter werden beim Export der Datenkategorie **Erweiterte Optionen** berücksichtigt. Für weitere Informationen siehe Import/Export.

4.7.1. OU-Filter als Subnetz-Filter einrichten

Sie können mit dem OU-Filter auf Client-Netzwerkadressen filtern, um zutreffende Geräte einer bestimmten OU zuzuordnen.

1. Wählen Sie **Optionen > Erweiterte Optionen... > Geräte**.
2. Aktivieren Sie unter **Eintragen neuer Geräte** die Option **OU von Geräten durch den OU-Filter festlegen**.
3. Wenn erforderlich, klicken Sie auf die Schaltfläche **...**, um den Dialog **OU-Filter** zu öffnen.
4. Wählen Sie in der **Filtertyp**-Liste den Eintrag `Subnetz-Filter (Client-Netz-werkadresse)`.
5. Geben Sie im Feld **Netzadresse** den relevanten IP-Bereich ein.
   Beispiel: `192.168.16.0` deckt alle IP-Adressen ab, die mit `192.168.16` beginnen.
6. Geben Sie im Feld **Netzmaske** das Netzpräfix an, um den Geräteteil zu bestimmen.
7. Wählen Sie über die Schaltfläche **...** die OU aus, der die Geräte zugeordnet werden sollen.
8. Klicken Sie auf **Hinzufügen**, um die neue Filterregel der Liste hinzuzufügen.

   Die Filterregel wird im unteren Feld angezeigt.



9. Wenn gewünscht, fügen Sie weitere Filterregeln hinzu und nehmen weitere Einstellungen vor. Für weitere Informationen siehe OU-Filterregeln bearbeiten.
10. Definieren Sie bei **Nicht zutreffende Geräte werden**, was mit Geräten passieren soll, die nicht dem Subnetz-Filter entsprechen.

Achtung

Wenn Sie die Option `der Standard OU zuweisen` wählen, werden alle nicht zutreffenden Geräte in die Standard OU verschoben. Dies betrifft auch Geräte, die bereits anderen OUs zugeordnet sind.

11. Überprüfen Sie alle aktiven Filterregeln sorgfältig, um unbeabsichtigte Zuordnungen zu vermeiden.
12. Bestätigen Sie mit **OK**.

Alle aktiven Filterregeln werden abgearbeitet. Die zutreffenden Geräte werden beim nächsten Neustart mithilfe des Subnetz-Filters der angegebenen OU zugeordnet. Falls parallel benutzerdefinierte Filterregeln vorhanden sind, haben diese keine Relevanz.

4.7.2. OU-Filter als benutzerdefinierten Filter einrichten

Sie können mit dem OU-Filter nach konfigurierten Asset-Informationen filtern, um zutreffende Geräte bestimmten OUs zuzuordnen.

Geräte mit eLux RP ab Version 4.6.0 senden ein Feld **OU-Filtertext** zum Scout Enterprise-Server, das bestimmte Geräte-Informationen enthält. Die Informationen des **OU-Filtertext**-Feldes können Sie im Report-Generator und für den benutzerdefinierten OU-Filter verwenden. Es enthält folgende Werte:

Host-Name, OS-Name, OS-Version, Seriennummer, Hersteller, Typ, BIOS-Version, CPU-Geschwindigkeit, Modell, Kernel-Version, Flash-Typ, Flash-Größe, RAM-Größe, Grafik.

1. Wählen Sie **Optionen > Erweiterte Optionen... > Geräte**.
2. Aktivieren Sie unter **Eintragen neuer Geräte** die Option **OU von Geräten durch den OU-Filter festlegen**.
3. Wenn erforderlich, klicken Sie auf die Schaltfläche **...**, um den Dialog **OU-Filter** zu öffnen.
4. Wählen Sie in der **Filtertyp**-Liste den Eintrag `Benutzerdefinierter Filter (konfigurierte Assetinformation)`.
5. Geben Sie im Feld **Filterregel** ein oder mehrere Filterkriterien an. Ein Filterkriterium besteht aus drei Teilen:
   - einer Geräte-Information aus dem **OU-Filtertext** als Zeichenfolge wie vorgegeben
   - dem Vergleichsoperator =
   - dem Wert, auf den Sie filtern möchten.

   Beispiel: `ELUX_OSNAME=eLux RP`

   Mehrere Filterkriterien können durch die Operatoren AND und OR verknüpft werden. Die Operatoren müssen in Großbuchstaben eingegeben werden.

   Wildcards sind nicht erlaubt, aber es werden alle Treffer gefunden, die mit der angegebenen Zeichenfolge beginnen.

   Beispiel für die Werte eines **OU-Filtertext**-Feldes:

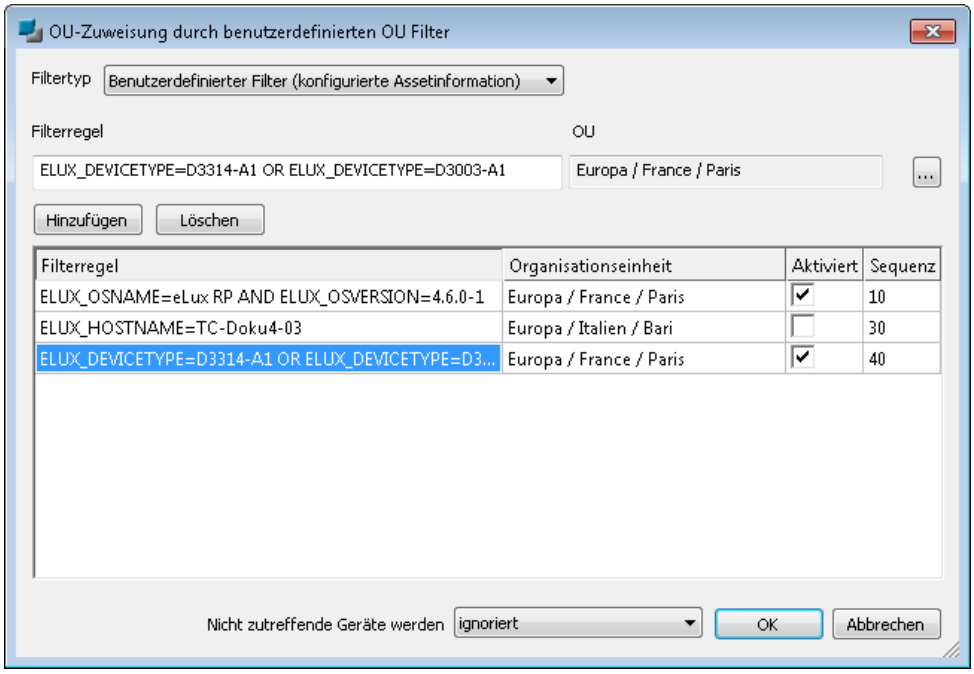
```
ELUX_HOSTNAME=Inga;ELUX_OSNAME=eLux RP5;ELUX_OSVERSION=5.3.0; ELUX_
SERIAL=44015379;ELUX_SUPPLIER=FUJITSU;ELUX_DEVICETYPE=D3314-A1; ELUX_
BIOS=V4.6.5.4 R1.4.0 for D3314-A1x;ELUX_CPU=998;ELUX_PRODUCT=D3314-
A1; ELUX_KERNEL=3.4.71;ELUX_FLASH=4GB NANDrive;ELUX_FLASHSIZE=3849;
ELUX_MEMORY=2048;ELUX_GRAPHICS=ATI AMD Radeon HD8210E
```

Beispiele für Filterregeln:

Beispiel 1: `ELUX_OSNAME=eLux RP5 AND ELUX_OSVERSION=5.2`
Beispiel 2: `ELUX_DEVICETYPE=D3314-A1 OR ELUX_DEVICETYPE=D3003-A1`

6. Wählen Sie im Feld rechts neben **Filterregel** die OU aus, der die Geräte zugeordnet werden sollen.
7. Klicken Sie auf **Hinzufügen**, um die neue Filterregel der Liste hinzuzufügen.

   Die Filterregel wird im unteren Feld angezeigt.



8. Wenn gewünscht, fügen Sie weitere Filterregeln hinzu und nehmen weitere Einstellungen vor. Für weitere Informationen siehe OU-Filterregeln bearbeiten.
9. Definieren Sie bei **Nicht zutreffende Geräte werden**, was mit Geräten passieren soll, die nicht dem benutzerdefinierten Filter entsprechen.

Achtung

Wenn Sie die Option `der Standard OU zuweisen` wählen, werden alle nicht zutreffenden Geräte in die Standard OU verschoben. Dies betrifft auch Geräte, die bereits anderen OUs zugeordnet sind.

10. Überprüfen Sie die aktiven Filterregeln sorgfältig, um unbeabsichtigte Zuordnungen zu vermeiden.
11. Bestätigen Sie mit **OK**.

Alle aktiven Filterregeln werden in der angegebenen Reihenfolge abgearbeitet. Die zutreffenden Geräte werden beim nächsten Neustart mithilfe des benutzerdefinierten Filters der angegebenen OU zugeordnet. Falls parallel Subnetz-Filterregeln vorhanden sind, haben diese keine Relevanz.

4.7.3. OU-Filterregeln bearbeiten

Einmal definierte Filterregeln im OU-Filter bleiben erhalten, bis sie explizit gelöscht werden. Die Filterregeln können in verschiedener Hinsicht bearbeitet werden.

1. Wählen Sie **Optionen > Erweiterte Optionen... > Geräte**.
2. Klicken Sie unter **Eintragen neuer Geräte** neben **OU von Geräten durch den OU-Filter festlegen** auf die Schaltfläche **...**.
3. Wählen Sie in der **Filtertyp**-Liste den relevanten Eintrag.
4. Nutzen Sie folgende Möglichkeiten zur Bearbeitung:

Option	Aktion	Beschreibung
Hinzufügen	Schaltfläche anklicken	**Benutzerdefinierter Filter**: Die Filterkriterien aus dem Feld **Filterregel** und die im Feld **OU** ausgewählte Ziel-OU werden als neue Filterregel in die Liste übernommen. Syntax für Filterkriterium: `<Zeichenfolge aus **OU Filtertext**>=<Wert>` Mehrere Filterkriterien können durch AND oder OR verknüpft werden. Die Operatoren müssen in Großbuchstaben eingegeben werden. Für Beispiele siehe OU-Filter als benutzerdefinierten Filter einrichten. **Subnetz-Filter**: Die Daten aus den Feldern **Netzadresse** und **Netzmaske** sowie die im Feld **OU** ausgewählte Ziel-OU werden als neue Filterregel in die Liste übernommen.
Löschen	Schaltfläche anklicken	Die markierte Filterregel wird gelöscht.
Filterregel bearbeiten	Filterregel markieren und F2-Taste drücken oder doppelklicken	Die Filterregel kann direkt in der Liste modifiziert werden.
Aktivieren / Deaktivieren	Option **Aktiviert** anklicken	Deaktivierte Filterregeln werden nicht ausgeführt. Neu hinzugefügte Filterregeln sind standardmäßig aktiv.

Option	Aktion	Beschreibung
Reihenfolge der Abarbeitung ändern (benutzerdefinierter Filter)	Sequenz-Nummer bearbeiten	Filterregeln mit niedriger Sequenz-Nummer werden vor Filterregeln mit hoher Sequenz-Nummer ausgeführt.

5. Definieren Sie bei **Nicht zutreffende Geräte werden**, was mit Geräten passieren soll, die nicht dem benutzerdefinierten Filter entsprechen.

Achtung

Wenn Sie die Option `der Standard OU zuweisen` wählen, werden alle nicht zutreffenden Geräte in die Standard OU verschoben. Dies betrifft auch Geräte, die bereits anderen OUs zugeordnet sind.

6. Überprüfen Sie alle aktiven Filterregeln sorgfältig, um unbeabsichtigte Zuordnungen zu vermeiden.
7. Bestätigen Sie mit **OK**.

Alle aktiven Filterregeln werden in der angegebenen Reihenfolge abgearbeitet. Die zutreffenden Geräte werden beim nächsten Neustart der angegebenen OU zugeordnet.

4.7.4. OU-Filter für einzelne Geräte deaktivieren

Wenn der OU-Filter aktiv ist, werden aktive Filterregeln ausgeführt und zutreffende Geräte beim nächsten Neustart in die angegebenen OUs verschoben. Wenn der Filter auf ein einzelnes Gerät nicht angewendet werden soll, können Sie den OU-Filter für das Gerät deaktivieren.

1. Öffnen Sie für das relevante Gerät **Erweiterte Konfiguration... > Management**.
2. Aktivieren Sie unter **Eintragung neuer Geräte** die Option **OU-Filter ignorieren**.
3. Bestätigen Sie mit **OK**.

Oder:

1. Ziehen Sie das Gerät per Drag&Drop in eine andere OU.
2. Bestätigen Sie den Vorgang mit **OK**.

Das Gerät ist der neuen OU zugeordnet und der OU-Filter ist für dieses Gerät deaktiviert.

4.8. Dynamische Gerätegruppen

Dynamische Gerätegruppen ermöglichen das OU-übergreifende Absetzen von Kommandos an eine frei definierbare Gerätegruppe. Beispielsweise können Sie organisationsweit allen Geräten mit einem bestimmten Image eine Nachricht senden. Oder Sie können alle Geräte mit einer bestimmten BIOS-Version OU-unabhängig mit einem BIOS-Update versorgen. Auch ein Geräteumzug zu einem anderen Scout Enterprise-Server kann auf eine Dynamische Gerätegruppe angewendet werden.

Grundlage für eine Dynamische Gerätegruppe ist ein im Scout Enterprise-Reportgenerator erstellter Report, der auf die relevanten Geräte filtert. Dieser Report wird einmalig in die Scout Enterprise-Konsole exportiert und wird dort anschließend als **Dynamische Gerätegruppe** angezeigt. Alle Kommandos, die auf OUs oder auf einzelne Geräte angewendet werden können, können auch auf eine Dynamische Gerätegruppe angewendet werden.

Die dynamischen Gerätegruppen werden in der Scout Enterprise-Konsole in einem eigenen Fenster angezeigt und bleiben zur Wiederverwendung erhalten, bis Sie sie löschen. Die Gerätegruppen bringen Sie mit einem Klick auf den aktuellen Stand.

Bei der Erstellung der dynamischen Gerätegruppen werden die Berechtigungen gemäß der Administratorenverwaltung berücksichtigt.

4.8.1. Voraussetzungen für Dynamische Gerätegruppen

- Scout Enterprise Version 13.4.2 oder höher
- Scout Enterprise-Reportgenerator ab Scout Enterprise Management Suite Version 13.4.2
- Die MAC-Adresse muss Bestandteil des zugrundeliegenden Report-Layouts sein. Der zugrundeliegende Report muss eine Liste von Geräten oder eine Liste von Inventareinträgen erzeugen.

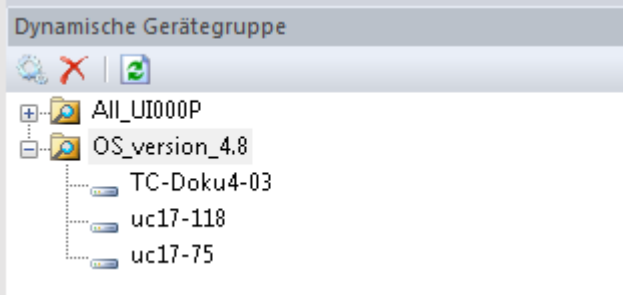
Für weitere Informationen zur Definition von dynamischen Gerätegruppen siehe Dynamische Gerätegruppen erstellen im Scout Enterprise-Reportgenerator-Handbuch.

4.8.2. Dynamische Gerätegruppen verwenden

Eine Dynamische Gerätegruppe basiert normalerweise auf einem in Scout Enterprise-Reportgenerator erstellten Report, der als Dynamische Gerätegruppe in die Scout Enterprise-Konsole exportiert wird. Für weitere Informationen zum Erstellen und Exportieren siehe Dynamische Gerätegruppen erstellen im Scout Enterprise-Reportgenerator-Handbuch.

Dynamische Gerätegruppe anzeigen

- Wählen Sie in der Scout Enterprise-Konsole **Ansicht > Fenster > Dynamische Gerätegruppen...**.



*Das Fenster **Dynamische Gerätegruppe** wird angezeigt. Die Dynamischen Gerätegruppen können erweitert werden, um die gefilterten Geräte einzublenden.*

Hinweis

Die Dynamische Gerätegruppe zeigt immer diejenigen Geräte an, die zum Zeitpunkt der letzten Reporterstellung den Kriterien entsprachen.

Für eine markierte Dynamische Gerätegruppe zeigt das **Eigenschaften**-Fenster **Erstelldatum**, **Geräteanzahl** und zugrundeliegenden **Filter** an. Das Erstelldatum bezieht sich auf das letzte Erzeugen des zugrundeliegenden Reports und zeigt an, ob die Dynamische Gerätegruppe aktuell ist.

Wenn beispielsweise neue Geräte in die Datenbank integriert wurden, die die im Report definierten Kriterien erfüllen, ist die Dynamische Gerätegruppe nicht mehr aktuell. Sie können die Gerätegruppe aktualisieren, indem Sie den Report aus der Scout Enterprise-Konsole heraus neu erzeugen.

Wenn Sie eine Dynamische Gerätegruppe nicht mehr benötigen, können Sie sie mit der Schaltfläche ✕ löschen. Der zugrundeliegende Report bleibt unabhängig davon bestehen.

Dynamische Gerätegruppe aktualisieren

1. Markieren Sie im Fenster **Dynamische Gerätegruppe** die relevante Gerätegruppe.
2. Klicken Sie in der Symbolleiste des Fensters **Dynamische Gerätegruppe** auf die Schaltfläche **Neu erzeugen**.

*Der zugrundeliegende Report wird neu erzeugt und exportiert. Die gefilterten Geräte werden entsprechend dem aktuellen Datenbankstand unter der Gerätegruppe im Fenster **Dynamische Gerätegruppe** angezeigt. Im **Eigenschaften**-Fenster wird unter **Erstelldatum** der aktuelle Zeitpunkt angezeigt.*

Hinweis

Die Schaltfläche **Aktualisieren** bezieht sich nur auf die Aktualisierung der Ansicht. Der Report bleibt davon unberührt.

Kommando oder Vormerkung auf Dynamische Gerätegruppe anwenden

1. Markieren Sie im Fenster **Dynamische Gerätegruppe** die relevante Dynamische Gerätegruppe und überprüfen Sie die im **Eigenschaften**-Fenster angezeigten Informationen.

2. Aktualisieren Sie die Dynamische Gerätegruppe mit der Schaltfläche , um sicherzustellen, dass genau die aktuell zutreffenden Geräte betroffen sind.
3. Öffnen Sie das Kontextmenü der Dynamischen Gerätegruppe und wählen Sie ein Kommando oder eine Vormerkung.

Kommandos und Vormerkungen werden OU-unabhängig auf die gefilterten Geräte angewendet. Alle verfügbaren Kommandos können auch über die Zeitplanung für eine spätere Ausführung vorgemerkt werden.

4.8.3. Sonderform Dynamische Gerätegruppen über Import

– ab Scout Enterprise Management Suite Version 14.9 –

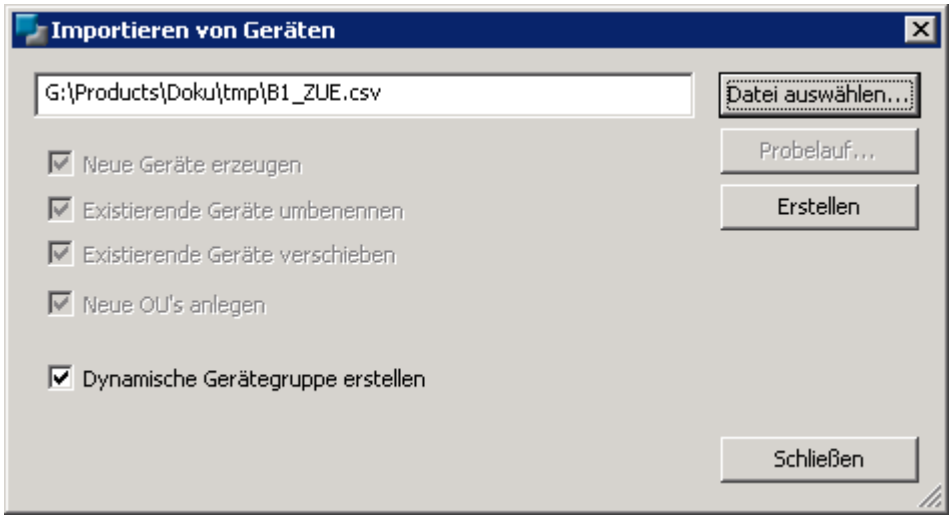
Alternativ zum Scout Enterprise-Reportgenerator kann zum Erstellen einer Dynamischen Gerätegruppe eine Geräteliste mit MAC-Adressen als Basis dienen. Der Vorteil besteht darin, dass Sie beliebige Geräte zusammenstellen können. Anstelle des Report-Generators wird die Import-Funktion der Scout Enterprise-Konsole als Werkzeug eingesetzt, um die relevanten Geräte zu einer Gerätegruppe zusammenzufassen. Beachten Sie, dass die Geräte bereits in Scout Enterprise registriert sein müssen, ein Import findet nicht statt.

Dynamische Gerätegruppe über Geräte-Import erstellen

Voraussetzung

Die relevanten Geräte müssen mit ihrer MAC-Adresse in einer `.csv`-Datei gelistet sein. Jede Zeile muss mit einer MAC-Adresse beginnen. Es dürfen weitere Informationen folgen, diese werden jedoch nicht ausgewertet.

1. Wählen Sie in der Scout Enterprise-Konsole **Datei > Import > Geräte...**.



2. Aktivieren Sie im Dialog **Importieren von Geräten** unten die Option **Dynamische Gerätegruppe erstellen**.

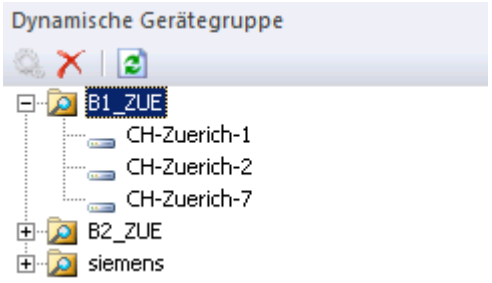
   Die Optionen für den Geräte-Import werden abgeblendet.

3. Klicken Sie auf **Datei auswählen...** und wählen Sie die relevante `.csv`-Datei aus dem Dateisystem.
4. Klicken Sie auf **Erstellen**.

Die `.csv`-Datei wird ausgewertet. Scout Enterprise erstellt eine neue Dynamische Gerätegruppe, die alle Geräte der `csv`-Liste enthält, deren MAC-Adresse in Scout Enterprise registriert ist. Die Dynamische Gerätegruppe übernimmt den Namen der `csv`-Datei.

Dynamische Gerätegruppe anzeigen

- Wählen Sie in der Scout Enterprise-Konsole **Ansicht > Fenster > Dynamische Gerätegruppen...**.



*Das Fenster **Dynamische Gerätegruppe** wird angezeigt. Die Dynamischen Gerätegruppen können erweitert werden, um die gefilterten Geräte einzublenden.*

Hinweis

Dynamische Gerätegruppen, die durch einen Geräte-Import erstellt wurden, können nicht mit der Schaltfläche  **Neu erzeugen** aktualisiert werden. Um die Gerätegruppe zu aktualisieren, müssen Sie den Geräte-Import mit der aktualisierten `csv`-Datei unter gleichem Namen erneut durchführen, siehe Anleitung oben.

Für eine markierte Dynamische Gerätegruppe zeigt das **Eigenschaften**-Fenster Informationen wie Erstelldatum und Geräteanzahl. Im Feld **Filter** wird der Eintrag `durch Geräte-Import erstellt` angezeigt.

Kommando oder Vormerkung auf Dynamische Gerätegruppe anwenden

1. Markieren Sie im Fenster **Dynamische Gerätegruppe** die relevante Dynamische Gerätegruppe und überprüfen Sie die im **Eigenschaften**-Fenster angezeigten Informationen.
2. Öffnen Sie das Kontextmenü und wählen Sie ein Kommando oder eine Vormerkung.

Kommandos und Vormerkungen werden OU-unabhängig auf alle Geräte der Dynamischen Gerätegruppe angewendet. Alle verfügbaren Kommandos können auch über die Zeitplanung für eine spätere Ausführung vorgemerkt werden.

4.9. Umzug von Geräten zu einem anderen Scout Enterprise-Server

Der Umzug von Geräten zu einem anderen Scout Enterprise-Server unterstützt verschiedene Szenarien der Geräte-Migration zwischen zwei Scout Enterprise-Servern. Dabei kann es sich beispielsweise um die Verlagerung der Geräte eines Test-/Abnahme-Servers auf einen Produktions-Server oder um die Konsolidierung mehrerer Scout Enterprise-Server zu einem einzigen Server handeln (Server-Fusion).

Der Umzug kann ab Version 14.6 auch ohne die Prüfung auf Verfügbarkeit des Ziel-Servers durch den Client erfolgen. Dieser sogenannte "Offline"-Umzug ermöglicht den Umzug auch dann, wenn der Ziel-Server zum Zeitpunkt des Umzugs vom Client netzwerktechnisch nicht erreicht werden kann. (Beispiel: Ein externer Dienstleister bereitet in seiner Umgebung Geräte für den produktiven Einsatz in der Kundenumgebung vor).

Client-Lizenzen und Subscription können wahlweise mitgenommen oder beim Quell-Server belassen werden.

Voraussetzungen:

- Scout Enterprise Version 14.5.0 oder höher
- eLux RP Version 4.10.0 oder höher

4.9.1. Umzugsverfahren

Das Umzugsverfahren wird vom Quell-Server (Geräte-abgebender Server) initiiert und vom Ziel-Server (Geräte-aufnehmender Server) abgeschlossen. Der eigentliche Umzugsprozess mit den erforderlichen Prüfungen der Rahmenbedingungen, dem Transfer der Client-Lizenzen und der anteiligen Subscription-Gültigkeit erfolgt durch den Client.

Der Administrator initiiert den Umzug durch die Vormerkung **Geräteumzug veranlassen** für die betroffenen Geräte in der Scout Enterprise-Konsole des Quell-Servers. Die Vormerkung enthält alle notwendigen Angaben. Mit dem nächsten Client-Neustart und dem damit verbundenen Konfigurationsabgleich am Quell-Server werten die Geräte diese Umzugsvormerkung aus.

Die dabei übermittelte Adresse des Ziel-Servers wird von den Clients auf Erreichbarkeit über das Netzwerk geprüft. Des weiteren prüfen die Geräte die Gültigkeit der Scout Enterprise-Version des Ziel-Servers (V14.5.0 oder höher). Wenn beide Prüfungen erfolgreich sind, erfolgt die Löschung der Geräte am Quell-Server.

Im Standardfall haben die Clients die vom Quell-Server erhaltene Information über Client-Lizenzen und Subscription-Gültigkeit an den Ziel-Server übermittelt, so dass diese Lizenz- und Subscription-Information am Quell-Server gelöscht und der Lizenz- und Subscriptionbestand des Ziel-Servers aktualisiert wird. Wenn Sie jedoch Lizenz- und Subscription-Information am Quell-Server belassen und nach dem Umzug für andere Geräte verfügbar machen möchten, konfigurieren Sie dies in der Vormerkung.

Die neuen Geräte werden am Ziel-Server der angegebenen Ziel-OU zugeordnet. Wenn keine Ziel-OU angegeben wurde, wird die Standard-OU oder die den OU-Filterregeln entsprechende OU verwendet (konfiguriert in **Optionen > Erweiterte Optionen > Geräte > Eintragung neuer Geräte**).

Abschließend erfolgt ein automatischer Neustart der Geräte zur Übernahme und Aktivierung der Konfigurationseinstelllungen des Ziel-Servers. Bei der Nutzung eines OU-Filters wird automatisch ein zusätzlicher Neustart der Geräte durchgeführt, um den Umzug abzuschließen.

Achtung

Die Geräteprofilreservierung durch einen Vorab-Eintrag der MAC-Adressen der neuen Geräte am Ziel-Server darf für den Geräteumzug NICHT genutzt werden. Falls Geräte VOR dem Umzug bereits am Ziel-Server vorhanden sind, erfolgt KEINE Korrektur des Lizenz- und Subscriptionbestandes.

4.9.2. Umzugsverfahren offline

– ab Scout Enterprise Management Suite Version 14.6 –

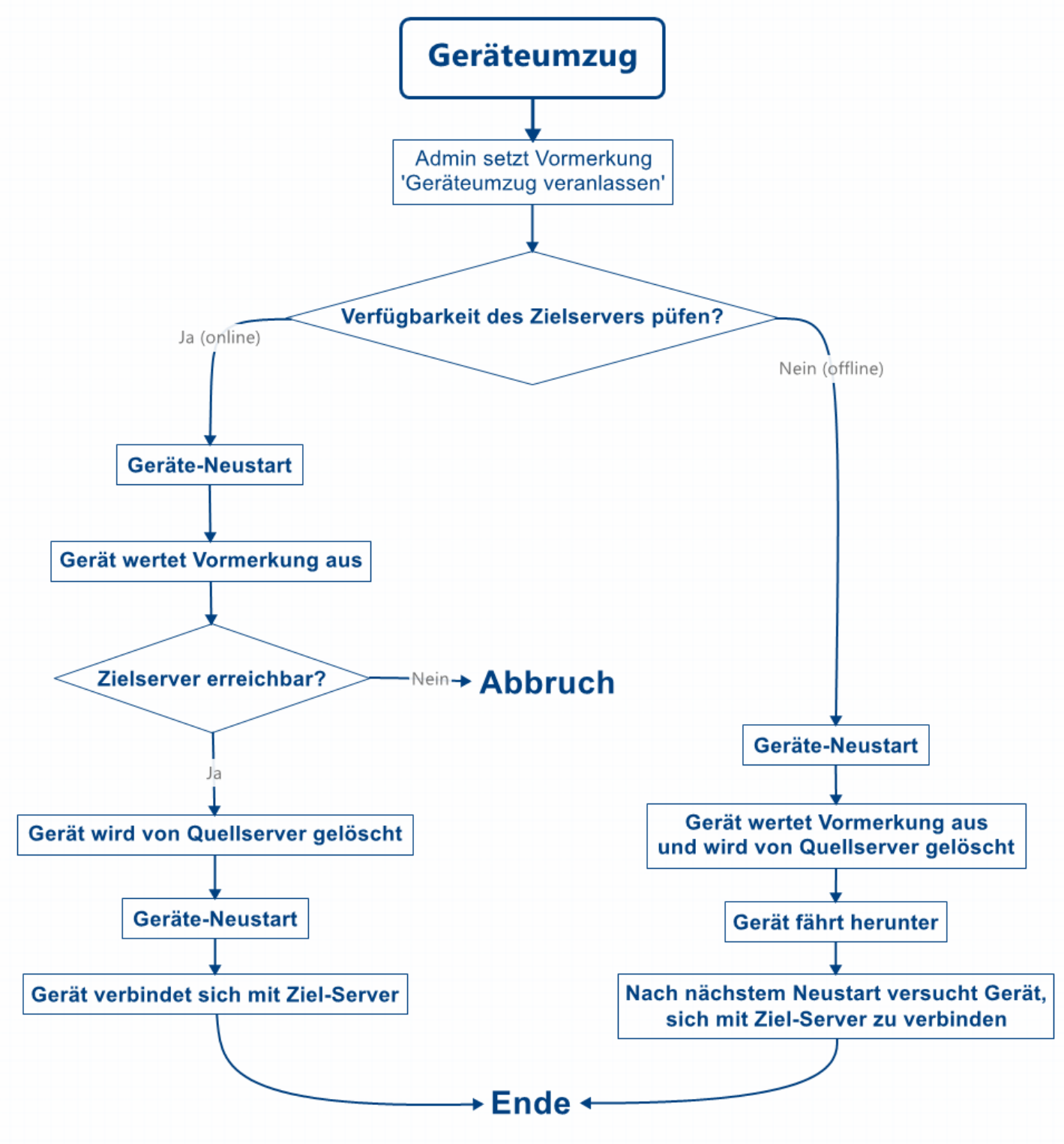
Das Umzugsverfahren wird vom Quell-Server (Geräte-abgebender Server) initiiert und von den betroffenen Geräten durchgeführt. Beim Offline-Verfahren entfällt die Prüfung des Geräte-aufnehmenden Ziel-Servers auf Verfügbarkeit und Durchführbarkeit.

Wie beim Online-Umzug initiiert der Administrator den Umzug durch die Vormerkung **Geräteumzug veranlassen** für die betroffenen Geräte in der Scout Enterprise-Konsole des Quell-Servers. Die Vormerkung enthält alle notwendigen Angaben. Mit dem nächsten Client-Neustart und dem damit verbundenen Konfigurationsabgleich am Quell-Server werten die Geräte diese Umzugsvormerkung aus.

Die betroffenen Geräte fahren herunter und werden am Quell-Server ohne weitere Prüfungen gelöscht. Beim nächsten Neustart versuchen die Geräte, eine Verbindung zum Zielserver herzustellen.

Client-Lizenzen und Subscription können wahlweise mitgenommen oder beim Quell-Server belassen werden. Die Vorgehensweise entspricht derjenigen im Online-Verfahren.

4.9.3. Ablauf des Geräteumzugs

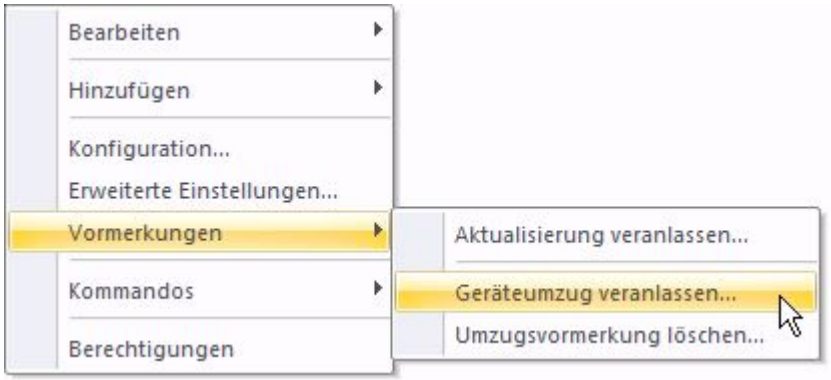


4.9.4. Geräteumzug veranlassen

Voraussetzung

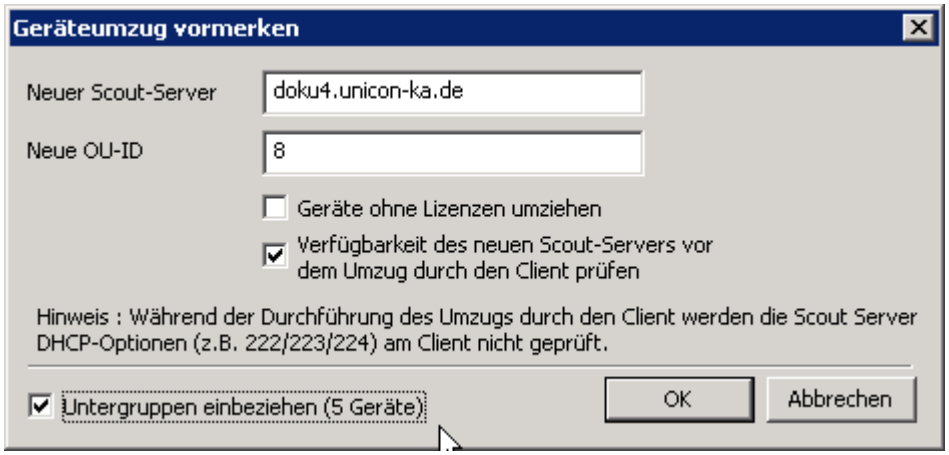
- Deaktivieren Sie auf dem Zielserver die Option **Erweiterte Konfiguration > Geräte > Nur bekannte Geräte akzeptieren**, falls aktiv.
- Um den Umzug zu einem anderen Scout Enterprise-Server bei Verwendung der Scout Enterprise Server DHCP-Optionen (222/223/224) zu gewährleisten, werden die DHCP-Optionen am Client während des Umzugs nicht geprüft. Wenn DHCP-Optionen für den Quell-Server konfiguriert wurden, müssen Sie am Ziel-Server in der Gerätekonfiguration **Netzwerk > LAN > Bearbeiten > Erweitert** die Option **DHCP Optionen ignorieren** aktivieren.

1. Markieren Sie ein Gerät, eine OU, eine Dynamische Gerätegruppe oder Geräte im Fenster **Alle Geräte**.
2. Wählen Sie im Kontextmenü die Option **Vormerkungen > Geräteumzug veranlassen...**.



*Der Dialog **Geräteumzug vormerken** öffnet.*

3. Geben Sie im Feld **Neuer Scout Enterprise-Server** den Namen (FQDN) oder die IP-Adresse des Ziel-Servers ein.
4. Geben Sie im Feld **Neue OU-ID** die ID der Ziel-OU am Ziel-Server ein.



Wenn Sie keine Angabe machen, werden die Geräte der Standard-OU oder der den OU-Filterregeln entsprechenden OU zugeordnet.

5. Wenn Sie die Lizenzen der umziehenden Geräte am Quell-Server belassen möchten, aktivieren Sie die Option **Geräte ohne Lizenzen umziehen**.

   Wenn Sie diese Option aktivieren, werden die auf den Geräten gespeicherten Client-Lizenzen gelöscht und anderen Geräten am Quell-Server verfügbar gemacht. Die Subscription-Gültigkeit für diese Geräte bleibt ebenfalls am Quell-Server.

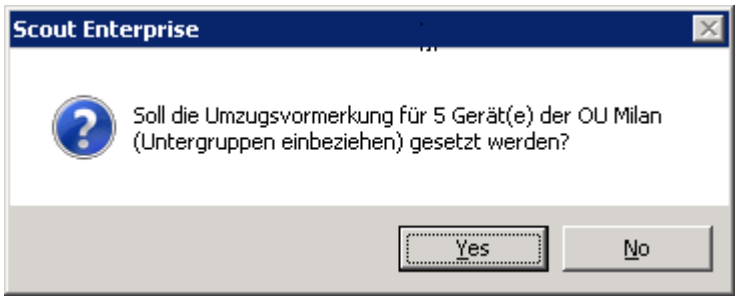
   Wenn Sie diese Option nicht aktivieren, werden sowohl die Client-Lizenzen als auch die anteilige Subscription-Gültigkeit mit umgezogen zum Ziel-Server.

6. Um vor dem Umzug die Verfügbarkeit des Zielservers prüfen zu lassen ("Online"-Umzug), stellen Sie sicher, dass die Option `Verfügbarkeit des neuen Scout-Servers vor dem Umzug prüfen` aktiv ist.

7. Wenn Sie Geräte in eventuell vorhandenen untergeordneten OUs berücksichtigen möchten, aktivieren Sie die Option **Untergruppen einbeziehen**.

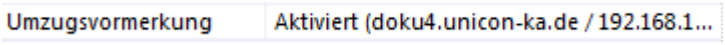
   Die jeweilige Anzahl der betroffenen Geräte wird im Dialog dynamisch aktualisiert.

8. Bestätigen Sie die Vormerkung und die abschließende Sicherheitsabfrage.



Wenn Sie den Umzug "online" durchführen, wird die Auflösbarkeit des Servernamens in eine IP-Adresse bzw. die Gültigkeit der eingegebenen IP-Adresse geprüft.

*Die Vormerkungen für den Geräteumzug werden gesetzt. Für jedes Gerät wird der aktuelle Status der **Umzugsvormerkung** im **Eigenschaften**-Fenster angezeigt.*



*Wenn für ein Gerät keine Umzugsvormerkung vorhanden ist, bleibt das Feld **Umzugsvormerkung** leer.*

Hinweis

Wenn das Feld **Umzugsvormerkung** im **Eigenschaften**-Fenster nicht angezeigt wird, klicken Sie auf die Schaltfläche , um die anzuzeigenden Felder zu konfigurieren.

Im Scout Enterprise-Reportgenerator können Sie alle Geräte mit aktivierter Umzugsvormerkung auswerten:

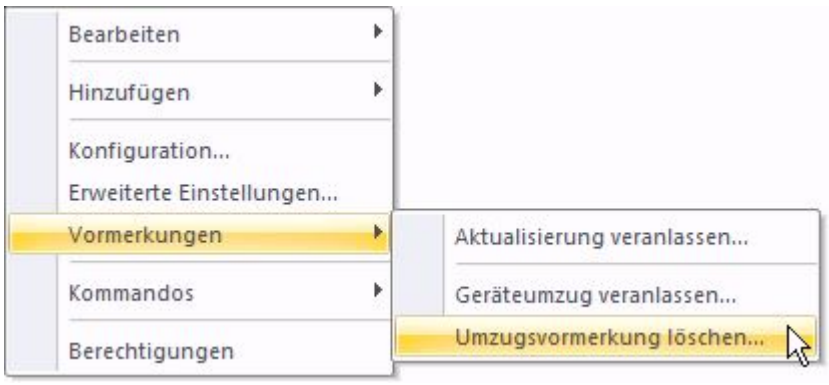
9. Wenn Sie die Durchführung des Geräteumzuges steuern möchten, exportieren Sie die im Report-Generator ermittelten Geräte in eine Dynamische Gerätegruppe und wenden das Kommando **Neustart der Geräte...** an.

   Die relevanten Geräte werden zu dem von Ihnen festgelegten Zeitpunkt umgezogen und bekommen ihre Konfiguration vom Ziel-Server.
   Auf diese Weise können Sie sicherstellen, dass der Geräteumzug außerhalb der Arbeitszeit stattfindet und dass alle betroffenen Geräte gleichzeitig umgezogen werden (Online-Umzug)).

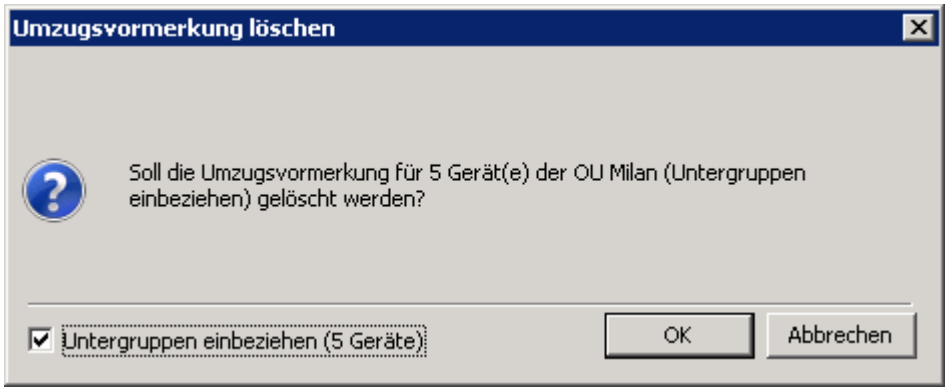
   Wenn Sie den Umzug "offline" durchführen, verbinden sich die relevanten Geräte erst dann zu ihrem neuen Server, wenn eine Verbindung möglich ist.

4.9.5. Umzugsvormerkung löschen

1. Öffnen Sie für die relevante OU, Gerät oder Dynamische Gerätegruppe das Kontextmenü und wählen Sie **Vormerkungen > Umzugsvormerkung löschen**.



2. Wenn Sie Geräte in eventuell vorhandenen untergeordneten OUs berücksichtigen möchten, aktivieren Sie im Dialog **Umzugsvormerkung löschen** die Option **Untergruppen einbeziehen**.



   Die jeweilige Anzahl der betroffenen Geräte wird im Dialog dynamisch aktualisiert.

3. Bestätigen Sie mit **OK**.

*Sobald das **Eigenschaften**-Fenster aktualisiert wurde, ist der Status **Umzugsvormerkung** für das relevante Gerät nicht mehr vorhanden.*

5. Geräte-Konfiguration

5.1. Konzept

Für die effiziente Verwaltung zahlreicher Thin Clients ist die Gerätekonfiguration eine zentrale Funktion. Die Anzahl der Clients mit gleicher Konfiguration soll im Sinne kostengünstiger IT-Prozesse möglichst groß sein. Gleichzeitig bestehen unterschiedliche standortspezifische Anforderungen, heterogene Hardware und weitere Faktoren, die eine einheitliche Konfiguration nicht zulassen.

Die Scout Enterprise Management Suite trägt dieser Situation Rechnung: Das Vererbungsprinzip führt zu größtmöglicher Effizienz, während jede Ebene bis zum einzelnen Gerät die Flexibilität für Änderungen bietet.

Die auf oberster Ebene definierte Basis-Konfiguration vererbt ihre Eigenschaften im Standardfall bis auf das einzelne Gerät. Zusätzlich können Sie auf allen Ebenen Abweichungen definieren.

Hinweis
Änderungen in der Geräte-Konfiguration werden beim nächsten Neustart der betroffenen Geräte aktiv.

Achtung
Beachten Sie, dass die Konfiguration der Clients in Abhängigkeit der auf den Clients installierten Software-Paketen erfolgt.

5.1.1. Vererbung der Konfiguration

Die Basiskonfiguration und die Konfiguration von OUs können auf niedrigere Instanzen vererbt werden.

Die Basiskonfiguration ist die höchste Instanz. Niedrigere Instanzen können weitere OUs oder auch einzelne Geräte sein. Jedes Element kann sich entweder auf die Konfiguration der übergeordneten Instanz in der Hierarchie beziehen oder individuell konfiguriert werden.

Wenn die Option **Übergeordnete Instanz verwenden** aktiv ist, so wird die Konfiguration des nächsthöheren Elementes in der Hierarchie (ein solches Element wird hier „Instanz" genannt) auf die aktuell bearbeitete Instanz angewendet. Standardmäßig ist die Verwendung der übergeordneten Instanz durch die Option **Übergeordnete Instanz verwenden** aktiv, sodass ein Gerät seine Konfiguration von der Basiskonfiguration erbt.

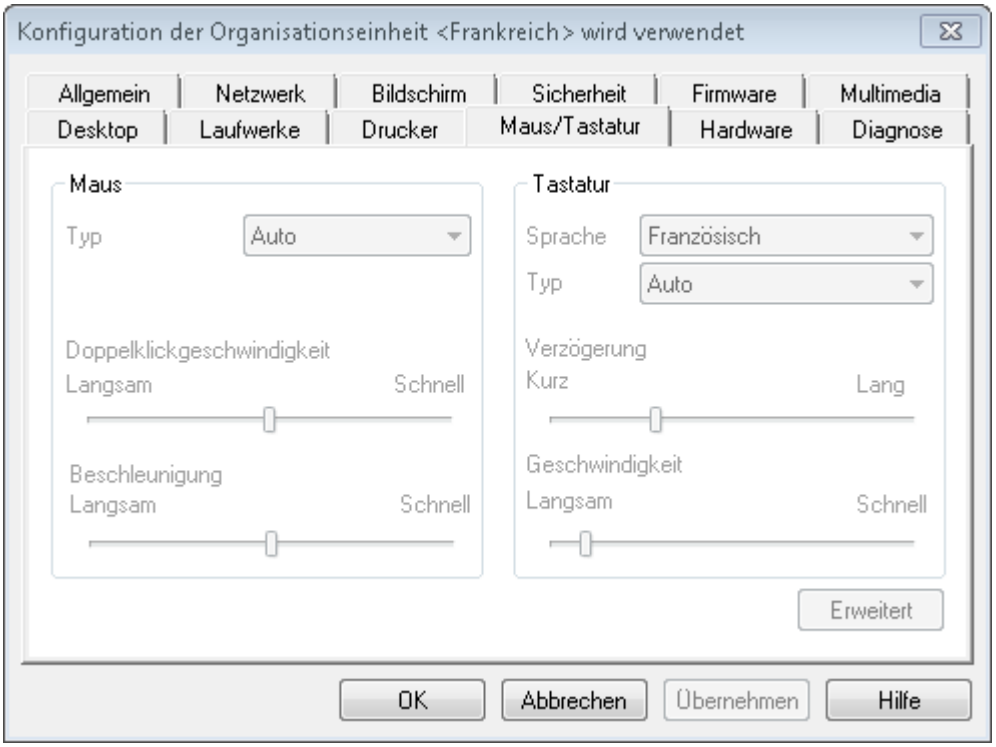
Die Setup-Einstellungen können auf drei Ebenen in der Scout Enterprise-Konsole verändert werden:

- Basiskonfiguration (**Optionen > Basiskonfiguration**)
- OU (**Kontextmenü > Konfiguration**)
- Gerät (**Kontextmenü > Konfiguration**)

Auf jeder Ebene können die Einstellungen der übergeordneten Ebene übernommen oder abweichende Einstellungen konfiguriert werden. Um abweichende Einstellungen konfigurieren zu können, müssen Sie die Vererbung unterbrechen.

Hinweis

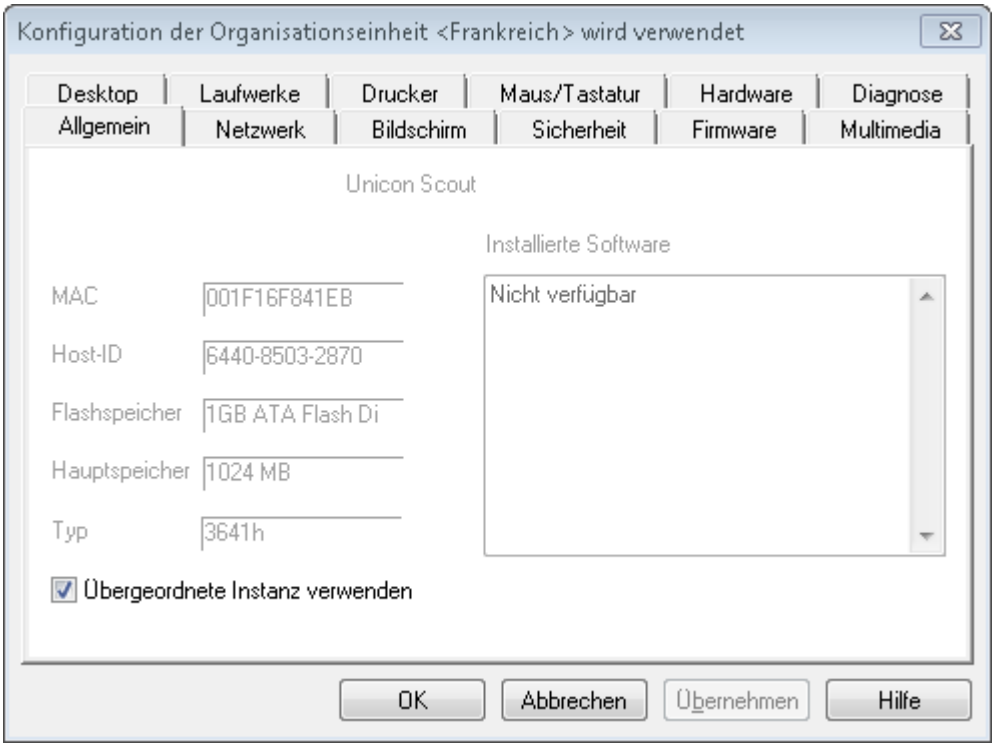
Beachten Sie den jeweils in der Titelleiste des Konfigurations-Dialogs angezeigten Gültigkeitsbereich. Das kann die Basis-Konfiguration oder eine übergeordnete OU sein.



Beispiel: Wenn Sie die Konfiguration einer Instanz öffnen, die der OU `Frankreich` untergeordnet ist, und wenn die Vererbung eingeschaltet ist, zeigt die Titelleiste die **Konfiguration der Organisationseinheit <Frankreich>** an. Eventuelle Änderungen müssen dort vorgenommen werden.

5.1.2. Vererbung unterbrechen - unabhängige Konfiguration

Wenn Sie für eine bestimmte OU oder für ein bestimmtes Gerät abweichende Einstellungen konfigurieren möchten, müssen Sie in der Konfiguration dieser Instanz die Vererbung unterbrechen.



1. Öffnen Sie das Kontextmenü der relevanten Instanz (OU oder Gerät) und wählen Sie den Eintrag **Konfiguration...**.

   Der Konfigurations-Dialog öffnet und zeigt in der Titelleiste die aktuell gültige Instanz für die Konfiguration an. Das kann die Basiskonfiguration oder eine übergeordnete OU sein. Für weitere Informationen siehe Konfiguration öffnen.

2. Deaktivieren Sie im Register **Allgemein** die Option **Übergeordnete Instanz verwenden**.

Die Vererbung ist unterbrochen. In der Titelleiste des Dialogs wird die aktuelle Instanz angezeigt und alle Optionen sind editierbar. Diese Instanz und die ihr untergeordneten Instanzen können unabhängig von den übergeordneten Instanzen konfiguriert werden.

Hinweis

Im Fenster **Unabhängige Konfigurationen** werden alle OUs und Geräte angezeigt, die NICHT die übergeordnete Instanz verwenden.

In **Ansicht > Einstellungen** können Sie festlegen, ob nach dem Ändern einer Konfiguration alle untergeordneten unabhängigen Konfigurationen geprüft werden sollen. Sie erhalten dann eine Übersicht über die jeweiligen Parameter und können komfortabel festlegen, ob und auf welche Instanzen die Änderungen übertragen werden sollen.

5.1.3. Lokale Konfiguration schützen

Die Benutzerrechte zur Bearbeitung der lokalen Gerätekonfiguration können für einzelne Geräte und OUs bis auf Feldebene eingestellt werden. Bestimmte Felder und Register können aus Sicherheitsgründen gesperrt und abgeblendet werden, während einzelne Funktionen wie beispielsweise die Monitoreinstellungen zugelassen werden können. Für weitere Informationen siehe Benutzerrechte ändern.

Wenn individuelle oder lokale Konfigurationen zugelassen werden, sollen diese beim Aktualisieren der Konfiguration beim Neustart der Geräte nicht überschrieben werden.

Lokale Konfiguration schützen:

1. Wählen Sie **Optionen > Erweiterte Optionen... > Geräte**.
2. Aktivieren Sie unter **Feldaktualisierung** die Option **Nur gesperrte Felder werden am Client aktualisiert**.

Beim nächsten Laden der Konfiguration werden nur die gesperrten Register und Felder aktualisiert. Lokale Benutzerkonfigurationen in nicht gesperrten Feldern bleiben erhalten.

Für den Fall, dass ein Benutzer eine fehlerhafte Konfiguration durchgeführt hat, kann der Administrator festlegen, dass beim nächsten Neustart des Geräts die gesamte Konfiguration neu geladen wird.

Einmalige Aktualisierung der gesamten Konfiguration veranlassen

- Öffnen Sie in Scout Enterprise für das entsprechende Gerät das Kontextmenü und wählen Sie **Vormerkung > Aktualisierung veranlassen...**

Für das Gerät wird vorgemerkt, dass beim nächsten Neustart die gesamte Konfiguration inklusive nichtgesperrten Feldern mit der in Scout Enterprise definierten Gerätekonfiguration überschrieben wird.

5.1.4. Konfiguration öffnen

Basiskonfiguration öffnen

- Wählen Sie im Scout Enterprise-Menü **Optionen > Basiskonfiguration...**

*Der Dialog **Basiskonfiguration** öffnet. Der Dialog enthält die globale Konfiguration, die für alle untergeordneten Elemente gilt, solange keine Abweichungen definiert sind.*

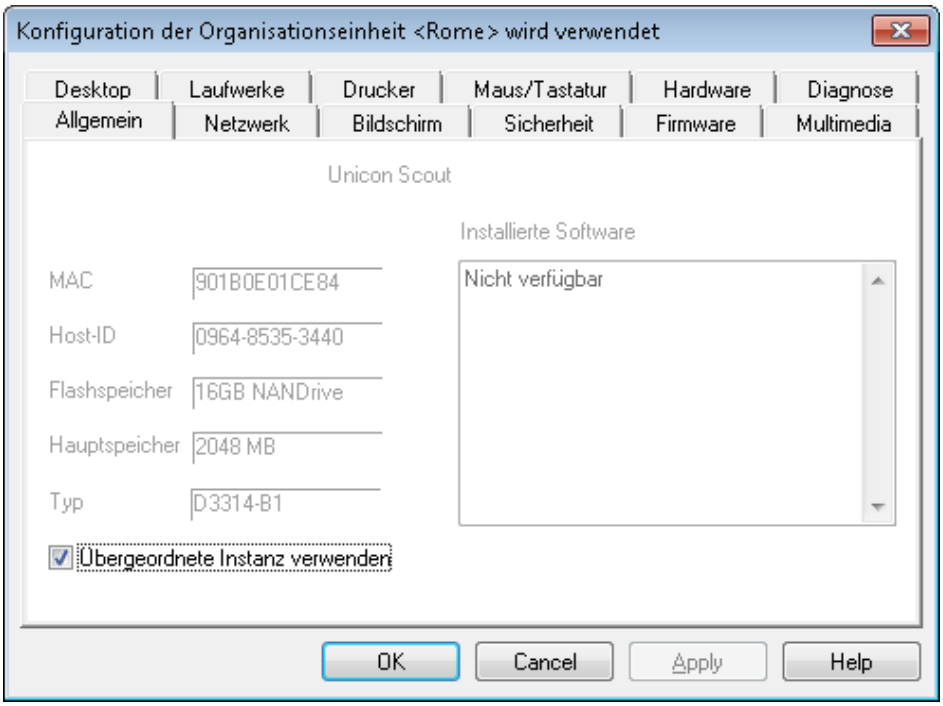
Konfiguration für ein Gerät oder OU öffnen

- Markieren Sie das relevante Element in der Baumstruktur und wählen Sie im Menü **Bearbeiten > Konfiguration...**

oder

- Öffnen Sie für das relevante Element das Kontextmenü und wählen Sie **Konfiguration...**

*Der Dialog **Konfiguration** für das markierte Element öffnet. Möglicherweise sind die Optionen abgeblendet, weil die Option **Übergeordnete Instanz verwenden** eingeschaltet ist. Die jeweilige OU oder die Basiskonfiguration wird dann in der Titelleiste angegeben.*



Jeweils gültige Konfiguration öffnen

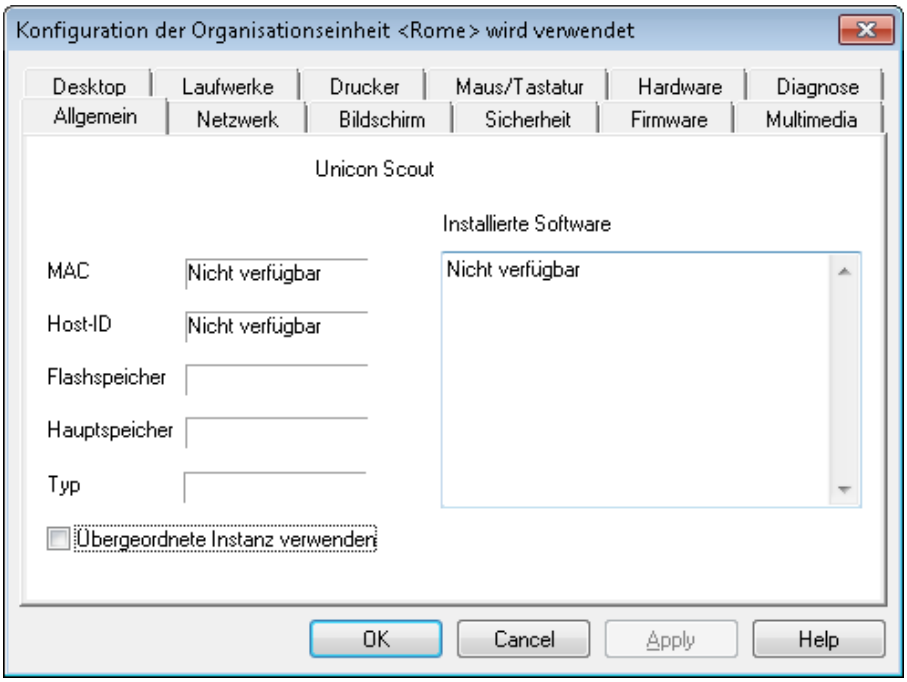
1. Markieren Sie das relevante Element in der Baumstruktur.
2. Um das **Eigenschaften**-Fenster anzuzeigen, wählen Sie **Ansicht > Fenster >**

Eigenschaften-Fenster.

*Im **Eigenschaften**-Fenster, in der Zeile **Konfiguration** wird die vom markierten Element verwendete Konfiguration angezeigt.*

3. Doppelklicken Sie im **Eigenschaften**-Fenster auf **Konfiguration**.

Die aktuell gültige Konfiguration wird geöffnet. Dies kann die Konfiguration einer übergeordneten Instanz sein.



5.1.5. Konfiguration zwischen OUs/Geräten vergleichen

Der Vergleich zwischen den Konfigurationen verschiedener Geräte oder verschiedener OUs ist über ein Fenster möglich, das Sie permanent einblenden können.

1. Wählen Sie den Menübefehl **Ansicht > Fenster > Konfigurationsvergleich**.

   *Das Fenster **Konfigurationsvergleich** wird im unteren Bereich eingeblendet.*

2. Ziehen Sie per Drag&Drop zwei oder mehr OUs oder Geräte in das Fenster **Konfigurationsvergleich**.
   Oder:
   Wählen Sie im Kontextmenü des Gerätes oder der OU den Eintrag **Bearbeiten > Zu Konfigurationsvergleich...**.

3. Klicken Sie in der Symbolleiste des Fensters **Konfigurationsvergleich** auf das Icon  .

   Die Konfigurationen der aufgelisteten OUs oder Geräte werden miteinander verglichen und die Unterschiede in den wesentlichen Eigenschaften werden angezeigt.

4. Wenn Sie alle Informationen anzeigen möchten, klicken Sie auf das Icon 

in der Symbolleiste des Fensters **Konfigurationsvergleich**.

   Alle Eigenschaften werden angezeigt.

Hinweis

Mit dem Soll-Ist-Vergleich für ein einzelnes Gerät können Sie überprüfen, ob der Client die aktuelle Konfiguration hat. Für weitere Informationen siehe Konfiguration vergleichen (Soll – Ist).

5.2. Konfigurationsmethode

Während die mit Scout Enterprise verwalteten Clients starten, verbinden sie sich zu ihrem Scout Enterprise-Server und prüfen, ob Aktualisierungen vorliegen. Aktualisierungen können sich auf die Gerätekonfiguration, aber auch auf Anwendungsdefinition, konfigurierte Dateiübertragung und Erweiterte Dateieinträge beziehen. Wenn aktualisierte Konfigurationsinformationen vorhanden sind, werden diese zum Client übertragen. Für weitere Informationen siehe Kommunikation zwischen Thin Client und Scout Enterprise Server.

5.2.1. Konfigurationslauf

Wenn bei der Prüfung auf aktualisierte Konfigurationsinformationen festgestellt wird, dass Aktualisierungen für einen Client vorliegen, werden die Konfigurationsinformationen ermittelt, komprimiert in der Datenbank abgespeichert und anschließend in einem Schritt an den Client übertragen. Bei Konfigurationsänderungen, die eine große Anzahl der Clients betreffen (beispielsweise Änderung von Anwendungsdefinitionen wegen Schwenk in eine andere Backend-Infrastruktur), kann die Ermittlung und komprimierte Speicherung der Konfigurationsinformationen vorab (z.B. abends/nachts) initiiert werden. Die dadurch vorbereiteten Konfigurationsinformationen werden beim nächsten Neustart der Clients (z.B. am nächsten Arbeitstag) in einem Schritt übertragen.

Die Vorbereitung der Konfigurationsinformationen wird über das Kommando **Konfigurationslauf** für eine Gruppe von Geräten (OU oder Dynamische Gerätegruppe) angestoßen. Die Ausführung kann sofort oder zeitgesteuert erfolgen. Der Bearbeitungsfortschritt ist im Dialog **Kommandoverlauf** ersichtlich.

Über den Konfigurationslauf werden Konfigurationsinformationen ausschließlich für diejenigen Clients vorbereitet, für die ein Delta in der Konfiguration ermittelt wurde.

5.2.2. Snapshot-Verfahren (Scout Enterprise Management Suite Version 14.5)

Die folgende Funktionalität ist ausschließlich in Scout Enterprise Version 14.5.x enthalten und nur dort zu berücksichtigen.

Hinweis

Ab Version 14.6.0 wurden die wesentlichen Vorteile des Snapshot-Verfahrens in das Standardverfahren integriert und damit eine Verbesserung der Gesamtperformance erreicht. Dabei wurde

- die Ermittlung der Konfigurationsinformationen zur Laufzeit mit
- der Übertragung der komprimierten Konfigurationsinformationen

kombiniert.

Standardmäßig wird die Ermittlung zur Laufzeit angewendet.

Snapshot-Verfahren aktivieren

- Wählen Sie in der Scout Enterprise-Konsole **Optionen > Erweiterte Optionen > Geräte > Konfigurationsmethode > Snapshot-Verfahren**.

Ab sofort wird bei der Verbindung von Clients mit der erforderlichen eLux RP-Version zum Scout Enterprise-Server nur noch auf die Snapshot-ID geprüft.

Hinweis

Zur Bereitstellung von Konfigurationsinformationen für die Clients muss nach der Aktivierung des Snapshot-Verfahrens ein initialer Konfigurations-Snapshot durch den Scout Enterprise-Administrator erstellt werden.

Snapshot-Verfahren

Die Ermittlung der Konfigurationsinformationen und die Übertragung an die Clients erfolgt mit dem neuen Snapshot-Verfahren in zwei unabhängigen Schritten:

- Ermittlung der Konfigurationsinformationen für **alle** Clients und Speichern in der Scout Enterprise-Datenbank (Konfigurations-Snapshot) zu einem frei definierbaren Zeitpunkt
- Übermittlung aktualisierter Konfigurationsinformationen an die Clients in einem kompakten Schritt bei Verbindung der Clients mit dem Scout Enterprise-Server nach Geräte-Neustart (nur bei Bedarf)

Durch dieses Verfahren wird die Konfigurationsermittlung vom Zeitpunkt der Verbindung der Clients zum Scout Enterprise Server entkoppelt. Das Risiko einer unvollständigen Konfigurationsübertragung

aufgrund erhöhter Serverlast bei ungünstigen Bedingungen wird damit weitestgehend ausgeschlossen.

Die Ermittlung der Konfigurationsinformationen erfolgt durch die Erstellung eines Konfigurations-Snapshots für alle verwalteten Geräte

- durch den Scout Enterprise-Administrator
- zu einem beliebigen Zeitpunkt
- in der Scout Enterprise-Konsole

Dabei werden für jeden Client die Konfigurationsinformationen ermittelt und mit einer eindeutigen Snapshot-ID in der Scout Enterprise-Datenbank abgespeichert.

Bei Verbindung eines Clients zum Scout Enterprise-Server prüft der Server, ob der Client bereits die Konfiguration mit der zuletzt erzeugten Snapshot-ID verwendet. Ist dies nicht der Fall, werden die komprimierten Konfigurationsinformationen des zuletzt erstellten Snapshots in einem Schritt zum Client übertragen.

Eine Ermittlung der Konfigurationsinformationen zur Laufzeit ist nicht mehr notwendig.

Hinweis
Wenn Sie ein **Update**-Kommando durchführen, werden die relevanten Informationen als URL an die Clients übermittelt. Hierbei werden die Werte aus der **Geräte-Konfiguration/Firmware** verwendet, die zum Zeitpunkt der Kommando-Ausführung eingetragen sind. Dies gilt auch dann, wenn diese Daten noch nicht Bestandteil des letzten Konfigurations-Snapshots sind. Für weitere Informationen siehe Update planen.

Voraussetzungen zur Anwendung des Snapshot-Verfahrens

- Scout Enterprise Management Suite Version 14.5
- eLux RP Version 4.10 und höher
  oder
  eLux RP Version 5.1 und höher

Clients mit älteren eLux RP-Versionen können die Konfigurationsinformationen des Snapshots nicht verarbeiten. Der Scout Enterprise-Server versorgt diese Geräte nach dem alten Verfahren der Konfigurationsermittlung zur Laufzeit.

Für nachträglich eingebundene Geräte, die die erforderliche eLux RP-Version nutzen, wird ein dynamischer Snapshot erzeugt. Für weitere Informationen siehe Dynamischer Snapshot.

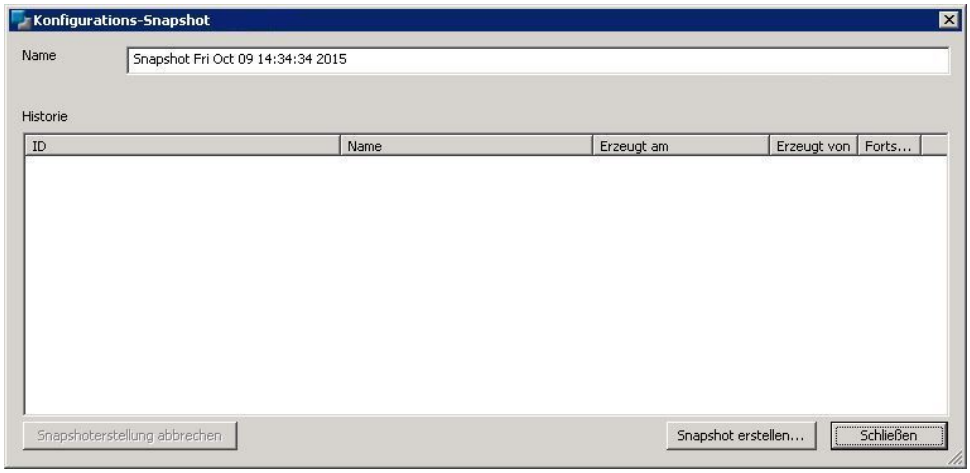
Konfigurations-Snapshot erstellen

Voraussetzung
Der Scout Enterprise-Administrator muss die entsprechende Menü-Berechtigung besitzen.

Achtung

Während der Erstellung eines Konfigurations-Snapshots werden alle Scout Enterprise-Konsolen (auch die eigene) gesperrt.

1. Wählen Sie in der Scout Enterprise-Konsole **Datei > Konfigurations-Snapshot erstellen**.



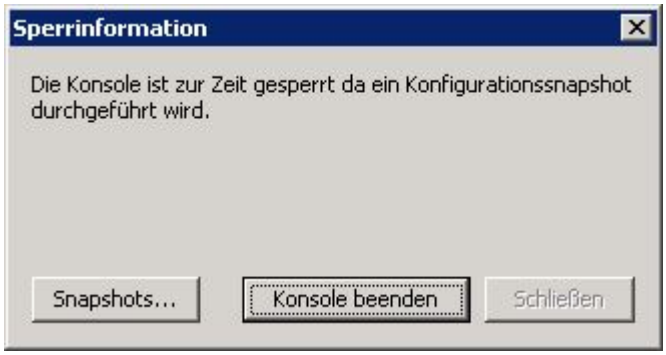
2. Ergänzen oder überschreiben Sie den vorgegebenen Snapshot-Namen und bestätigen Sie mit **Snapshot erstellen...**

   Der Scout Enterprise-Serverdienst ermittelt die geschätzte Laufzeit des Snapshots für alle Geräte.

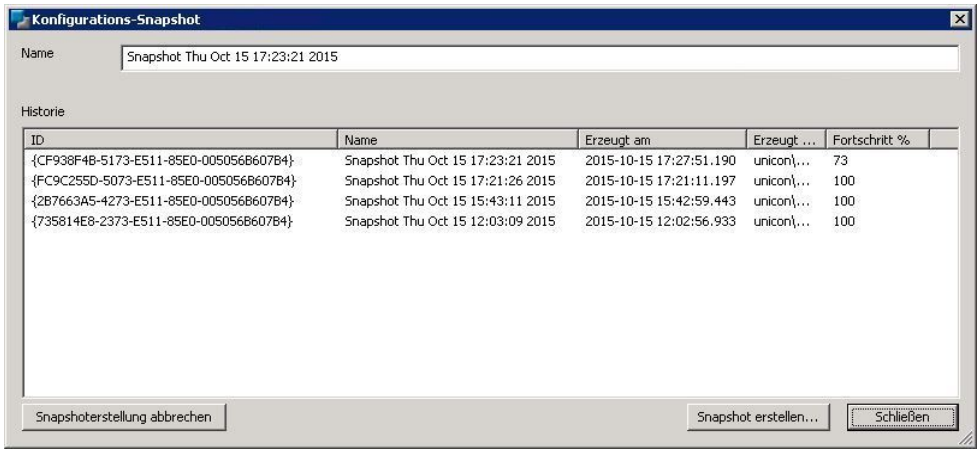
3. Bestätigen Sie mit **Ja**.

   *Der Snapshot wird in der Historie des Dialogs eingetragen und der Verarbeitungsstatus wird in der Spalte **Fortschritt %** angezeigt.*

   *Während der Snapshot-Erstellung sind alle Scout Enterprise-Konsolen gesperrt und der Dialog **Sperrinformation** wird angezeigt:*



4. Wenn gewünscht, klicken Sie im **Sperrinformation**-Dialog auf **Snapshots...** (nur für berechtigte Administratoren sichtbar), um in den Dialog **Konfigurations-Snapshot** zurückzukehren:



Der Prozess der Snapshot-Erstellung kann jederzeit abgebrochen werden. Die bis zum Abbruch erstellten Konfigurationsinformationen werden dann verworfen.

Ein Snapshot mit einer eindeutigen ID für alle Geräte ist erstellt. Von nun an prüfen Clients mit der erforderlichen eLux RP-Version beim Starten lediglich gegen die Snapshot-ID des Scout Enterprise-Servers.

Hinweis

Sobald Sie Änderungen an der Geräte-Konfiguration, den Anwendungsdefinitionen, der konfigurierten Dateiübertragung oder den Erweiterten Dateieinträgen vornehmen, ist die Erstellung eines neuen Snapshots erforderlich.

Dynamischer Snapshot

Bei der Erstinbetriebnahme neuer Geräte oder beim Geräteumzug von einem anderen Scout Enterprise-Server kann bei eingeschaltetem Snapshot-Verfahren folgende Situation entstehen:

Geräte mit der erforderlichen eLux RP-Version (Version 4.10 und höher oder Version 5.1 und höher) werden zu einem Zeitpunkt in die Verwaltung mit Scout Enterprise eingebunden, der nach der letzten Snapshot-Erstellung liegt. Für diese Geräte wird ein dynamischer Snapshot erzeugt. Hierbei werden automatisch die nach dem alten Verfahren ermittelten Konfigurationsdaten in der Scout Enterprise-Datenbank abgespeichert und anschließend an den Client übertragen.

Ein dynamischer Snapshot wird also nach dem letzten Konfigurations-Snapshot des Administrators für Geräte erstellt, die den Snapshot "verpasst" haben. Wenn die Gerätekonfiguration nach dem letzten Konfigurations-Snapshot verändert wurde, enthält der dynamische Snapshot bereits die neuen Konfigurationseinstellungen.

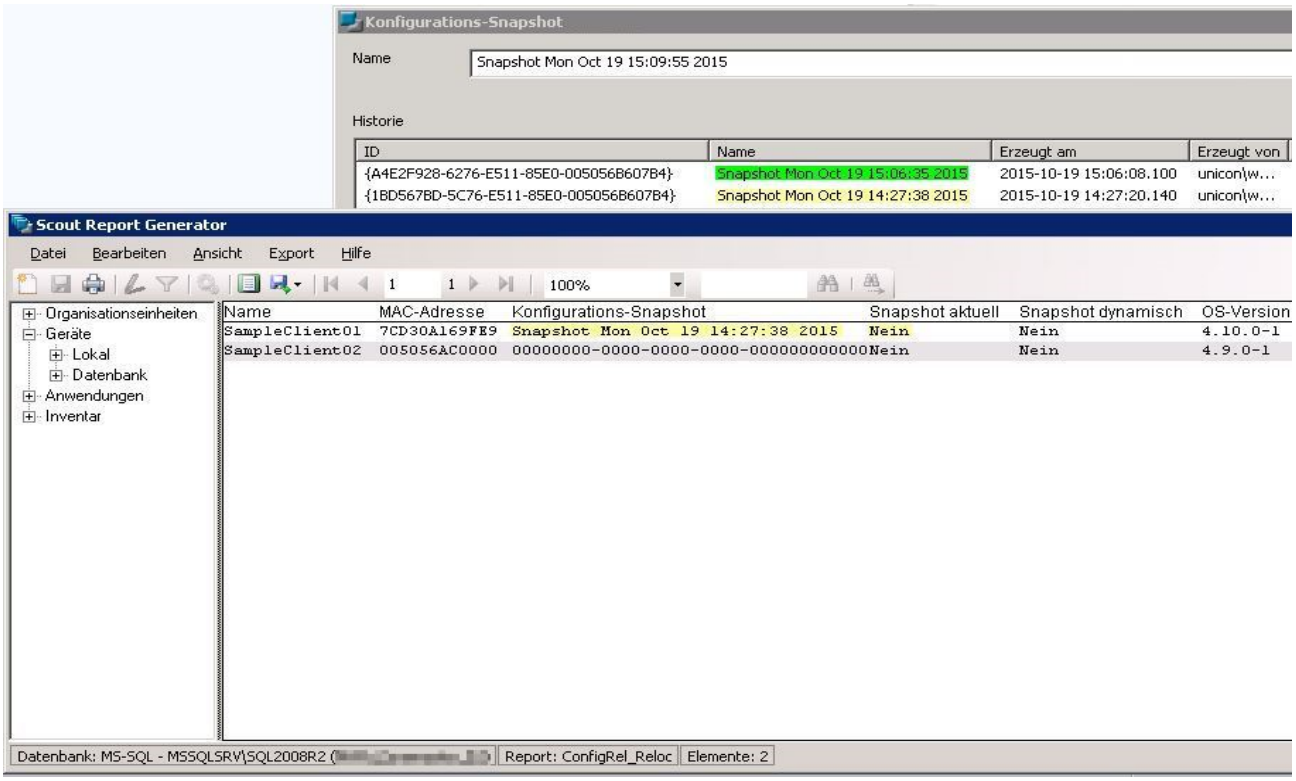
Mit der erneuten Erstellung eines Konfigurations-Snapshots durch den Scout Enterprise-Administrator werden die Konfigurationsinformationen für alle Geräte wieder vereinheitlicht.

Mit Hilfe eines Reports ermitteln Sie alle Geräte, die nicht die aktuellen Konfigurationsinformationen des letzten Snapshots verwenden bzw. nach dem letzten Snapshot in die Scout Enterprise-Vewaltung aufgenommen wurden. Für weitere Informationen siehe Auswertung der Konfigurationsinformationen.

Auswertung von Konfigurationsinformationen

Hinweis
Die Auswertung der auf den Clients verwendeten Konfigurationsinformationen bezieht sich auf das Snapshot-Verfahren.

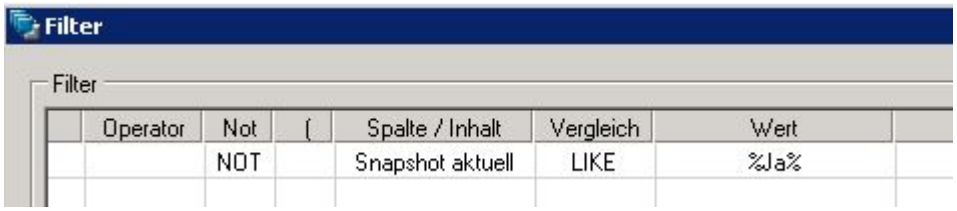
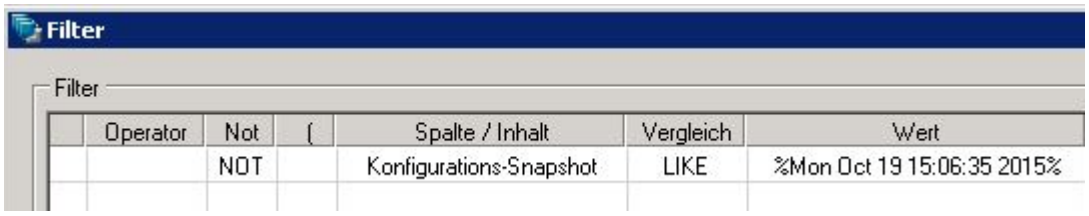
Der Report-Generator bietet die Möglichkeit, alle Geräte zu listen, die nicht die aktuellen Konfigurationsinformationen des letzten Snapshots verwenden:



Hinweis

Geräte mit älteren eLux-Versionen werden im Feld **Konfigurations-Snapshot** mit dem Wert `00000000-0000-0000-0000-000000000000` und im Feld **Snapshot aktuell** mit dem Wert `Nein` angezeigt.

Folgende Felder können Sie als Filterkriterien verwenden:

Feld	Beispiel/Beschreibung
Snapshot aktuell	
Konfigurations-Snapshot	
Snapshot dynamisch	Ermittlung von Geräten, die **nach** der letzten Snapshot-Erstellung in die Verwaltung des Scout Enterprise-Servers aufgenommen wurden (z.B. Erstinbetriebnahme neuer Geräte oder Geräteumzug von einem anderen Scout Enterprise-Server). Für weitere Informationen siehe Dynamischer Snapshot.

5.2.3. Ermittlung zur Laufzeit

– Verfahren bis Scout Enterprise Management Suite Version 14.4 –

Sobald sich ein Client nach dem Geräte-Neustart mit dem Scout Enterprise-Server verbindet, werden die Konfigurationsdaten unter Berücksichtigung der Vererbung ermittelt und in mehreren Einzelschritten (je nach Komplexität der Konfiguration) an den Client übertragen.

Der Scout Enterprise-Server ermittelt die relevanten Konfigurationsinformationen zur Laufzeit. Das bedeutet, dass alle bis zu diesem Zeitpunkt in der Scout Enterprise-Konsole durchgeführten Konfigurationsänderungen berücksichtigt werden und direkt an die Clients übertragen werden.

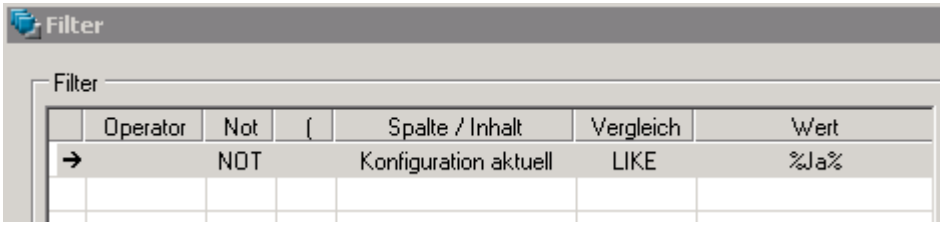
Die zeitgleiche Verbindung einer großen Anzahl von Clients mit dem Scout Enterprise Server kann – je nach Client-Anzahl und Systemperformance des Servers und der Datenbank – zu einer hohen Auslastung des Scout Enterprise-Servers führen. In extremen Situationen (z.B. mehrere tausend Geräte werden gleichzeitig eingeschaltet und die Systemperformance von Server oder Datenbank ist nicht ausreichend) kann es zu einer unvollständigen oder nicht durchgeführten Übertragung der Konfigurationsinformationen an Geräte kommen.

Hinweis
Die Übertragung der Konfigurationsinformationen an die Geräte kann zusätzlich – unabhängig von der Konfigurationsmethode – durch die **Handshake**-Funktion gewährleistet und optimiert werden. Für weitere Informationen siehe Optimierung durch Handshake.

5.3. Auswertung von Konfigurationsinformationen

Der Report-Generator bietet die Möglichkeit, alle Geräte zu listen, die nicht die aktuellen Konfigurationsinformationen verwenden:

Hinweis
Geräte mit älteren eLux-Versionen werden im Feld **Konfiguration aktuell** mit dem Wert `Nein` angezeigt.



5.4. Register Allgemein

Im Register **Allgemein** befindet sich die Option **Übergeordnete Instanz verwenden**. Wenn die Option aktiv ist, sind alle anderen Felder im Dialog abgeblendet.

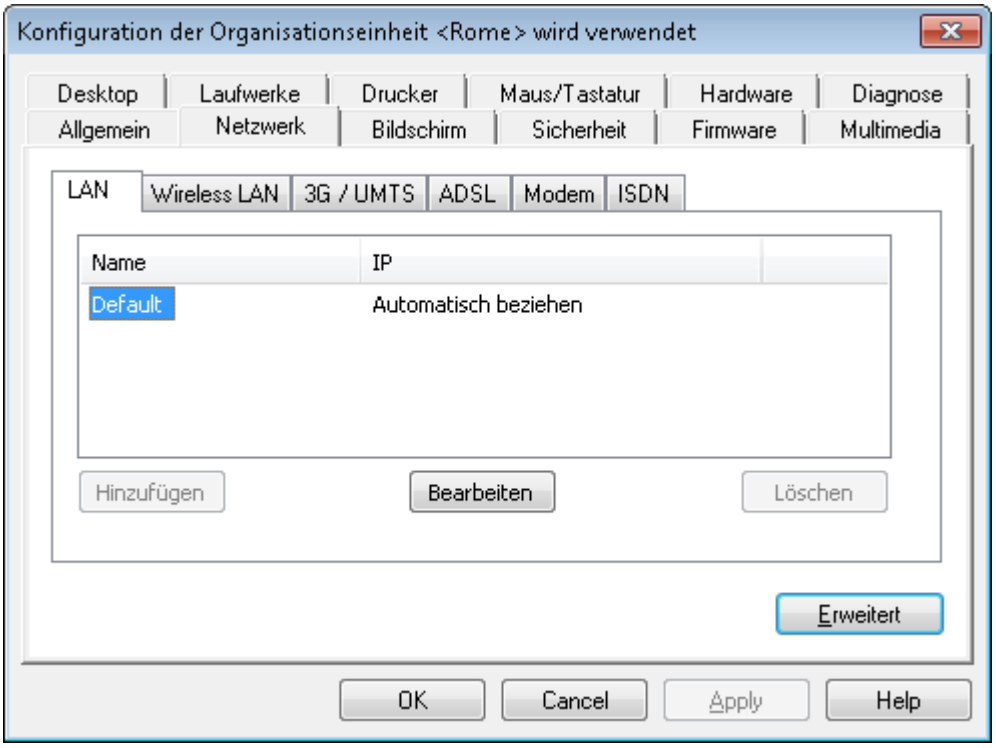
Hinweis
In manchen Situationen kann es sinnvoll sein, die Option **Übergeordnete Instanz verwenden** vorübergehend auszuschalten. Für weitere Informationen, siehe Vererbung unterbrechen.

Außerdem werden einige gerätespezifische Hardwareinformationen angezeigt, wenn es sich um die Konfiguration eines einzelnen Geräts handelt. Weitere Geräte-Eigenschaften finden Sie im **Eigenschaften**-Fenster der Scout Enterprise-Konsole.

Option	Beschreibung
MAC-Adresse	Geräteadresse der Hardware (MAC=Media Access Control)
Host-ID	Dem Gerät zugewiesene eLux Host-ID, für das Lizenzierungsverfahren erforderlich
Flash-Speicher	Kurze Beschreibung des Flash-Speichertyps und dessen Größe
Arbeitsspeicher	Größe des Arbeitsspeichers (RAM) in Megabyte.
Typ	Produktbeschreibung seitens des Hardwarelieferanten (Zeichenkette).

5.5. Register Netzwerk

Abhängig vom installierten Image und der eingebauten Hardware können Sie mehrere Netzwerkprofile parallel einrichten. Konfigurierte Netzwerkverbindungen kann der Benutzer am Client über das entsprechende Systray-Icon auswähen.



5.5.1. Erweiterte Netzwerkeinstellungen

Unter **Konfiguration > Netzwerk > Erweitert** finden Sie die Hosts-Liste und Funktionen, die sich auf alle Netzwerkverbindungen beziehen.

Timeout für Verbindung einstellen

- Geben Sie unter **Management Timer** die relevante Timeout-Zeit in Sekunden in das jeweilige Feld ein.
  - bei **Verbindungsaufbau**.
  - bei **Leerlauf**.

Nachdem die angegebene Zeit verstrichen ist, wird die Client-Verbindung abgebrochen.

Die Option **Sende Keepalive-Paket** sorgt dafür, dass der Client sich im angegebenen Zeitintervall beim Scout Enterprise Server meldet. Für weitere Informationen siehe Definieren von Statusmeldungen (keep alive messages).

Hosts-Liste für Netzwerke ohne DNS-Server festlegen

Wenn das Netzwerk nicht über einen Domain Name Server (DNS) verfügt, können Hostnamen vom Gerät lokal aufgelöst werden. Voraussetzung ist, dass die Hostnamen in der Host-Liste gepflegt werden.

1. Klicken Sie auf **Neu**.
2. Geben Sie die Hostnamen und IP-Adressen ein.
3. Bestätigen Sie mit **OK**.

Beim Neustart des Thin Client wird die Host-Liste automatisch übertragen.

5.5.2. LAN-Verbindung konfigurieren

1. Öffnen Sie in der Scout Enterprise Konsole für das relevante Gerät oder OU den Dialog **Konfiguration > Netzwerk**. Am Client wählen Sie das Register **Setup > Netzwerk**.
2. Wählen Sie das Register **LAN** und klicken Sie auf die Schaltfläche **Hinzufügen**.

   *Der Dialog **Netzwerkprofil bearbeiten** öffnet.*
3. Geben Sie im Register **Ethernet** an, ob die IP-Adresse vom Server bezogen werden soll, oder bearbeiten Sie die Felder zur IP-Adresse.
4. Im Register **Erweitert** können Sie Einstellungen zu DHCP und DNS vornehmen und die IEEE 802.1x-Authentifizierung aktivieren.
5. Bestätigen Sie mit **OK**.

5.5.3. WLAN-Verbindung konfigurieren

Folgende Konfigurationsmöglichkeiten stehen zur Verfügung:

A. Ein WLAN-Profil kann in der Scout Enterprise-Konsole in der Geräte-Konfiguration für ein Gerät, eine OU oder alle Geräte definiert werden, siehe unten.
   Authentifizierung über einen RADIUS-Server (EAP) ist hierbei nicht möglich.

B. Ein WLAN-Profil kann lokal am Client erstellt werden. Ab eLux RP Version 5.6 können lokale und über Scout Enterprise definierte Profile automatisch zusammengeführt werden, so dass ein automatisches Verbinden je nach Umgebung stattfinden kann.

C. Corporate WLAN: Eine WLAN-Konfiguration kann als Unternehmensnetzwerk über eine WPA-Konfigurationsdatei mit und ohne 802.1x verteilt werden. Hierfür ist ein Dummy-WLAN-Profil in der Gerätekonfiguration erforderlich, das für die Clients versteckt werden kann.[1]
   Ab eLux RP Version 5.6 können Benutzer parallel zum Corporate WLAN individuelle WLAN-Profile lokal am Client erstellen. Für die konfigurierten WLAN-Netzwerke kann ein automatisches Verbinden je nach Umgebung oder Priorität stattfinden. Für weitere Informationen siehe WPA-Unterstützung und Corporate WLAN.

[1] ab eLux RP Version 5.6

WLAN-Profil in der Scout Enterprise-Gerätekonfiguration erstellen (A)

1. Öffnen Sie in der Scout Enterprise Konsole für die relevante OU den Dialog **Konfiguration > Netzwerk**.
2. Wählen Sie das Register **Wireless LAN** und klicken Sie auf **Hinzufügen**.
3. Aktivieren Sie im Dialog **Netzwerkprofil bearbeiten** die Option **Automatisch starten**.

   Hinweis
   Wenn die Option **Automatisch starten** nicht aktiv ist, erfolgt kein automatischer Start eines WLAN-Netzes aus der vorhandenen Liste am Client. In diesem Fall muss das WLAN lokal am Client über das Systray gestartet werden.

4. Geben Sie im Register **IP** an, ob die IP-Adresse vom Server bezogen werden soll, oder bearbeiten Sie die Felder zur IP-Adresse.
5. Bearbeiten Sie im Register **Medium** folgende Felder:

Option	Beschreibung
SSID	Service Set Identifier Name für das WLAN-Netzwerk
Timeout	Zeitspanne in Sekunden für den Verbindungsaufbau bis zum Abbruch
Kanal	Wird standardmäßig automatisch gewählt
Verschlüsselung	Art der Authentifizierung Wählen Sie `WPA` oder `WPA2` mit Pre-shared key (PSK) - verwenden Sie nicht `WPA-EAP` oder `802.1x`. Um über EAP (Extensible Authentication Protocol) zu authentifizieren, verwenden Sie eine WPA-Konfigurationsdatei. Für weitere Informationen siehe WPA-Unterstützung.

6. Im Register **Erweitert** können Sie Einstellungen zu DHCP und DNS vornehmen.
7. Bestätigen Sie mit **OK**.

Hinweis
Ein lokales WLAN-Profil am Client (B) kann mit entsprechenden Benutzerrechten in der eLux-Systemsteuerung mit der gleichen Vorgehensweise erstellt werden.

WLAN-Profil-Editor am Client anzeigen

Vorhandene WLAN-Netzwerke werden am Client über das Netzwerk-Symbol im Systray angezeigt. Zusätzlich kann der WLAN-Profil-Editor in einem Popup-Fenster angezeigt werden, sobald ein unbekanntes WLAN-Netzwerk erkannt wird:

- Verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole:

Datei	`/setup/terminal.ini`
Abschnitt	`Layout`
Eintrag	`NotifyNewWLAN`
Wert	`true`

Für weitere Informationen siehe Erweiterte Dateieinträge.

5.5.4. WPA-Unterstützung

Zur Sicherung Ihres WLAN können Sie die WPA-Verschlüsselung mit Hilfe des Programms `WPA-Supplicant` einsetzen. Diese Software übernimmt den Schlüsselaustausch mit dem WPA-Authentifizierer und steuert die Verbindung mit IEEE 802.11i-Netzwerken. Unterstützt werden WPA (IEEE 802.1x) und WPA2 (IEEE 802.11i). Die Authentifizierung kann über Pre-shared key (PSK) und für IEEE 802.1x über das Extensible Authentication Protocol (EAP) erfolgen.

Die Konfiguration wird in der Textdatei `wpa.conf` vorgenommen, die akzeptierte Netzwerke und Sicherheitsrichtlinien enthalten kann. Die Konfigurationsdatei wird auf den Clients lokal gespeichert im Verzeichnis */setup/wlan/*.

`WPA-Supplicant` ist eine freie Software. Für weitere Informationen siehe http://packages.debian.org/de/sid/wpasupplicant.

WPA-Konfigurationsdatei bereitstellen

1. Erstellen Sie eine Textdatei mit Namen *wpa.conf* mit Hilfe des Programms wpa_supplicant. Ein Beispiel finden Sie weiter unten.
2. Konfigurieren Sie die Dateiübertragung für die relevanten Geräte mit Hilfe der Funktion Erweiterte Konfiguration > Dateien.
3. Aktivieren Sie im Dialog **Dateien hinzufügen** die Option **Datei in Datenbank importieren** und wählen Sie über die Schaltfläche **...** die soeben erstellte Datei *wpa.conf* als Quelldatei aus dem Dateisystem.
4. Setzen Sie den Pfad für den Client im Feld **Zieldatei** auf */setup/wlan/wpa.conf*.
5. Bestätigen Sie mit **OK** und **Übernehmen**.

Für weitere Informationen siehe Konfigurierte Dateiübertragung.

Hinweis
Zusätzlich ist die Konfiguration eines Dummy-WLAN-Profils in der Gerätekonfiguration erforderlich. Für weitere Informationen siehe Corporate WLAN.

Beispiel für eine WPA-Konfigurationsdatei mit 802.1x

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
```

```
ap_scan=1
network={
    ssid=__MYSSID__
    scan_ssid=1
    key_mgmt=WPA-EAP
    eap=TLS
    identity=__IDENTITY__
    priority=6
    ca_cert="/setup/cacerts/serverca.pem"
    client_cert="/setup/cacerts/client.pem"
    private_key="/setup/cacerts/client.key"
}
```

5.5.5. Corporate WLAN

Ein Corporate WLAN als Unternehmensnetzwerk, das Zugriff auf interne Ressourcen bietet, kann über 802.1x abgesichert werden und mit Firewall Richtlinien versehen werden, die auf Grup-penzugehörigkeit, Standort oder Geräte abgestimmt werden.

Eine entsprechende WLAN-Konfiguration verteilen Sie über die WPA-Konfigurationsdatei, siehe WPA-Unterstützung.
Zusätzlich definieren Sie ein Dummy-WLAN-Profil in der Gerätekonfiguration, siehe unten.

Wenn Sie ein Corporate WLAN einsetzen, können Sie den Benutzern erlauben, parallel dazu eigene WLAN-Profile zu erstellen.[1] Beispielsweise könnte ein mobiler Thin Client am Arbeitsplatz über die Docking-Station eine LAN-Verbindung verwenden und beim Abdocken automatisch auf das Corporate WLAN wechseln. Sobald der Client am Heimarbeitsplatz eingesetzt wird, verbindet sich eLux zu dem manuell konfigurierten WLAN.

Corporate WLAN konfigurieren

1. Erstellen Sie in der Basis-Konfiguration in **Netzwerk > Wireless LAN** ein neues WLAN-Profil. Dieses Profil dient nur als Dummy und ist am Client nicht sichtbar.[2]

Option	Wert	Beschreibung
Name	`#Dummy#`	Dieser Name sorgt dafür, dass dieses WLAN-Profil am Client für den Benutzer nicht sichtbar ist.[3] Dieser Name ist obligatorisch.
Automatisch star-ten	aktiviert	obligatorisch

[1] ab eLux RP Version 5.6
[2] ab eLux RP Version 5.6
[3] ab eLux RP Version 5.6

Option	Wert	Beschreibung
SSID	*<DummySSID>*	beliebig
Timeout		Verwenden Sie den Standardwert.
Kanal		Verwenden Sie den Standardwert.
Verschlüsselung	`WPA (PSK)`	Verwenden Sie nicht `WPA-EAP` oder `802.1x`.
PSK	*<Kennwort>*	beliebig, mindestens acht Zeichen

Für weitere Informationen siehe WLAN-Verbindung konfigurieren.

2. Setzen Sie einen erweiterten Dateieintrag, um die WLAN-Profile zusammenzuführen:

Datei	`/setup/terminal.ini`
Abschnitt	`Network`
Eintrag	`MergeWLANProfile`
Wert	`true`

Für weitere Informationen siehe Erweiterte Dateieinträge.

3. Verteilen Sie Ihre Corporate WLAN-Konfiguration über eine WPA-Konfigurationsdatei.

   Um eine höhere Priorität als für manuell erstellte WLAN-Profile (Priorität `5`) zu erreichen, setzen Sie den Wert **Priority** auf `6` oder höher.

   Für weitere Informationen siehe WPA-Unterstützung.

Der Benutzer kann lokal am Client zusätzlich zum Corporate WLAN eigene WLAN-Profile hinterlegen:

Lokales WLAN-Profil erstellen

1. Erstellen Sie in der Systemsteuerung **Setup > Netzwerk > Wireless LAN** ein neues WLAN-Profil.

   Wenn keine Netzwerkverbindung vorhanden ist, startet der WLAN-Profil-Editor in einem Popup-Fenster.

2. Aktivieren Sie im Dialog **Netzwerkprofil bearbeiten** die Option **Automatisch starten**.
3. Bearbeiten Sie die weiteren Felder. Für weitere Informationen siehe WLAN-Verbindung konfigurieren.
4. Stellen Sie die Verbindung zu dem definierten WLAN beim ersten Mal über das Systray-Netzwerksymbol und die Schaltfläche **Verbinden** her.

Wenn die Verbindung zu einem WLAN vorhanden ist, wird das verbundene Netzwerk im Systray beim Bewegen des Mauszeigers über das Netzwerksymbol angezeigt.

5.5.6. G3/UMTS-Verbindung

Option	Beschreibung
Name	Name für die Netzwerkverbindung
APN	Access Point Name, Zugangspunkt des Providers
Timeout	Timeout-Wert in Sekunden, bevor eLux die Verbindung abbricht
Benutzername	der von Ihrem Provider zugewiesene Benutzername
Kennwort	das von Ihrem Provider zugewiesene Kennwort
PIN der SIM-Karte	die von Ihrem Provider zugewiesene PIN Ihrer SIM-Karte
Geschützt	Lokale Benutzer können das Profil nicht ändern.
DNS-Server 1	Nameserver, wenn erforderlich
DNS-Server 2	Nameserver, wenn erforderlich

5.5.7. ADSL-Verbindung

Option	Beschreibung
Name	Name für die Netzwerkverbindung
Timeout	Timeout-Wert in Sekunden, bevor eLux die Verbindung abbricht
Benutzername	der von Ihrem Provider zugewiesene Benutzername
Kennwort	das von Ihrem Provider zugewiesene Kennwort
Identifizierung	das von Ihrem Provider genutzte Protokoll
Geschützt	Lokale Benutzer können das Profil nicht ändern.

Bei ISDN, ADSL oder Modem unterstützt eLux die dynamische Änderung der IP-Adressen.

5.5.8. Modem-Verbindung

Option	Beschreibung
Name	beliebiger Name für die Netzwerkverbindung
Rufnummer	Rufnummer Ihres Providers.
Timeout	Timeout-Wert in Sekunden. Nach der definierten Wartezeit bricht eLux die ADSL-Verbindung ab.
Benutzername	der von Ihrem Provider zugewiesene Benutzername
Kennwort	das von Ihrem Provider zugewiesene Kennwort
Identifizierung	das von Ihrem Provider genutzte Protokoll

Option	Beschreibung
Geschwindigkeit	Baudrate für Ihr Modem. Die Einstellung muss größer als die tatsächlich höchste Baudrate des Modems sein.
Geschützt	Lokale Benutzer können das Profil nicht ändern.

Bei ISDN, ADSL oder Modem unterstützt eLux die dynamische Änderung der IP-Adressen.

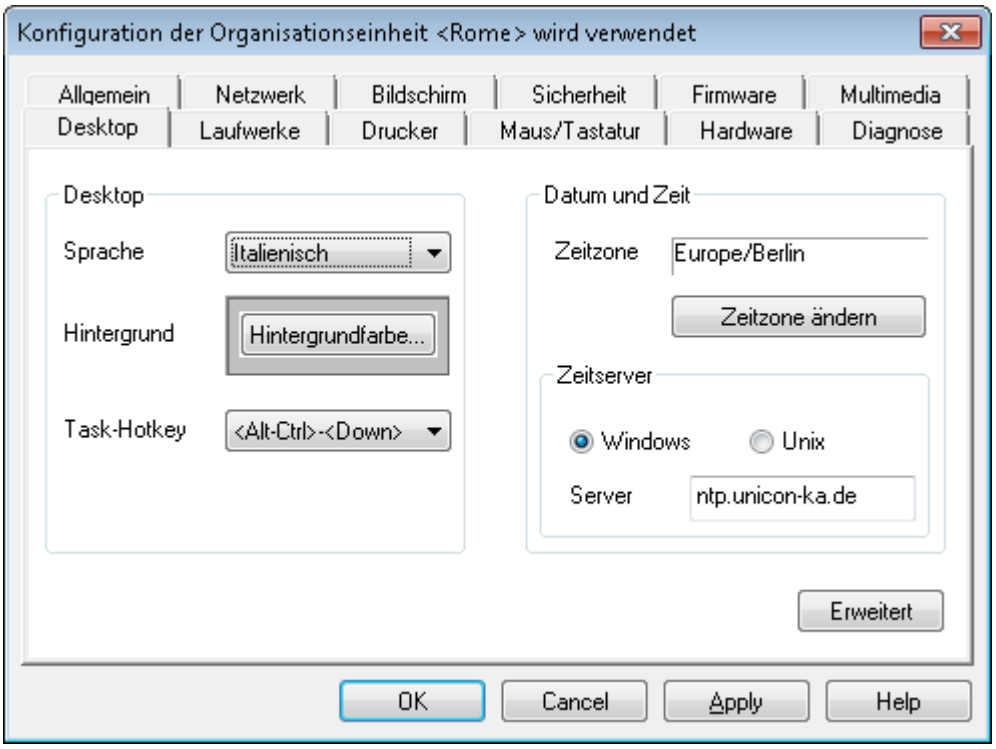
5.5.9. ISDN-Verbindung

Option	Beschreibung
Name	beliebiger Name für die Netzwerkverbindung
Rufnummer	Rufnummer Ihres Providers.
Timeout	Timeout-Wert in Sekunden. Nach der definierten Wartezeit bricht eLux die ADSL-Verbindung ab.
Benutzername	der von Ihrem Provider zugewiesene Benutzername
Kennwort	das von Ihrem Provider zugewiesene Kennwort
MSN	Nummer für Mehrfachanschluss. Wenn Sie die Rückruf-Funktion nutzen, geben Sie Ihre Telefonnummer ohne Vorwahl ein. Wird die Rückruf-Funktion nicht genutzt, geben Sie 0 (Null) ein.
Identifizierung	das von Ihrem Provider genutzte Protokoll
Rückruf	Aktivieren Sie die Option, wenn Ihr Provider die Rückrufoption unterstützt.
IP-Adresse benutzen	nur, wenn Ihr Provider eine statische IP-Adresse für Ihr eLux-Terminal reserviert
Geschützt	Lokale Benutzer können das Profil nicht ändern.

Bei ISDN, ADSL oder Modem unterstützt eLux die dynamische Änderung der IP-Adressen.

5.6. Register Desktop

In **Konfiguration > Desktop** passen Sie die Oberfläche von eLux an und nehmen Einstellungen zu Datum und Uhrzeit vor.



5.6.1. Desktop konfigurieren

1. Öffnen Sie in der Scout Enterprise Konsole für das relevante Gerät oder OU den Dialog **Konfiguration > Desktop**. Am Client wählen Sie in der Systemsteuerung das Register **Setup > Desktop**.
2. Wählen Sie im Listenfeld **Sprache** die Sprache aus, mit der die Anwendungen gestartet und die Bildschirmelemente dargestellt werden sollen.

Hinweis
Die Sprache bezieht sich auf die Anzeige der Bildschirmelemente, nicht jedoch auf Eingabesprache und Textdienste..
Die Anwendungen müssen kompatibel zur eingestellten Sprache sein, damit sie korrekt ausgeführt werden.

Die Elemente der eLux-Oberfläche wie Startmenü und Systemsteuerung werden nur bei Auswahl der Sprache `Deutsch` *auf Deutsch angezeigt, bei allen anderen Sprachen werden sie auf Englisch angezeigt.*

3. Klicken Sie auf die Schaltfläche **Hintergrund**, um eine Farbe für den Hintergrund auszuwählen.

Hinweis
Die Hintergrundfarbe wird nur dann aktiv, wenn die Option **Klassischer Desktop** eingeschaltet ist, siehe Erweiterte Desktop-Einstellungen.

4. Wählen Sie im Listenfeld **Task-Hotkey** die Tastenkombination, die Sie zum Wechseln zwischen den Anwendungen verwenden möchten.

   Um keinen Konflikt mit der Standard-Tastenkombination `ALT+TAB` für den Task-Wechsel innerhalb eines Windows Desktops zu produzieren, ist standardmäßig `ALT+STRG+↑` konfiguriert.

5.6.2. Zeitzone und Zeitserver einstellen

- Um die Zeitzone einzustellen, wählen Sie **Konfiguration > Desktop** und wählen unter **Datum und Zeit** die entsprechende Zeitzone.
- Um einen Zeitserver anzugeben, wählen Sie **Konfiguration > Desktop** und tragen unter **Datum und Zeit** und **Zeitserver** den entsprechenden Servernamen oder die IP-Adresse ein.

Für weitere Informationen zur Synchronisierung mit einem Zeitserver siehe Zeitserver im eLux-Handbuch.

5.6.3. Erweiterte Desktop-Einstellungen

Im Register **Desktop > Erweitert** finden Sie weitere Optionen zur Konfiguration des Desktops:

Option	Beschreibung
Interaktiver Desktop	Icons, die auf dem Desktop angezeigt werden
Desktop schreibbar	Anwender dürfen Icons auf dem Desktop hinzufügen.
Klassischer Desktop	Das Modern User Interface wird deaktiviert. Eine auf dem **Desktop**-Register definierte **Hintergrundfarbe** wird angezeigt.
Windowmanager	Wenn die Option **Animierte Fenster** aktiv ist, wird der Fensterinhalt während des Verschiebens von Fenstern angezeigt. Wenn die Option **Maximieren/Vollbild auf einzelnen Monitor** aktiv ist, können Sie bei mehreren angeschlossenen Monitoren jeder Anwendung (ICA und RDP) einen Monitor zuordnen..
Taskleiste	Konfigurationseinstellungen der Taskleiste am unteren Bildschirmrand.

Option	Beschreibung
Schnell-Setup (Systray)	Systray-Icons, die in der Taskleiste angezeigt werden: **Multimedia**: Auswahl der Ein-/Ausgabegeräte, Lautstärkenregelung, Testklang **Maus/Tastatur**: Maus-/Tastaturgeschwindigkeit, Linkshänder-Maus, Tastatursprache **Bildschirm**: Information, Auflösung, Anordnung **USB-Massenspeichergeräte**: USB-Geräteinfo **Netzwerkstatus anzeigen**: LAN/WLAN, Netzwerkinfo, Trennen/Verbinden, Konfiguration **Geräteinformation**: MAC, IP, Name, Seriennummer, freie Infofelder **Datum/Zeit**: Anzeige/Einstellung von Datum, Zeit und Zeitzone
Hintergrundbild (nur Scout Enterprise)	Zwei Methoden zur Definition von Hintergrundbildern stehen zur Verfügung: • Geben Sie im Textfeld **Serverdatei** den Dateinamen der Bilddatei inklusive Pfad relativ zum Scout Enterprise Server-Verzeichnis (`\UniCon\Scout\Server`) ein. • Wählen Sie die Datei über die Schaltfläche **Laden** aus dem Dateisystem. Die Datei wird in die Scout Enterprise-Datenbank importiert. Diese Variante hat Priorität vor einer im Feld **Serverdatei** angegebenen Bilddatei. Mit der Schaltfläche **Löschen** löschen Sie das Hintergrundbild wieder aus der Datenbank. In die Datenbank importierte Dateien werden automatisch beim SQL-Datenbank-Backup mitgesichert. Für im Dateisystem referenzierte Dateien besteht die Möglichkeit, den Inhalt der Dateien unter Beibehaltung des Namens dynamisch zu ändern. Das Hintergrundbild wird nicht bei jedem Bootvorgang des Clients übertragen, sondern nur, wenn sich an der Konfiguration der Dateien oder den Dateien selbst etwas ändert. eLux NG unterstützt weder Desktop-Wallpapers noch gestapelte Bilder.
	Hinweis Stellen Sie sicher, dass auf dem Flash-Speicher des Thin Client genügend Speicherplatz vorhanden ist. Das Hintergrundbild wird im `\setup`-Verzeichnis auf dem Flash-Speicher gespeichert.
Autostart	Die Systemsteuerung wird beim Systemstart nach der angegebenen Verzögerung in Sekunden aufgerufen.
Arbeitsflächen	Anzahl der Desktops

5.6.4. eLux Modern User Interface

Das Modern User Interface ist eine Alternative zum klassischen Desktop und stellt dem Benutzer Ressourcen aus Citrix StoreFront-Stores und dem Citrix Webinterface zur Verfügung, aber auch beliebige andere für den Client konfigurierte Anwendungen.

Modern User Interface aktivieren

Voraussetzung
Die Clients müssen über eLux RP Version 4.8.0 oder höher verfügen und der ICA client V13.1.3 oder höher muss installiert sein.

- Deaktivieren Sie in der Gerätekonfiguration in **Desktop > Erweitert** die Option **Klassischer Desktop**.

Das Layout des Modern User Interface können Sie auf Ihre Bedürfnisse anpassen. Beispielsweise können Sie die Größe der Anwendungssymbole verändern oder ein eigenes Logo einblenden.

Layout des Modern User Interface anpassen

1. Verwenden Sie für die relevanten Geräte die Scout Enterprise-Funktion **Erweiterte Dateieinträge**, um die Client-Datei `/setup/terminal.ini` anzupassen:

Datei	`/setup/terminal.ini`
Abschnitt	`Layout`
Eintrag und Wert	siehe Tabelle unten

2. Fügen Sie folgende neue Einträge hinzu und geben Sie die gewünschten Werte an:

Eintrag	Wertebereich	Default	Beschreibung
DesktopLayout	small, medium, large	medium	Größe der Anwendungssymbole auf dem Desktop
DesktopLogo	*Name und Pfad der Grafikdatei*	*eLux-Logo*	Ersetzt das eLux-Logo in der oberen linken Ecke durch die angegebene Grafikdatei. Beispiel: `setup/-public/myPic.png`

Hinweis
Die Grafikdatei muss für die Dateiübertragung konfiguriert sein. Für weitere Informationen, siehe Erweiterte Konfiguration > Dateien.

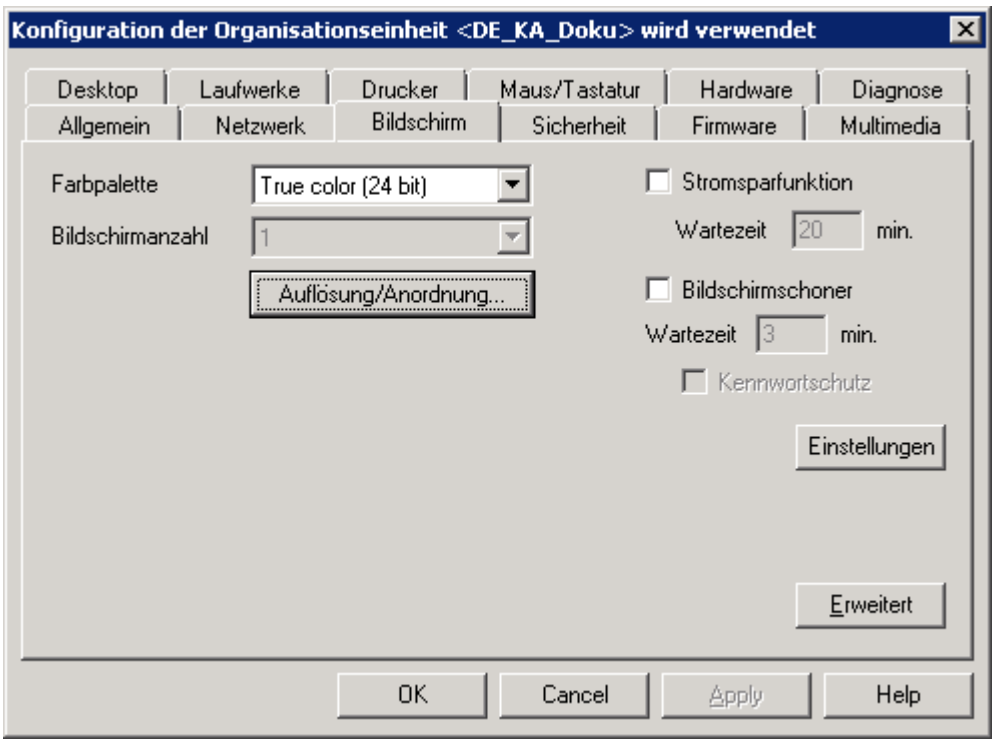
Eintrag	Wertebereich	Default	Beschreibung
DesktopTextColor	#<*rgb*>	#ffffff	Textfarbe für Anwendungssymbole
DesktopBackgroundColorMenu	#<*rgb*>	#000000	Hintergrundfarbe der Menüs

Bestätigen Sie jeden Eintrag mit **Hinzufügen**.

3. Um ein Hintergrundbild im Modern User Interface anzuzeigen, konfigurieren Sie die relevante Grafikdatei in der Gerätekonfiguration. Für weitere Informationen siehe Erweiterte Desktop-Einstellungen.

Für weitere Informationen zum Modern User Interface siehe Oberfläche im eLux-Handbuch.

5.7. Register Bildschirm



5.7.1. Bildschirmeinstellungen und Multimonitorbetrieb

In **Konfiguration > Bildschirm** können Sie im Feld **Farbpalette** die Farbtiefe festlegen, sowie Stromsparfunktion und Bildschirmschoner definieren.

Weitere Grundeinstellungen wie Bildschirmauflösung, Frequenz und Rotation legen Sie im Dialog **Auflösung/Anordnung** fest. In diesem Dialog können Sie außerdem bis zu acht Monitore (ab Scout Enterprise Management Suite Version 14.9[1]) anordnen und konfigurieren.

Hinweis
Eine hohe Auflösung und eine große Farbtiefe benötigen mehr Grafik- und Arbeitsspeicher. Das kann dazu führen, dass die mögliche Anzahl parallel geöffneter Anwendungen eingeschränkt ist.

Bei Verwendung von Adaptern sowie bei Nutzung des analogen VGA-Ports für den Anschluss von Monitoren an den Thin Client besteht keine Gewährleistung für den Betrieb der Thin Clients, da diese Konstellationen kein Bestandteil funktionaler Abnahmetests sind.

Multimonitorbetrieb einrichten

1. Klicken Sie auf die Schaltfläche **Auflösung/Anordnung...**, um den gleichnamigen Dialog zu öffnen.

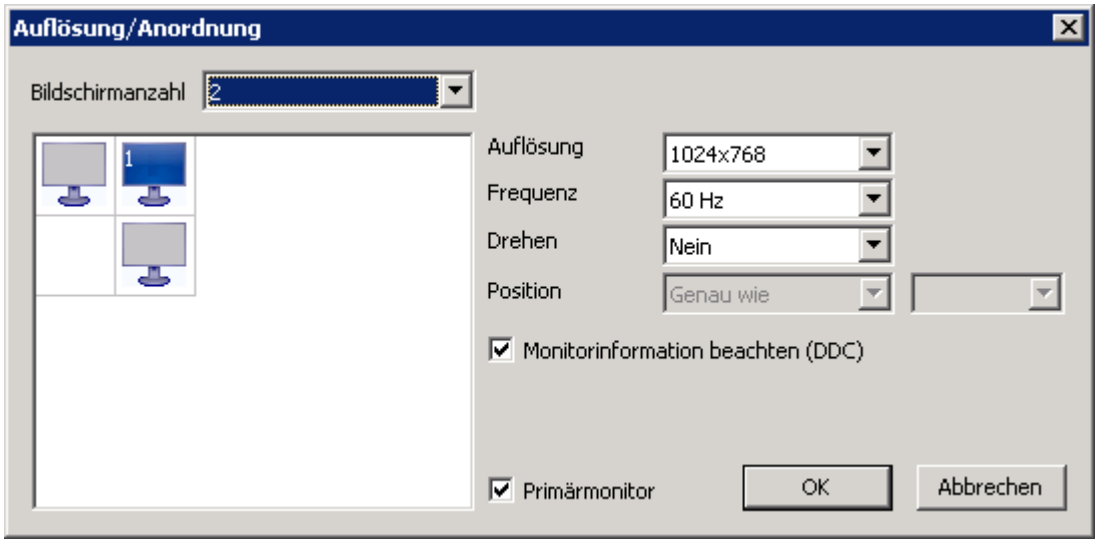
[1] bis Scout Enterprise Management Suite Version 14.8 können maximal vier Monitore konfiguriert werden

Im Feld Bildschirmanzahl ist standardmäßig 1 Monitor angegeben. Dieser Monitor wird im Feld unterhalb als blaues Monitor-Symbol mit einer 1 dargestellt. Standardmäßig ist der erste Monitor als Primärmonitor definiert (siehe Option im unteren Bereich).

Wenn Sie den ersten Monitor frei positionieren möchten, beachten Sie die Schrittanleitung unten.

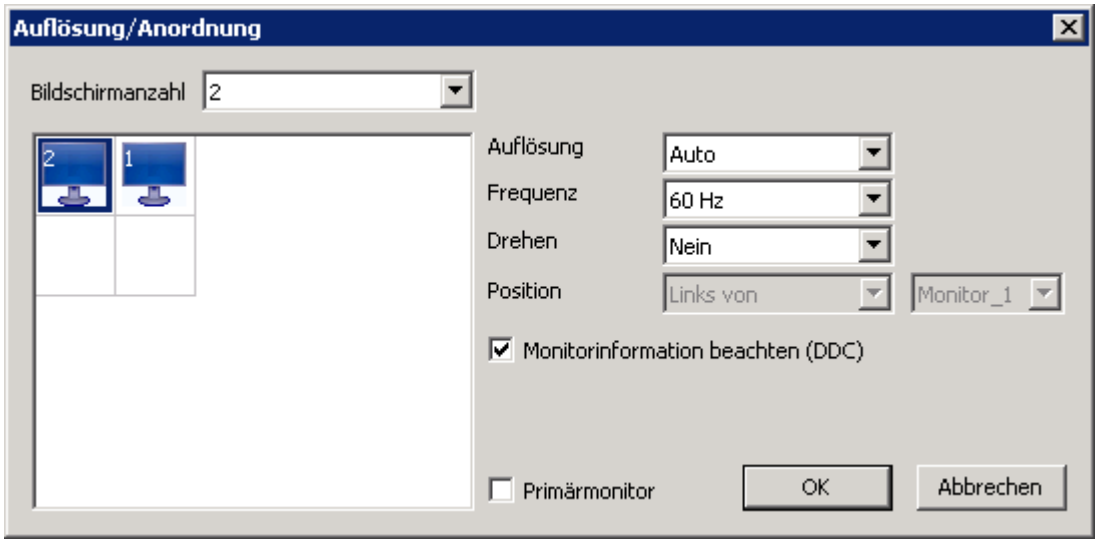
2. Wählen Sie im Feld **Bildschirmanzahl**, wie viele Monitore an den Thin Client angeschlossen sind.

   Für jeden zusätzlichen Monitor werden die möglichen Positionen (horizontal und vertikal) als graue Monitor-Symbole angezeigt.



3. Doppelklicken Sie auf das graue Monitorsymbol, das die Position Ihres zweiten Monitors bezeichnet.

   Das gewählte Monitor-Symbol wird blau dargestellt und mit einer 2 gekennzeichnet.



4. Wenn Sie mehr als zwei Monitore angegeben haben, doppelklicken Sie nacheinander auf die gewünschten grauen Monitor-Symbole.

   Jeder definierte Monitor wird als blaues Monitor-Symbol dargestellt und mit seiner Zahl gekennzeichnet.

Hinweis

Eine Vier-Bildschirm-Konfiguration wird von folgenden Geräten unterstützt: Dell Z50QQ, Hewlett-Packard t620 Plus und Hewlett-Packard t730.

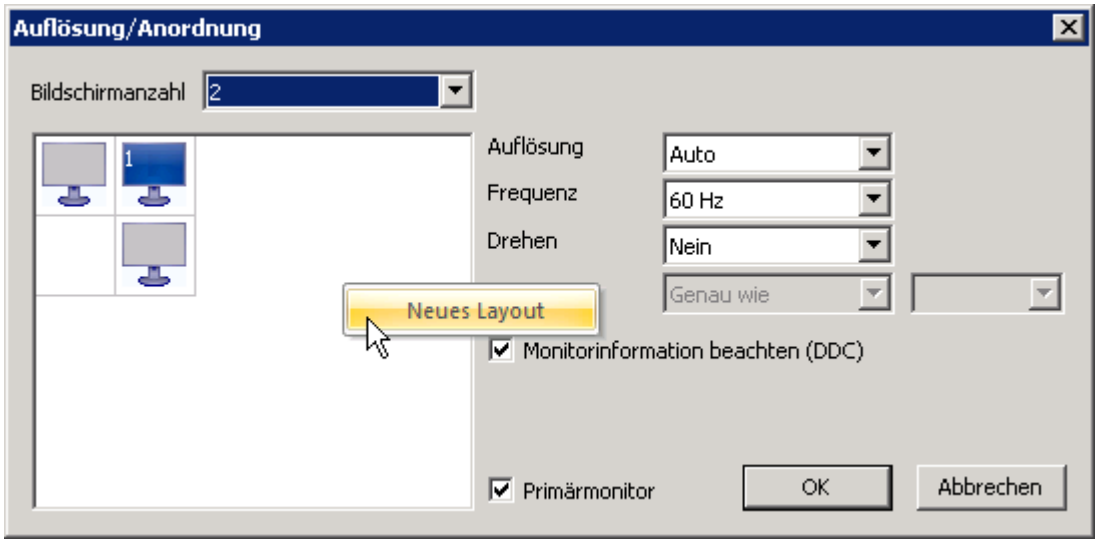
Anordnung aller Monitore frei definieren

Wenn Sie die Position des ersten Monitors selbst definieren möchten, verwenden Sie ein neues Layout.

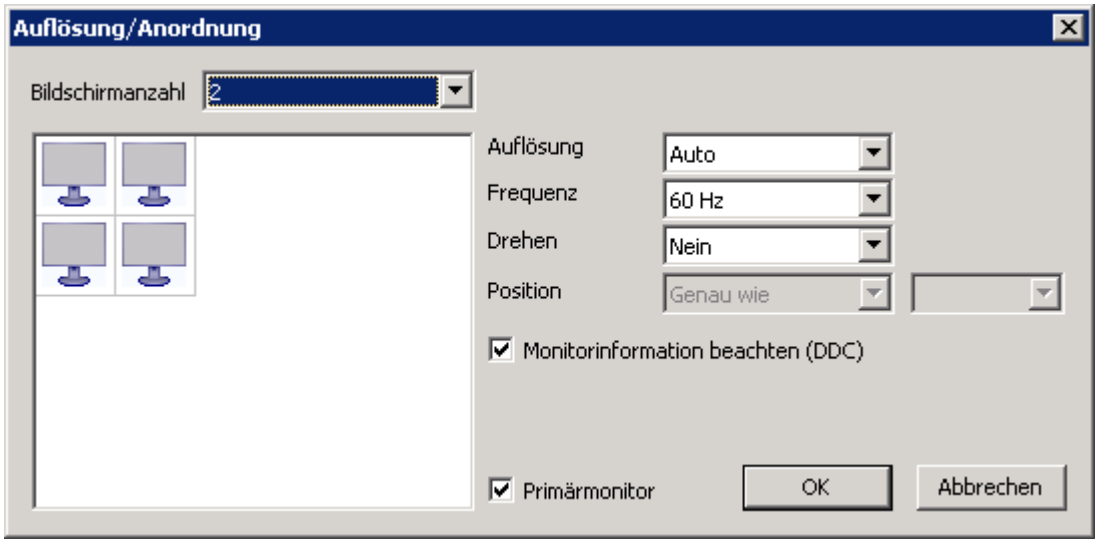
1. Wählen Sie im Dialog **Auflösung/Anordnung**, im Feld **Bildschirmanzahl**, wie viele Monitore an den Thin Client angeschlossen sind.

   Der erste Monitor wird blau dargestellt. Für jeden zusätzlichen Monitor werden die möglichen Positionen (horizontal und vertikal) als graue Monitor-Symbole angezeigt.

2. Klicken Sie mit der rechten Maustaste in den weißen Bereich neben den Monitor-Symbolen und wählen Sie im Kontextmenü **Neues Layout**.



Für die gewählte Bildschirmanzahl werden alle möglichen Monitor-Positionen als graue Monitor-Symbole angezeigt:



3. Doppelklicken Sie auf die relevante Monitor-Position für den ersten Monitor. Doppelklicken Sie anschließend auf die relevanten Monitor-Positionen für die weiteren Monitore.

Erweiterten Desktop oder Mehrschirmbetrieb konfigurieren

Wenn mehr als ein Monitor angegeben sind, konfiguriert das System die Monitore standardmäßig zur Nutzung eines erweiterten Desktops (zusammenhängende Arbeitsoberfläche über alle Monitore). Alternativ können Sie für einzelne Monitore den Mehrschirmbetrieb oder Klon-Modus (gleiche Anzeige auf mehreren Monitoren) aktivieren:

- Klicken Sie mit der rechten Maustaste auf ein blaues Monitor-Symbol und wählen Sie im Kontextmenü **Genau wie** *x*.

Die Einstellung für den Mehrschirmbetrieb können Sie über die Funktion **Neues Layout** (siehe oben) wieder aufheben.

Bildschirmeinstellungen setzen

1. Markieren Sie ein blaues Monitor-Symbol.
2. Legen Sie für den markierten Monitor Auflösung, Frequenz, und Rotation mit Hilfe der Listenfelder rechts fest.

Hinweis

Um Bildschirmauflösungen zu nutzen, die nicht in der Auswahlliste angeboten werden, können Sie die gewünschte Auflösung manuell in die Scout Enterprise-Datenbank in die Tabelle `dbo.Resolution` eintragen. Nach dem Ändern der Tabelle ist ein Neustart der Scout Enterprise-Konsole erforderlich.

3. Wenn Sie möchten, dass der Client die vom Monitor unterstützten Werte abruft und berücksichtigt, aktivieren Sie für den markierten Monitor die Option **Monitorinformation beachten (DDC)**. Wenn Sie die Option deaktivieren, wird das Feld **Anschlusstyp** aktiv.
4. Um den markierten Monitor zum Primärmonitor zu machen, aktivieren Sie die Option **Primärmonitor**.
5. Bestätigen Sie mit **OK** und **Übernehmen**.

Achtung

Wenn Ihre Monitore die gewählten Einstellungen nicht unterstützen, kann es erforderlich sein, den Client in den Grundzustand zu versetzen und die Konfiguration anschließend zu wiederholen.

5.7.2. Bildschirmschoner einstellen

1. Aktivieren Sie im Register **Bildschirm** die Option **Bildschirmschoner**.
2. Geben Sie im Feld **Wartezeit** die Wartezeit in Minuten an, bevor sich der Bildschirmschoner einschalten soll.
3. (Nur Scout Enterprise:) Um zum Entsperren des Bildschirms das Kennwort anzufordern, aktivieren Sie die Option **Kennwortschutz**.

   Dazu muss die Benutzerauthentifizierung eingeschaltet sein. Das Kennwort für den Bildschirmschoner ist mit dem Wert aus `$ELUXPASSWORD` vorbelegt. Für weitere Informationen siehe Anwendungsmöglichkeiten für Benutzervariablen.
4. Klicken Sie auf **Einstellungen**, um den Bildschirmschoner auszuwählen und zu konfigurieren.
5. Bestätigen Sie mit **OK** und **Übernehmen**.

5.7.3. Fontserver konfigurieren

Ein Fontserver dient zur zentralen Verwaltung von Schriften. Die Schriften werden auf einem Server abgelegt und können von einem Client bei Bedarf angefordert werden.

1. Klicken Sie im Dialog **Konfiguration > Bildschirm** auf die Schaltfläche **Erweitert**.
2. Klicken Sie im Dialog **Erweiterte Bildschirmeinstellungen** auf **Neu**, **Bearbeiten** oder **Löschen**, um einen Font-Server zu erstellen, zu bearbeiten oder zu löschen.
3. Wenn Sie einen Font-Server erstellen, tragen Sie im Dialog **FontServer definieren** im Feld **FontServer:Port** die IP-Adresse oder den Namen des Font-Servers sowie dessen Portnummer ein, getrennt durch einen Doppelpunkt. Verwenden Sie folgendes Format:
   `<Fontserver-Name/IP-Adresse>:<Portnummer>`
   Beispiel: `192.168.10.23:7100`
   Oder: Tragen Sie im Feld **Font-Pfad** den Pfad ein, in dem die Fonts installiert sind.
   Beispiel: `/smb/g/fonts`

4. Bestätigen Sie mit **OK** und **Übernehmen**.

5.7.4. Backingstore

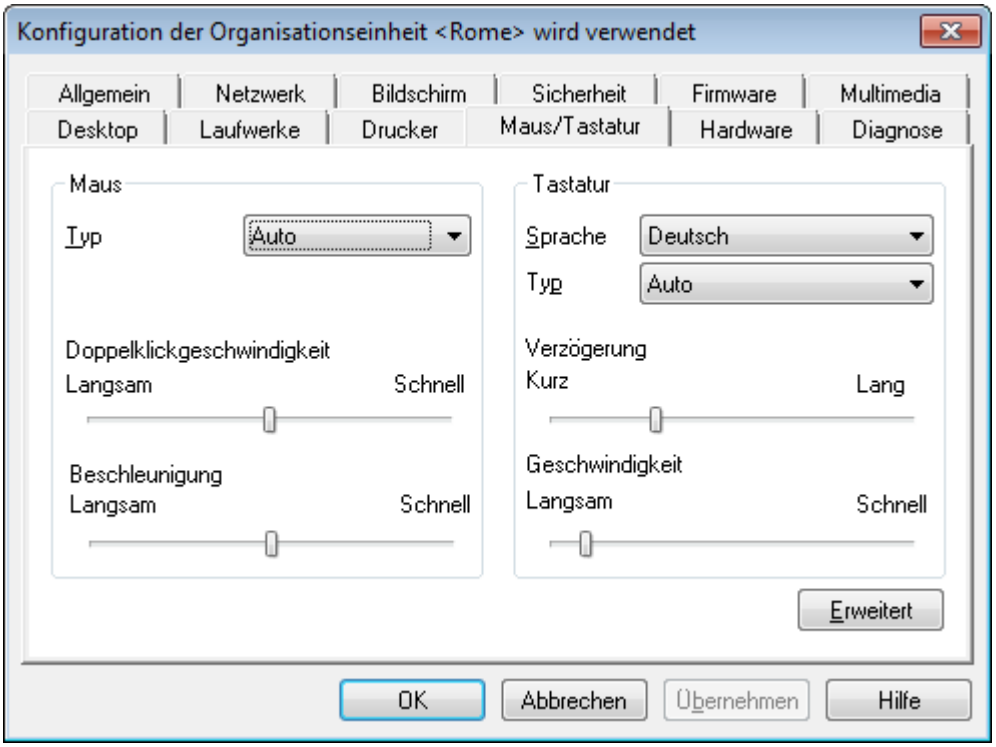
Backingstore speichert Bildschirminformationen auf dem lokalen X11 Server des Thin Clients. Es wird das Bild (engl. pixmap) jedes Fensters im X-Server hinterlegt, egal ob es sichtbar ist oder nicht. Sinn der Funktion ist es, beim Fokussieren eines verdeckten Fensters die gespeicherten Bildinformationen des X-Serves zum Bildschirmaufbau zu verwenden. Da das Fensterbild nicht von der Anwendung neu übertragen werden muss, wird der Bildschirm schneller aufgebaut.

Diese Funktion ist bei langsamen Netzwerkverbindungen wie ISDN sehr sinnvoll. Die einzelnen Pixmaps werden im Arbeitsspeicher hinterlegt, d.h. der X-Server benötigt mehr Speicherplatz. Es sollten mindestens 128 MB Arbeitsspeicher zur Verfügung stehen.

Backingstore einschalten

1. Wählen Sie **Bildschirm > Erweitert**.
2. Aktivieren Sie die Option **Backingstore**.

5.8. Register Maus/Tastatur



5.8.1. Maus konfigurieren

1. Wählen Sie im Register **Maus/Tastatur** unter **Maus** den Typ der verwendeten Maus oder `Auto`.

   Normalerweise wird der Maustyp automatisch erkannt.

2. Schieben Sie unter **Doppelklick-Geschwindigkeit** den Schieberegler nach rechts, um die Geschwindigkeit zu erhöhen.

   Die Doppelklick-Geschwindigkeit definiert den Zeitintervall zwischen zwei Klicks, die als Doppelklick gewertet werden sollen.

3. Schieben Sie unter **Beschleunigung** den Schieberegler nach rechts, um die Beschleunigung des Mauszeigers zu erhöhen.

   Je schneller der Mauszeiger ist, desto geschmeidiger sind die Bewegungen.

5.8.2. Tastatur konfigurieren

1. Wählen Sie im Register **Maus/Tastatur** unter **Tastatur** im Listenfeld **Sprache** die relevante Tastaturbelegung.
2. Im Feld **Typ** belassen Sie den Eintrag auf `Auto`.

   Die Tastatur wird automatisch vom Client erkannt.

3. Schieben Sie unter **Verzögerung** den Schieberegler nach rechts, um die Verzögerung zu erhöhen.

   Die Verzögerung steuert, wie lang eine Taste gedrückt gehalten werden muss, bis ein Zeichen wiederholt wird.

4. Schieben Sie unter **Geschwindigkeit** den Schieberegler nach rechts, um die Geschwindigkeit zu erhöhen.

   Die Geschwindigkeit steuert, wie schnell ein Zeichen wiederholt wird, wenn eine Taste gedrückt gehalten wird.

5.8.3. Erweiterte Maus- und Tastaturkonfiguration

1. Klicken Sie auf dem Register **Maus/Tastatur** auf die Schaltfläche **Erweitert**.
2. Bearbeiten Sie folgende Felder:

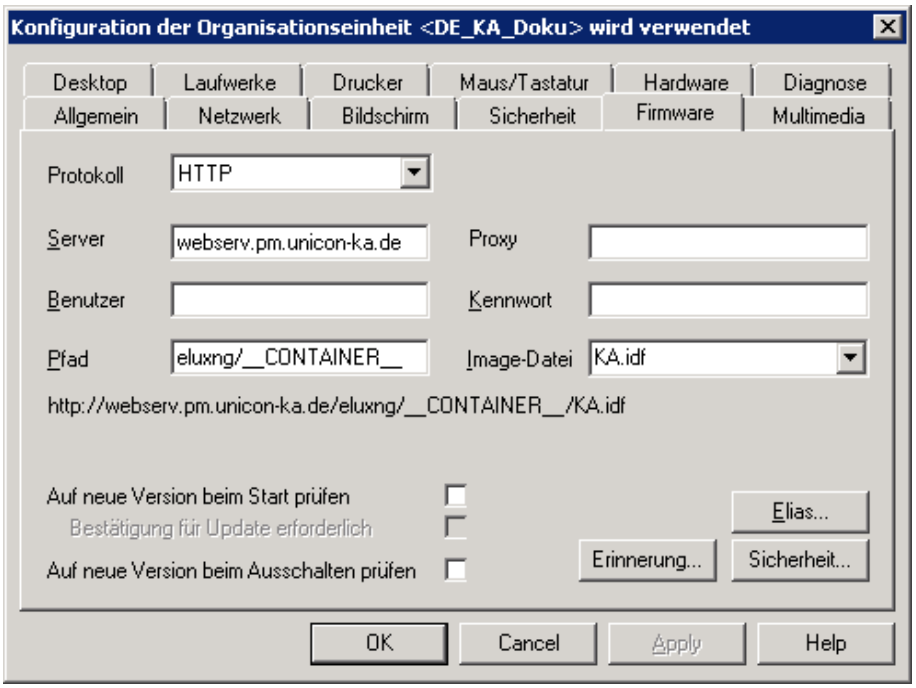
Option	Beschreibung
3-Tasten-Maus-Emulation	Schaltet die Simulation der dritten Maustaste für eine 2-Tasten-Maus ein: Gleichzeitiges Drücken von linker und rechter Maustaste.
Linkshändig	Vertauscht die Funktion der Maustasten.
Tottasten	Sogenannte Deadkey-Tasten lösen erst in Kombination mit einer zweiten Taste die Anzeige eines bestimmten Zeichens aus. Beispielsweise funktionieren Akzenttasten als Tottasten und ermöglichen so die korrekte Eingabe von Buchstaben mit Akzenten (`+ A => à). Standardmäßig ist die Option aktiv. Deaktivieren Sie die Option, wenn eine Anwendung keine Tottasten unterstützt. Einige Hardwareplattformen bieten diese Option nicht an.
Numlock	Schaltet den Nummernblock der Client-Tastatur beim Gerätestart ein und ermöglicht das Eingeben von Zahlen über den Nummernblock.
Konsolenumschaltung aktiv	Der Benutzer kann per Tastenkombinationen zwischen den Konsolen des Thin Client umschalten. Wenn die Option nicht aktiv ist, wird immer die Konsole 1 (eLux Desktop) angezeigt. Für weitere Informationen siehe Tastenkombinationen.
Multimedia-/Zusatztasten	Aktiviert Mulitimedia- und andere Tasten mit Sonderfunktionen auf der Tastatur.

3. Bestätigen Sie mit **OK**.

Die Änderungen werden beim nächsten Systemstart aktiv.

5.9. Register Firmware

Im Register **Firmware** passen Sie Einstellungen zum Firmware-Update (Software-Update) der Clients über das Netzwerk an.



Die Imagedefinitionsdatei (engl: image definition file, kurz: IDF) definiert die auf dem Thin Client zu installierende Software. Das Register **Firmware** enthält alle erforderlichen Informationen zum Zugriff auf das relevante IDF.

Das IDF wird mit dem Programm ELIAS erstellt und auf einem Webserver oder FTP-Server zur Verfügung gestellt.

5.9.1. Voraussetzungen

- Webserver (zum Beispiel IIS), der die eLux Software-Pakete und Image Definition Files via HTTP oder FTP zur Verfügung stellt
- Software-Container mit eLux-Software-Paketen auf dem Webserver (Bestandteil der Installation des Bundles eLux[version]_AllPackages.zip von www.myelux.com)
- Das Tool ELIAS (eLux Image Administration Service) zur Erstellung und Änderung von Image Definition Files im Software-Container auf dem Webserver (Bestandteil der Scout Enterprise-Installation)
- Scout Enterprise-Konsole zur Konfiguration des Firmware-Updates für die Clients (Bestandteil der Scout Enterprise-Installation)

5.9.2. Firmware-Update konfigurieren

1. Öffnen Sie in der Scout Enterprise Konsole für das relevante Gerät oder OU den Dialog **Konfiguration > Firmware**. Am Client wählen Sie in der Systemsteuerung das Register **Setup > Firmware**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Protokoll	Netzwerk-Protokoll des Webservers zur Übertragung der Software-Pakete an die Clients (HTTP, HTTPS, FTP, FTPS)
Server	Name (FQDN) oder IP-Adresse des Webservers, der die eLux-Software-Pakete und Image Definition Files zur Verfügung stellt
Proxy (optional)	IP-Adresse und Port (fix 3128) des Proxy-Servers Format: `IP-Adresse:Port` Beispiel: `192.168.10.100:3128`
Benutzer und Kennwort (optional)	Benutzername und Kennwort für den Zugriff auf den eLux-Software-Container des FTP-Servers, wenn erforderlich
Pfad	Verzeichnispfad der eLux Software-Pakete auf dem Web/FTP-Server Verwenden Sie Slashes `/` als Trennzeichen zwischen den Verzeichnissen. Beispiel: `eluxng/UC_RP5` entspricht dem IIS-Webserver-Verzeichnis `C:\inetpub\wwwroot\eluxng\UC_RP5\` Wenn mehrere eLux-Versionen eingesetzt werden, kann das Container-Verzeichnis durch das Container-Makro parametrisiert werden.
Image-Datei	Name des Image Definition Files (IDF) auf dem Webserver, das die Clients für das Firmware-Update verwenden sollen. Der Name darf keine Leerzeichen enthalten, Groß-/Kleinschreibung ist zu berücksichtigen und die Dateiendung `.idf` muss angegeben werden. Beispiel: `myImage.idf` Wenn unterschiedliche BIOS-Implementierungen eingesetzt werden (UEFI und non-UEFI), kann im IDF-Namen das BIOS-Makro verwendet werden.
	Hinweis Aus den Feldern **Protokoll**, **Server**, **Pfad** und **Image-Datei** wird eine URL-Adresse erzeugt, die von den Clients beim Firmware-Update verwendet wird, um die Übertragung von Image Definition File und eLux-Software-Paketen zu initiieren. Die URL-Adresse wird unterhalb des **Pfad**-Feldes angezeigt.

Option	Beschreibung
Auf neue Version beim Start / Ausschalten prüfen	Der Thin Client prüft automatisch beim Ein- oder Ausschalten, ob Firmware-Updates verfügbar sind. Zusätzlich kann die Funktion **Bestätigung für Update erforderlich** aktiviert werden, damit der Anwender das Update bei Bedarf verhindern kann.
Schaltfläche **ELIAS...**	Das Tool ELIAS wird gestartet und öffnet das im Feld **Image-Datei** angegebene Image Definition File.
Schaltfläche **Sicherheit...**	In den **Sicherheitseinstellungen** können Sie die Signaturprüfung vor Update durch den Client konfigurieren. Die Signaturprüfung kann für die Image Definition Files und/oder die eLux-Software-Pakete durchgeführt werden.
Schaltfläche **Erinnerung...**	In den **Erinnerungseinstellungen** können Sie festlegen, ob und wie oft ein Anwender ein Firmware-Update verschieben darf und welche Zeitintervalle er für die nächste Erinnerung setzen kann. Für weitere Informationen siehe Verschiebung des Updates durch den Anwender.

3. **Nur für eLux**: Klicken Sie auf die Schaltfläche **Update**, um die Firmware-Parameter zu testen. Für weitere Informationen siehe Firmware-Update einspielen im eLux-Handbuch.

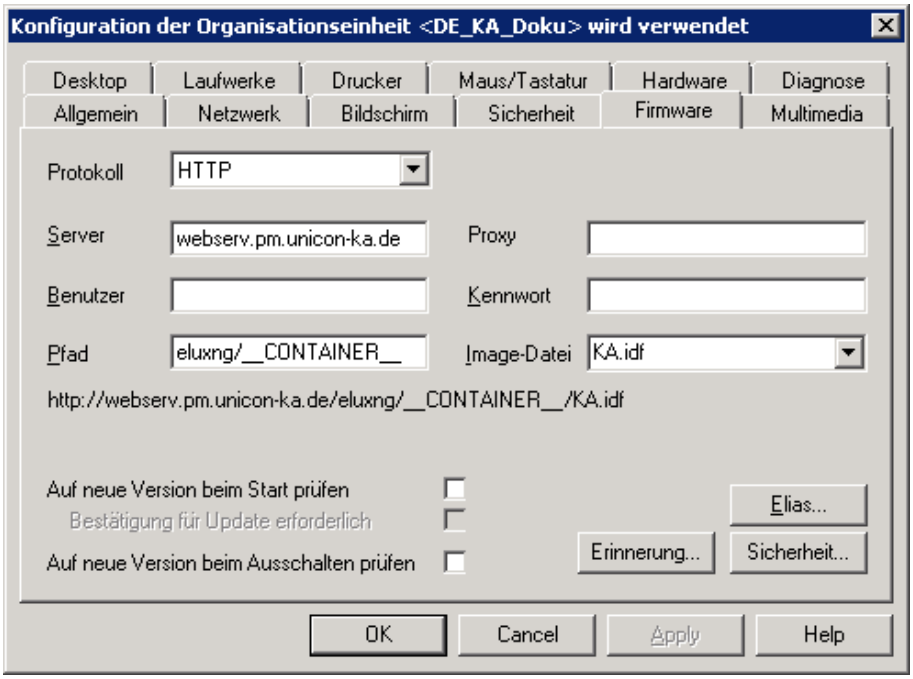
   Wenn die Parameter korrekt sind, wird eine Verbindung zum Scout Enterprise-Server hergestellt, um die Notwendigkeit eines Updates zu prüfen.

Hinweis

Wir empfehlen das Testen der Firmware-Parameter an einem Client (Schritt 3) vor der Firmware-Konfiguration in Scout Enterprise.

5.9.3. Unterschiedliche eLux-Versionen

Standardmäßig wird durch die Installation eines eLux-Containers in einer neu installierten Scout Enterprise-Konsole oder eLux-Systemsteuerung in der Gerätekonfiguration **Firmware > Pfad** folgender Eintrag gesetzt: `__CONTAINER__`.



Die Zeichenfolge `__CONTAINER__` parametrisiert als Teil des Verzeichnispfades den relevanten Software-Container (Verzeichnis) auf Ihrem Web- oder FTP-Server. Das ist hilfreich, wenn Sie unterschiedliche eLux-Versionen verwalten.

Beispiel:

Wenn Sie Geräte mit eLux RP4 und eLux RP5 betreiben, müssen die eLux RP4-Clients auf den `UC_RP`-Container zugreifen und die eLux RP5-Clients auf den `UC_RP5`-Container. Um alle Clients mit der jeweils richtigen Software zu versorgen, verwenden Sie in der Gerätekonfiguration **Firmware > Pfad** aller Clients das Container-Makro `__CONTAINER__`. Das Container-Makro wird von den Clients entsprechend ihrer installierten eLux-Version entweder nach `UC_RP` oder nach `UC_RP5` aufgelöst. Damit kann für beide Plattformen ein gleichnamiges Image Definition File verwendet werden, welches zuvor über ELIAS für eLux RP4 und für eLux RP5 definiert wurde.

Hinweis
In manchen Fällen ist es sinnvoll, den Container-Makronamen durch einen festen Containernamen zu ersetzen. In diesem Fall muss der Eintrag im Feld **Pfad** dem tatsächlichen Containernamen auf dem Webserver entsprechen.

Schreibweise des Container-Makronamens

Wenn Sie umgekehrt einen festen Containernamen durch den Container-Makronamen ersetzen möchten, achten Sie auf die korrekte Schreibweise:

Zwei Unterstriche gefolgt von dem Wort `CONTAINER` (in Großbuchstaben) gefolgt von zwei Unterstrichen.

Hinweis

Das Container-Makro können Sie sowohl in der Geräte-Konfiguration als auch in den Recovery-Einstellungen (**Optionen > Recovery-Einstellungen**) verwenden.

5.9.4. Unterschiedliche BIOS-Implementierungen (UEFI)

Hinweis
eLux RP 5.3 und neuere Versionen unterstützen Geräte mit UEFI (Unified Extensible Firmware Interface).

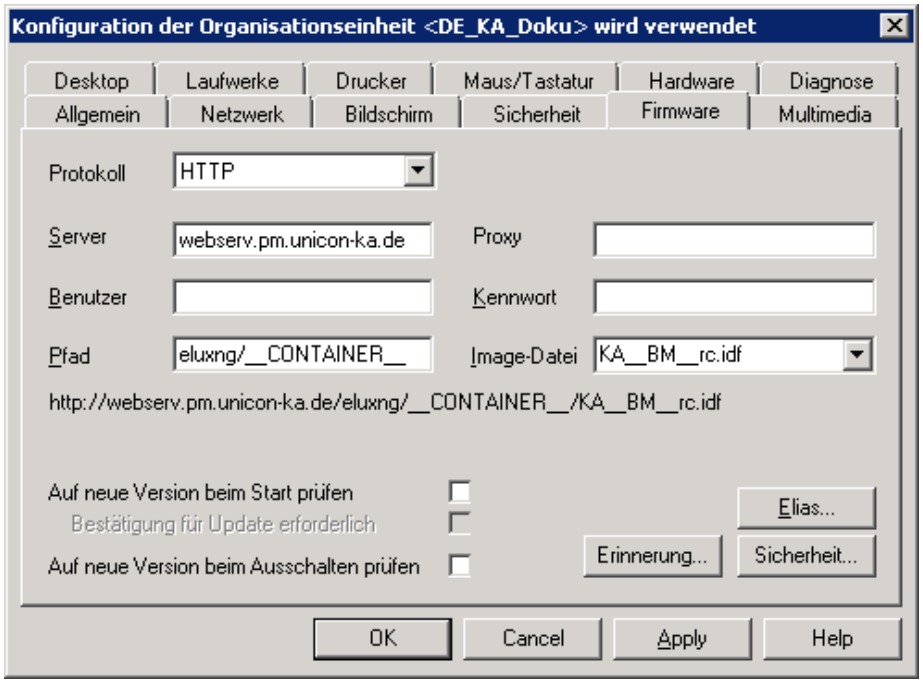
Für diese Geräte muss die Image-Datei das eLux-Paket des 64-Bit-Kernels mit integriertem UEFI-Support enthalten (beispielsweise `kernel-4.4.x-1.UC_RP5-1.0.zip`).

Damit Geräte mit unterschiedlichen BIOS-Implementierungen über eine gemeinsame Firmware-Konfiguration aktualisiert werden können, steht das BIOS-Makro `__BM__` (BIOS-Modus) zur Verfügung. Das Makro wird in den Dateinamen der Image-Datei in der Firmware-Konfiguration eingetragen. Vor dem Ausführen eines Updates löst der Client das Makro entsprechend seiner BIOS-Implementierung auf (Gerät mit UEFI | Gerät ohne UEFI).

Firmware-Update mit BIOS-Makro für gemischte Umgebungen konfigurieren

1. Erstellen Sie in ELIAS eine IDF-Datei für die UEFI-Geräte. Das IDF muss das Paket für den 64-Bit-Kernel enthalten. Der IDF-Dateiname muss die Zeichenfolge `EFI` an einer beliebigen Position enthalten.
   Beispiel: `KAEFIrc.idf`
2. Erstellen Sie in ELIAS eine zweite IDF-Datei für die Geräte ohne UEFI. Der IDF-Dateiname muss demjenigen für UEFI-Geräte entsprechen, darf jedoch die Zeichenfolge `EFI` nicht enthalten.
   Beispiel: `KArc.id`

   Hinweis
   Die Image-Dateien für UEFI-Geräte und Non-UEFI-Geräte dürfen sich in unterschiedlichen Containern befinden, wenn unterschiedliche eLux-Versionen eingesetzt werden. Das Container-Makro in der Firmware-Konfiguration sorgt dafür, dass nach dem relevanten Container aufgelöst wird.
3. Öffnen Sie in der Scout Enterprise-Konsole für die relevante OU den Dialog **Konfiguration > Firmware**.
4. Geben Sie im Feld **Image-Datei** den Dateinamen Ihrer IDF-Datei ein. Statt der Zeichenfolge `EFI` fügen Sie an derselben Position innerhalb des Dateinamens die Zeichenfolge `__BM__` für das BIOS-Makro ein. Die Dateierweiterung `.idf` und der Rest des Dateinamens müssen erhalten bleiben.



Die in der Abbildung angegebene Image-Datei setzt das Vorhandensein der IDF-Datei `KArc.idf` für Geräte ohne UEFI und `KAEFIrc.idf` für UEFI-Geräte voraus.

5. Bearbeiten Sie die weiteren Felder des Registers **Firmware**. Für weitere Informationen siehe Firmware-Update konfigurieren.

Wenn für die relevante OU ein Update-Kommando ausgeführt wird, lösen die Clients der OU das BIOS-Makro entsprechend ihrer BIOS-Implementierung auf (mögliche Werte: `EFI` | <none>). Im Beispiel oben werden folgende URLs erzeugt:

UEFI-Geräte: `http://webserv.pm.unicon-ka.de/eluxng/UC_RP5/KAEFIrc.idf`

Geräte ohne UEFI: `http://webserv.pm.unicon-ka.de/eluxng/UC_RP5/KArc.idf`

Auswirkungen des BIOS-Makro auf Clients mit alter eLux RP-Firmware

Clients mit einem älteren Firmware-Stand als eLux RP V.5.3 können das BIOS-Makro nicht auflösen. Ein Firmware-Update mit der Zeichenfolge `__BM__` im URL schlägt fehl, da die angegebene IDF-Datei im Container `UC_RP` bzw. `UC_RP5` nicht gefunden werden kann.

Abhilfe:

- Speichern Sie die IDF-Datei für ältere eLux RP4 oder eLux RP5-Versionen im Container `UC_RP` oder `UC_RP5` zusätzlich unter einem Dateinamen, der das nicht aufgelöste BIOS-Makro enthält.

Beispiel: `W:\Inetpub\wwwroot\eluxng\UC_RP5\KA__BM__rc.idf`

Schreibweise des BIOS-Makronamens

Achten Sie auf folgende Schreibweise:

Zwei Unterstriche gefolgt von der Zeichenfolge `BM` (in Großbuchstaben) gefolgt von zwei Unterstrichen.

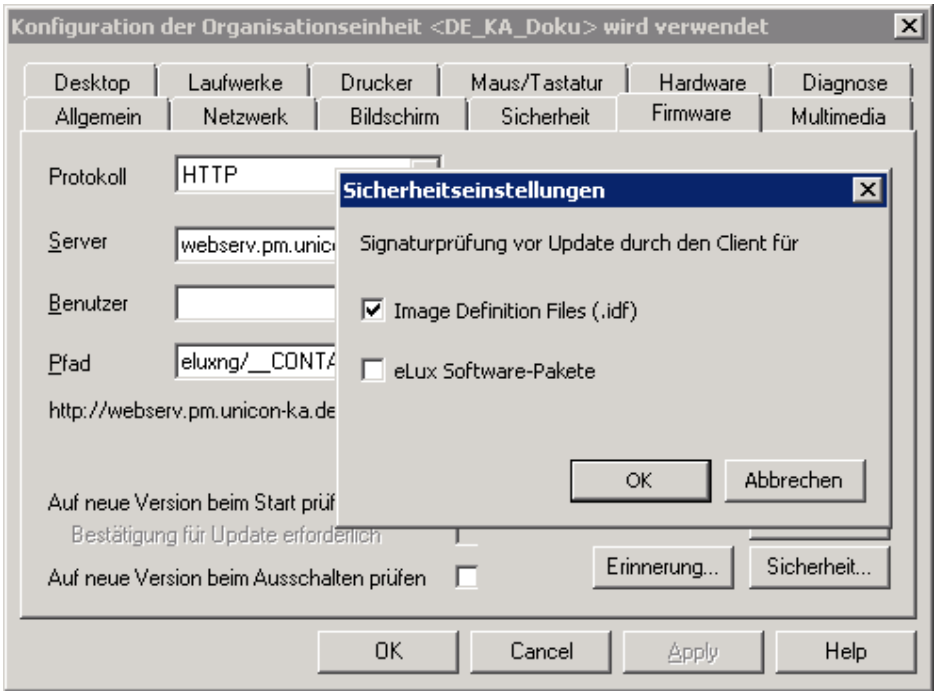
Hinweis

Das BIOS-Makro können Sie sowohl in der Geräte-Konfiguration als auch in den Recovery-Einstellungen (**Optionen > Recovery-Einstellungen**) verwenden.

5.9.5. Firmware-Sicherheit durch Signatur

Scout Enterprise kann so eingestellt werden, dass der Client vor jedem Update die Signaturen für Image Definition File (IDF) und/oder eLux Software-Pakete prüft. In diesem Fall wird das Update nur dann durchgeführt, wenn die Signaturprüfung von IDF und/oder eLux Software-Paketen erfolgreich abgeschlossen werden konnte. Falls das IDF oder eines der zu installierenden eLux Software-Pakete eine ungültige oder nicht prüfbare Signatur besitzt, schlägt das Update fehl.

Signaturprüfung vor Update einschalten



1. Klicken Sie in **Konfiguration > Firmware** auf die Schaltfläche **Sicherheit...**.

   *Der Dialog **Sicherheitseinstellungen** öffnet.*

2. Aktivieren Sie für **Signaturprüfung vor Update durch den Client** die Option **Image Definition File** und/oder die Option **eLux Software-Pakete**.

3. Bestätigen Sie mit **OK**.

> **Hinweis**
> In eLux befinden sich beide Optionen direkt auf dem **Firmware**-Register.

*Das Ergebnis der Signaturprüfung wird in der Update-Logdatei am Client dokumentiert. Die Update-Logdatei wird nach jedem Update-Vorgang zum Scout Enterprise-Server gesendet. Sie kann in der Scout Enterprise-Konsole für ein markiertes Gerät im **Eigenschaften** -Fenster durch Doppelklick auf das Feld **Update-Status** eingesehen werden.*

Für die Prüfung der Signaturen am Client wird neben dem Root-Zertifikat auch das Signatur-Zertifikat lokal am Client im Verzeichnis /SETUP/CACERTS benötigt. Wenn Sie eigene Zertifikate zur Signatur von IDFs oder selbst erstellten eLux-Paketen verwenden, können Sie die Übertragung der Zertifikate mit der Scout-Funktion **Erweiterte Optionen… > Erweiterte Einstellungen… > Dateien** konfigurieren. Für die von Unicon bereitgestellten eLux-Pakete werden die erforderlichen Zertifikate bereits mit dem BaseOS eLux RP 4.7.0 oder höher zur Verfügung gestellt.

Für weitere Informationen zum Erstellen von IDF-Signaturen siehe IDF signieren im ELIAS-Handbuch.

Hinweis

Die Signaturprüfung von eLux Software-Paketen erfordert eine Update-Partition auf dem Client. Bei Geräten ohne Update-Partition kann die Signaturprüfung ausschließlich für Image Definition Files (IDF) erfolgen, jedoch nicht für eLux Software-Pakete.

5.9.6. Verschiebung des Updates durch den Anwender

Mit der Option zur Verschiebung des Updates kann der Anwender den Zeitpunkt des Firmware-Updates durch ein Update-Kommando selbst steuern. Damit kann der Anwender ein Firmware-Update während der Nutzung des Clients verhindern.

Der Client meldet den jeweils aktuellen Status des Updatevorganges an den Scout Enterprise-Server zurück. Die Stati sind für den Administrator in der Scout Enterprise-Konsole im Feld **Updatestatus** des entsprechenden **Eigenschaften**-Fensters ersichtlich.

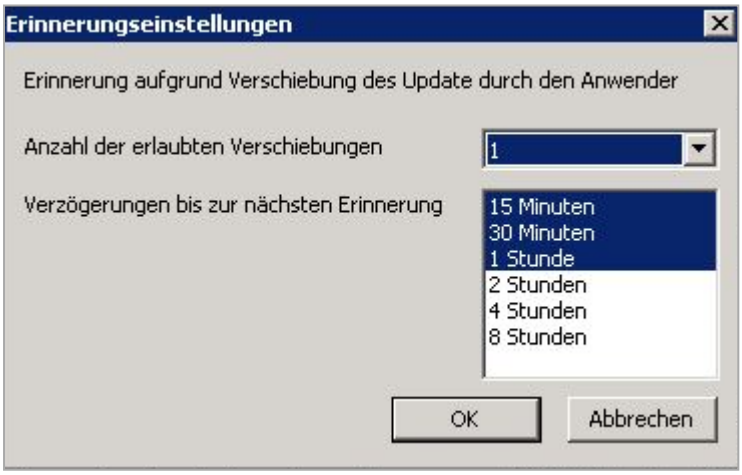
Darüber hinaus kann im Report-Generator das Feld **Updatestatus** nach dem Wert `Verschoben` ausgewertet werden (neben den Stati `Erfolgreich`, `Nicht erfolgreich` und `Nicht notwendig`).

Verschiebung von Firmware-Updates durch den Anwender konfigurieren

1. Klicken Sie in **Konfiguration > Firmware** auf die Schaltfläche **Erinnerungen...**

   *Der Dialog **Erinnerungseinstellungen** öffnet.*

2. Wählen Sie im Listenfeld die **Anzahl der erlaubten Verschiebungen**.
3. Definieren Sie im Feld **Verzögerungen bis zur nächsten Erinnerung** einen oder mehrere Zeitintervalle, aus denen der Anwender die Verzögerung bis zur nächsten Erinnerung auswählen kann. Markieren Sie dazu einen oder mehrere Einträge.

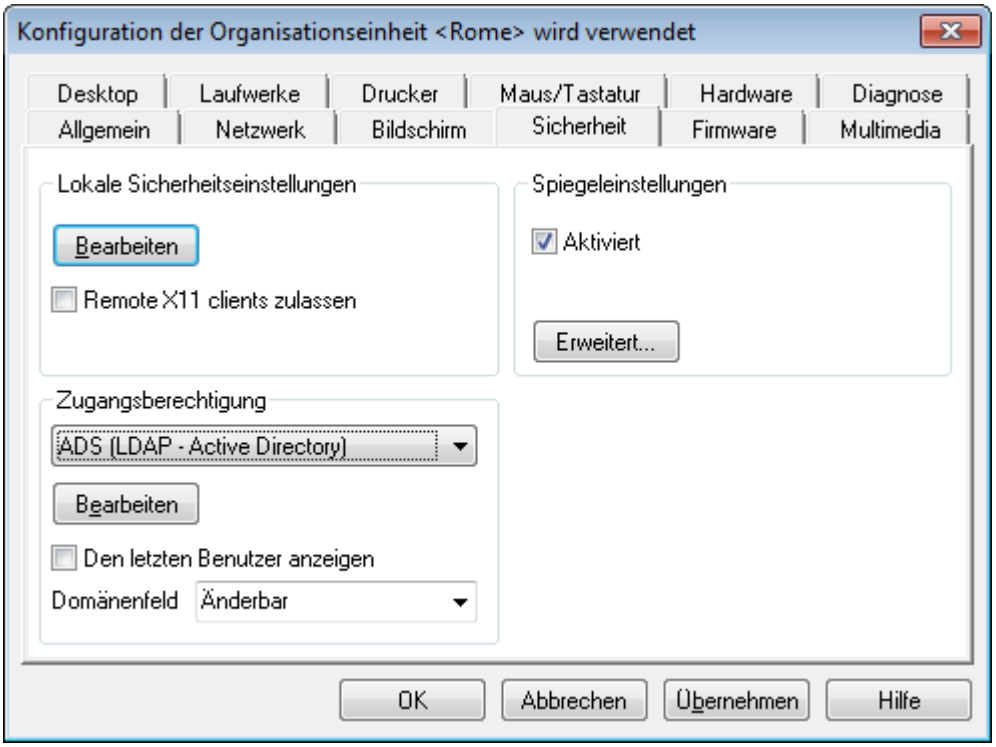


*Die Möglichkeit zur Verschiebung von Firmware-Updates ist aktiviert. Wenn der Administrator ein Update-Kommando mit aktivierter Option **Benutzer informieren für** konfiguriert, erhält der Anwender eine Systemmeldung mit der Option zum Verschieben des Updates. Für weitere Informationen siehe* Auswirkungen beim Update mit Verschieben-Option*.*

Achtung

Die Verschiebung des Updates muss einmal im **Firmware**-Register konfiguriert werden und zusätzlich für jedes Update-Kommando durch die Benutzerinformation zugelassen werden. Für weitere Informationen siehe .Update über Kommando ausführen.

5.10. Register Sicherheit



5.10.1. Spiegelung konfigurieren

1. Schalten Sie im Register **Sicherheit > Spiegeleinstellungen** die Option **Aktiviert** ein.
2. Wählen Sie **Erweitert**, um die Spiegelung zu konfigurieren.

Option	Beschreibung
Kennwort (optional)	Geben Sie ein Spiegelungs-Kennwort (maximal acht Zeichen) an, das beim Start einer Spiegelung abgefragt wird.
Nur Lesezugriff	Erlaubt nur lesenden Zugriff
Bestätigung erforderlich	Vor der Spiegelung muss der Benutzer bestätigen.
Spiegelungsinformation übertragen	Protokolliert die Spiegelungssitzung
Verschlüsselte Übertragung	Sendet die Daten über eine verschlüsselte Verbindung
Nur von Scout Enterprise erlauben	Erlaubt Spiegelung nur von einem Scout Enterprise-Server oder der Scout Enterprise Mirror App
Abmelden bei Verbindungsabbruch[1]	Sobald die Verbindung abbricht, findet eine automatische Abmeldung statt.
XDMCP	Aktiviert das XDMCP-Protokoll

3. Bestätigen Sie mit **OK** und **Übernehmen**.

Für weitere Informationen siehe Spiegelung.

Hinweis
Eine Spiegelungssitzung kann vom Gespiegelten jederzeit abgebrochen werden.

[1] ab Scout Enterprise Management Suite 14.8

5.10.2. Lokale Sicherheit

Um zu verhindern, dass Anwender lokal am Client fehlerhafte oder ungewünschte Konfigurationen vornehmen, können Sie die Benutzerrechte für die lokale Gerätekonfiguration deaktivieren oder einschränken.

Die Benutzerrechte können Sie für einzelne Geräte und OUs bis auf Feldebene einstellen. Beispielsweise können Sie aus Sicherheitsgründen alle Register sperren und nur einzelne Funktionen wie die Monitoreinstellungen zulassen. Für weitere Informationen siehe Lokale Konfiguration schützen

Register und Felder, die Sie zur Bearbeitung sperren, werden am Client abgeblendet.

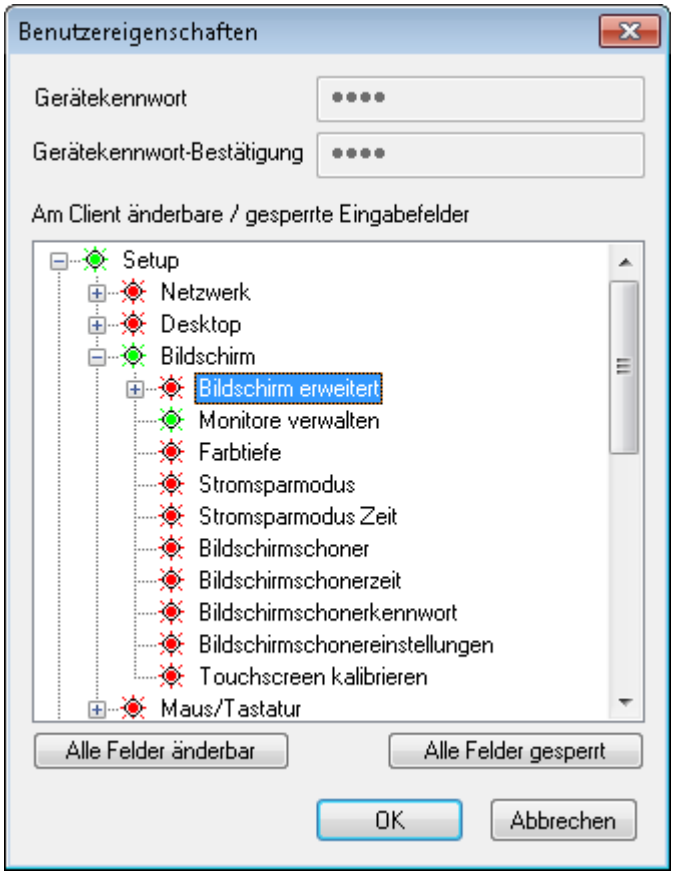
Benutzerrechte ändern

Die eLux-Systemsteuerung enthält das Register **Konfiguration** mit den Anwendungsdefinitionen für die installierten Anwendungen und das Register **Setup** mit der Gerätekonfiguration. Für beide Register können Sie die Benutzerrechte für alle aufgeführten Funktionen bearbeiten. Zusätzlich werden allgemeine Funktionen wie beispielsweise **Abmelden** angezeigt. Eine Funktion kann entweder zugelassen oder gesperrt werden.

Hinweis
Wenn Sie die individuelle Konfiguration einzelner Funktionen zulassen, können Sie die betroffenen Felder oder Register vor dem Überschreiben durch eine aktualisierte Gerätekonfiguration in Scout Enterprise schützen. Für weitere Informationen siehe Individuelle Konfiguration schützen.

Benutzerrechte für die Gerätekonfiguration bearbeiten

1. Klicken Sie im Register **Sicherheit** unter **Lokale Sicherheitseinstellungen** auf die Schaltfläche **Bearbeiten**.



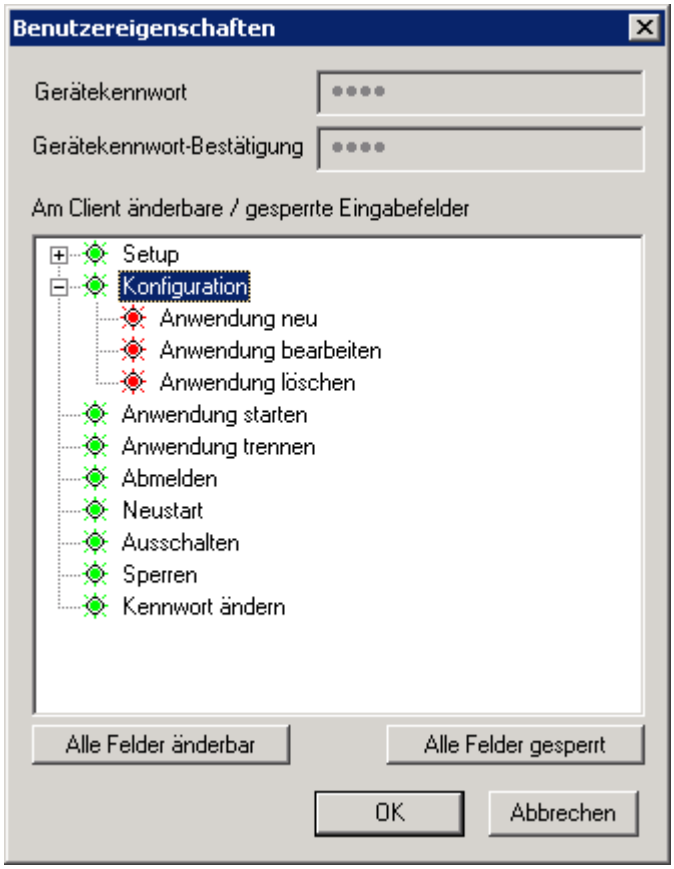
*Der Knoten **Setup** bezieht sich auf die Gerätekonfiguration und entspricht den Registern und Feldern der Systemsteuerung.*

2. Erweitern Sie die relevanten Knoten unterhalb von **Setup**.
3. Verändern Sie den Status der relevanten Funktionen per Doppelklick oder Leertaste.

Zugelassene Funktionen werden grün dargestellt, gesperrte Funktionen werden rot dargestellt. Die veränderten Benutzerrechte werden beim nächsten Neustart der Clients aktiv.

Benutzerrechte für die Anwendungsdefinitionen bearbeiten

1. Klicken Sie im Register **Sicherheit** unter **Lokale Sicherheitseinstellungen** auf die Schaltfläche **Bearbeiten**.



*Der Knoten **Konfiguration** bezieht sich auf die definierten Anwendungen.*

2. Verändern Sie den Status der unter **Konfiguration** untergeordneten Funktionen per Doppelklick oder Leertaste, je nachdem, ob die Benutzer Anwendungsdefinitionen erstellen, bearbeiten oder löschen dürfen.
3. Wenn Sie den Knoten **Konfiguration** sperren, wird das Register **Konfiguration** in der Client-Systemsteuerung abgeblendet und die Benutzer können die Anwendungsdefinitionen nicht sehen.

Hinweis

Wenn Sie individuelle Konfiguration schützen und die drei Funktionen für die Anwendungen sperren, empfehlen wir auch den übergeordneten Knoten **Konfiguration** zu sperren, um sicherzustellen, dass die Anwendungsdefinitionen korrekt aktualisiert werden.

Zugelassene Funktionen werden grün dargestellt, gesperrte Funktionen werden rot dargestellt. Die veränderten Benutzerrechte werden beim nächsten Neustart der Clients aktiv.

Verbindung zu X11-Clients zulassen

Auf Remote-Rechnern ausgeführte X11-Anwendungen können auf diesem Client dargestellt werden.

- Aktivieren Sie im Register **Sicherheit** unter **Lokale Sicherheitseinstellungen** die Option **Remote X11 Clients zulassen**.

Achtung

Wenn Sie die Verbindung zu X11-Clients zulassen, ist der Zugriff auf den Client-Bildschirm durch X11-Hilfsprogramme möglich und es können beispielsweise Screenshots erstellt werden.

5.10.3. Zugangsberechtigung konfigurieren

Hinweis
Voraussetzung für die Benutzerauthentifizierung ist, dass die **User authorisation modules** auf den Clients installiert sind.

1. Wählen Sie im Register **Sicherheit** unter **Zugangsberechtigung** eine Authentifizierungsmethode.

Keine	schaltet Benutzerauthentifizierung aus
ADS (LDAP - Active Directory)	Active Directory-Server Client-Daten können am Server abgelegt werden.
LDAP (LDAP - Server)	Lightweight Directory Access Protocol-Server
SMB (Windows NT 4.0)	Windows NT Primary Domain Controller (PDC)
ADS + SmartCard	SmartCard über AD
SmartCard (Smarty)	Authentifizierung mit personifizierter SmartCard, die jedoch nicht mehr unterstützt wird
SmartCard (X.509)	SmartCard über LDAP

2. Klicken Sie auf die Schaltfläche **Bearbeiten**. Legen Sie Server, eine Serverliste oder Domänen fest. Weitere Informationen finden Sie auf den folgenden Seiten. Wenn gewünscht, definieren Sie Benutzervariablen. Für weitere Informationen siehe Benutzervariablen.
3. Aktivieren Sie die Option **Letzten Benutzer anzeigen**, wenn Sie die Benutzer bei der Anmeldung unterstützen möchten.
4. Wählen Sie im Listenfeld **Domänenfeld**, ob die Benutzer die Domäne ändern dürfen oder ob die Domäne ausgeblendet werden soll.
5. Bestätigen Sie mit **OK**.

Wenn Sie eine Authentifizierungsmethode konfiguriert haben, werden bei der nächsten Client-Anmeldung Benutzername und Kennwort abgefragt.

Hinweis
Für Geräte, die nicht mit Scout Enterprise verwaltet werden, kann sich der Administrator mit dem Benutzernamen `LocalLogin` und dem Gerätekennwort anmelden und ggf. Einstellungen korrigieren.

Active Directory (AD)

Ab Scout Enterprise Management Suite Version 14.8 können Sie mehrere Domänen definieren, die der Benutzer im Anmelde-Dialog neben der Standard-Domäne auswählen kann. Die Domänen-Einträge können mit einem sprechende Namen angezeigt werden.

Hinweis
Damit sich Benutzer an mehreren Domänen anmelden können, müssen auf den Clients müssen folgende Software-Pakete installiert sein:

userauth >= 3.0.0-8
securitylibs >= 1.6.0.2-2
baseosrp >= 5.4.0-1

Register Verzeichnis

- Erstellen Sie einen oder mehrere Einträge mit **Hinzufügen** und bearbeiten Sie den Eintrag anschließend (F2 oder Doppelklick).

Option	Beschreibung
Name (optional)[1]	Anzeigename für die Domäne
Server, Serverliste oder Domäne	IP-Adresse oder Name des Domänen-Controllers Mehrere Server können durch Leerzeichen getrennt angegeben werden Wenn sich der Server in einem anderen Subnetz als der Client befindet, muss der fully qualified domain name (FQDN) angegeben werden. Wenn Sie mehrere Domänen Einträge definieren[2], kann der Benutzer aus einem Listenfeld wählen. Die Domänen werden mit ihrem Anzeigenamen angezeigt. Der oberste Eintrag ist die Standard-Domäne im AD-Anmelde-Dialog am Client.
Suchbasis[3]	Knotenpunkt im Domänen-Baum (Directory Tree), ab dem die Benutzer gesucht werden sollen Beispiel:`DC=IhreDomain,DC=de` Nur eLux: Klicken Sie auf **Werte ermitteln**, damit der Client nach dem Server sucht und die Daten automatisch einträgt.

Hinweis
Wir empfehlen, einen Windows Zeitserver einzurichten. Bei unterschiedlicher Systemzeit von Domain Controller und Client können AD-Abfragen nicht erfolgreich gestellt werden.

[1]ab Scout Enterprise Management Suite Version 14.8
[2]ab Scout Enterprise Management Suite Version 14.8
[3]ab Scout Enterprise Management Suite Version 14.8 mit Rechtsklick auf den Anzeigenamen

Register Serverprofil (nur Scout Enterprise)

Wenn Sie die Option **Serverprofil verwenden** aktivieren, werden beim Abmelden verschiedene Benutzerdaten (nur Daten, die nicht von Scout Enterprise verwaltet werden) zusammengepackt und auf einem Server-Verzeichnis abgelegt. Beim Anmelden werden diese Daten wiederhergestellt. Dadurch erhält jeder Benutzer seine Benutzerdaten unabhängig vom Client, an dem er sich anmeldet. Das Profil-Verzeichnis muss im AD im UNC-Format vorgegeben werden.

Hinweis

Beim Ausschalten über die **Beenden**-Schaltfläche der Systemsteuerung ist bei Verwendung von AD die Option **Kennwort ändern** verfügbar.

Lightweight Directory Access Protocol (LDAP)

LDAP ist ein TCP/IP-basiertes Protokoll, das den Zugriff auf Verzeichnisdienste ermöglicht.

Option	Beschreibung
Server	IP-Adresse oder Name des LDAP-Servers Mehrere Server können durch Leerzeichen getrennt angegeben werden. Wenn sich der Server in einem anderen Subnetz als der Client befindet, muss der fully qualified domain name (FQDN) angegeben werden.
Suchbasis	Knotenpunkt im Domänen-Baum (Directory Tree), ab dem die Benutzer gesucht werden sollen Beispiel: `o=<Firma>,l=<Ihre Stadt>,c=<Ihr Land>` Nur eLux: Klicken Sie auf **Werte ermitteln**, damit der Client nach dem Server sucht und die Daten automatisch einträgt.
Version	Zu verwendende LDAP-Version

SMB (Windows NT 4.0)

Benutzerinformationen werden zentral auf dem PDC verwaltet und können auf einen BDC repliziert werden..

Option	Beschreibung
Domäne	NT-Domäne
Erster	Hostname des PDC (=NetBIOS-Name) IP-Adresse ist nicht zulässig.
Zweiter	Hostname des BDC (=NetBIOS-Name) Die Angabe mehrerer BDCs ist nicht zulässig. IP-Adresse ist nicht zulässig

SmartCard

Register SmartCard

Option	Beschreibung
Verhalten beim Ziehen der SmartCard	Wenn Sie die Option `Bildschirm sperren` wählen, überprüfen Sie, ob in **Setup > Bildschirm > Bildschirmschoner** die Option **Kennwortschutz** aktiviert ist
Anmeldung mit Benutzer/Kennwort erlauben	SmartCard-Anwendung erlaubt Anmeldung mit Benutzername/Kennwort durch Drücken der ESC-Taste.

Register Zertifikat

Die Zertifikat-basierte Anmeldung erfordert die Prüfung des Benutzer-Zertifikats gegen das Root-Zertifikat.

- Markieren Sie ein oder mehrere Root-Zertifikate und klicken Sie auf **Hinzufügen...**.

Die markierten Zertifikate werden zum Client übertragen.

5.10.4. Benutzervariablen

Die Werte von Benutzervariablen werden beispielsweise vom Authentifizierungsserver beim Anmelden ausgelesen. Die Variablen können zusätzlich in bestimmten Feldern der eLux-Systemsteuerung als Parameter verwendet werden.

Vorgegebene Benutzervariablen sind `$ELUXUSER`, `$ELUXDOMAIN` und `$ELUXPASSWORD`. Diese werden beim Anmelden eingetragen, wenn die Benutzerauthentifizierung eingeschalltet ist.

Bei der Authentifizierung über LDAP oder ActiveDirectory können Sie zusätzlich eigene Variablen definieren.

Hinweis
Um Benutzervariablen verwenden zu können, muss das Paket **User authorisation modules** und **Open LDAP** installiert sein.

Anwendungsmöglichkeiten für Benutzervariablen

Die Benutzervariablen können in den folgenden Feldern verwendet werden, wenn die Benutzerauthentifizierung eingeschaltet ist.

Hinweis
Benutzervariablen werden ohne führendes `$`-Zeichen definiert, müssen aber bei der Anwendung mit dem `$`-Zeichen eingeleitet werden.

Konfiguration

Befehl	Funktion	Benutzervariable
Start > Sperren	Manuelle Aktivierung der Bildschirmsperre	Das Kennwort ist mit dem aktuellen Wert aus `$ELUXPASSWORD` vorbelegt

Setup

Register	Feld	Benutzervariable
Laufwerke	Benutzername	`$ELUXUSER`
	Kennwort	`$ELUXPASSWORD`
	Verzeichnis, Server, Freigabename	Jede `$ELUX`-Variable
	Browser Homeverzeichnis	Jede `$ELUX`-Variable
Bildschirm	Bildschirmschoner-Kennwort	`$ELUXPASSWORD`

Anwendungen

Register	Feld	Benutzervariable
ICA/RDP	Server	Jede `$ELUX`-Variable
	Benutzername	`$ELUXUSER`
	Kennwort	`$ELUXPASSWORD`
	Domäne	`$ELUXDOMAIN`
Browser	Proxytyp, Proxy-Port	Jede `$ELUX`-Variable
Tarantella	Server	Jede `$ELUX`-Variable
Lokal / Benutzerdefinierte Anwendung	Parameter für alle Programme, die über die Kommandozeile aufgerufen werden Beispiel: `eluxrdp /v:MyHost.MyDomain.de /u:$ELUXUSER /p:$ELUXPASSWORD`	Jede `$ELUX`-Variable

Neue Benutzervariable definieren

Für die Zugangsberechtigung über AD und LDAP können Sie eigene Benutzervariablen definieren (lokale Variablen).
Die Variablen basieren auf LDAP-Attributen und werden in der Form `Lokale Variable = LDAP-Variable` definiert

1. Wählen Sie in **Konfiguration > Sicherheit** im Feld **Zugangsberechtigung** entweder `AD` oder `LDAP` als Authentifizierungsmethode.
2. Klicken Sie auf **Bearbeiten**.

3. Bearbeiten Sie im Dialog **Zugangskonfiguration > Benutzervariablen** folgende Felder:

Option	Beschreibung
Lokale Variable	Der Name für die lokale Variable muss mit der Zeichenkette `ELUX` beginnen (kein einleitendes `$`-Zeichen) und kann eine beliebige Zeichenfolge enthalten. Beispiel: `ELUXFULLNAME` Durch Verwendung des `#`-Zeichens am Ende des Variablennamens können mehrere Einträge übertragen werden. Beispiel: `ELUXmemberOf#`
LDAP Variable	Um auf LDAP-Variablen zugreifen zu können, verwenden Sie den entsprechenden LDAP-Variablennamen und ordnen ihn der eigenen Variable als Attribut zu. Beispiel 1: `ELUXFULLNAME` = `displayName` Beispiel 2: `ELUXmemberOf#` = `memberOf` Wenn mehrere `memberOf`-Werte innerhalb der Suchbasis auf dem Authentifizierungsserver vorhanden sind, werden diese den lokalen Variablen `ELUXmemberOf_1`, `ELUXmemberOf_2` etc. zugeordnet.

4. Bestätigen Sie mit **OK** und **Übernehmen**.

Hinweis
Benutzervariablen werden ohne führendes `$`-Zeichen definiert, müssen aber bei der Anwendung mit dem `$`-Zeichen eingeleitet werden.

5.11. Register Multimedia

Die angeschlossenen **Ausgabe**-Geräte werden nach ihrem Anschluss gruppiert:

USB	Geräte über USB-Anschluss
Analog	über Klinken-Stecker (Jack) angeschlossene oder eingebaute Geräte
Digital	Geräte über DisplayPort oder HDMI

Für jede Geräteklasse können Sie den Grad der Lautstärke und **Ton aus** getrennt regeln.

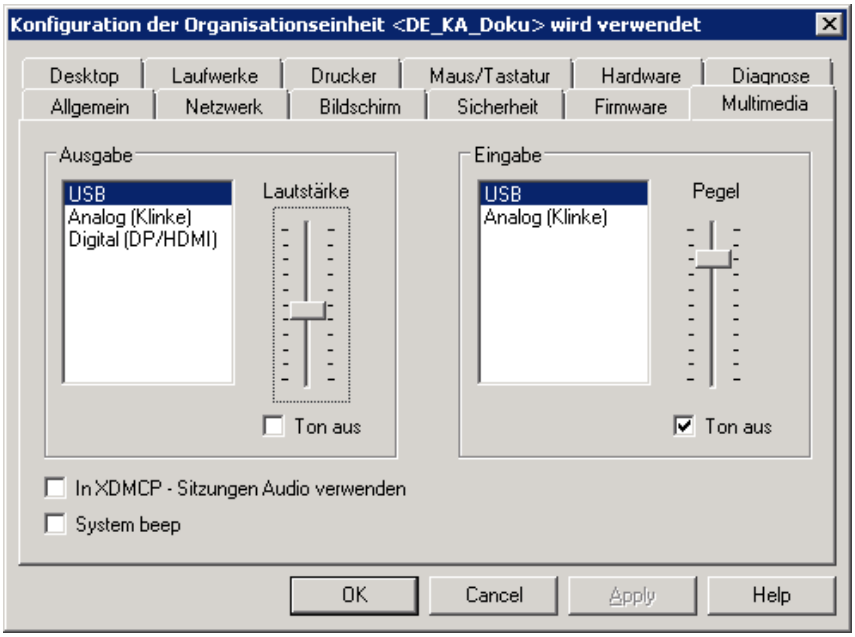
Standardmäßig ist die Priorität in folgender Reihenfolge definiert: USB – Analog – Digital. Um die Priorität zu ändern, verschieben Sie die Listeneinträge per Drag-und-Drop.

Die angeschlossenen **Eingabe**-Geräte werden nach ihrem Anschluss gruppiert:

USB	Geräte über USB-Anschluss
Analog	über Klinken-Stecker (Jack) angeschlossene oder eingebaute Geräte

Für jede Geräteklasse können Sie die Empfindlichkeit und **Ton aus** getrennt regeln.

Standardmäßig ist die Priorität in folgender Reihenfolge definiert: USB – Analog. Um die Priorität zu ändern, verschieben Sie die Listeneinträge per Drag-und-Drop.



Option	Beschreibung
Lautstärke (Ausgabe)	Schieberegler für die Lautstärke der Ausgabe für die markierte Geräteklasse (0 bis 100)

Option	Beschreibung
Pegel (Eingabe)	Schieberegler für die Empfindlichkeit der Eingabe (Mikrofon) für die markierte Geräteklasse (0 bis 100)
Ton aus (Ausgabe und Eingabe)	Es wird kein Ton abgespielt bzw. aufgenommen.
In XDMCP-Sitzungen Audio verwenden	Töne in X-Server-Sitzungen werden wiedergegeben
System beep	Akustische Systemrückmeldung beim Ausschalten des Thin Client

5.12. Register Laufwerke

Definieren Sie freigegebene Netzwerk-Verzeichnisse auf Ihrem Windows-Server als Laufwerke, auf die der Client zugreifen kann. Ein so definiertes Laufwerk kann beispielsweise als Speicherort für Browser-Dateien verwendet werden.

5.12.1. Netzlaufwerk definieren

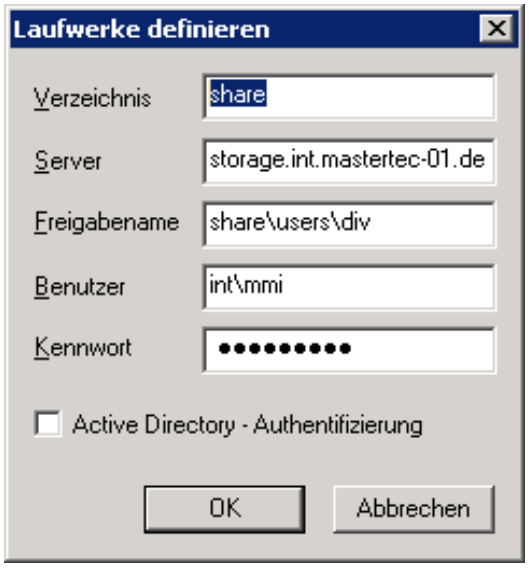
1. Klicken Sie im Register **Laufwerke** auf **Neu**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Verzeichnis	Frei wählbarer Verzeichnisname
Server	Name des Servers inklusive Pfad
Freigabename	Windows-Freigabename
Benutzername und Kennwort	Windows-Benutzername und Kennwort für den Zugriff auf das Verzeichnis
Domäne	Kann alternativ im Feld **Benutzer** angegeben werden: `<Domäne\Benutzer>` oder `<Benutzer@Domäne>`
AD-Authentifizierung (nur Scout Enterprise)	Die Active Directory-Anmeldedaten werden für den Zugriff verwendet. Die Felder **Benutzername** und **Kennwort** werden deaktiviert.
Test (nur eLux)	überprüft, ob die Verbindung mit den angegebenen Daten hergestellt werden kann

> **Hinweis**
> Um auf Netzlaufwerke mit AD-Authentifizierung zugreifen zu können, müssen für eLux RP 5.3 die eLux-Pakete **userauth-3.0.0-3** und **securitylibs-1.6.0.2-1** auf den Clients installiert sein. Für eLux RP 5.3 und höhere Versionen muss das Paket **Network drive share** und das hierin enthaltene Feature-Paket **Linux Key Management Utilities** auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

3. Bestätigen Sie mit **OK** und **Übernehmen**.

Vor dem Verzeichnisnamen wird automatisch der Verzeichnispfad `/smb/` eingefügt. Die Daten sind lokal unter dem Verzeichnis `/smb/<Verzeichnisname>` verfügbar.



Hinweis
Verwenden Sie LDAP-Benutzervariablen. Für weitere Informationen siehe Anwendungsmöglichkeiten für Benutzervariablen.

Um Browser-Einstellungen wie Bookmarks dauerhaft verfügbar zu machen, definieren Sie ein Netzlaufwerk als Browser-Homeverzeichnis. Für weitere Informationen siehe Speicherort für Browserdateien festlegen.

5.12.2. Mountpoints

Für den Zugriff auf lokale Ressourcen muss ein sogenannter Mountpoint verwendet werden. Die Mountpoints für eLux sind:

Samba	`/smb`
NFS	`/nfs`
Internes CD-ROM	`/media/cdrom`
USB Peripherie	`/media/usbdisk*`

*Für USB werden die Mountpoints chronologisch zugewiesen. Das erste Gerät erhält den Mountpoint `/media/usbdisk`, das zweite `/media/usbdisk0` usw.

Aktive Geräte werden mit Mountpoint im Systray angezeigt, wenn die Option im Register **Desktop > Erweitert** unter **Taskleiste** aktiv ist.

Hinweis
Aus Sicherheitsgründen muss die Option **Massenspeichergeräte erlauben** im Register Hardware aktiviert werden.

Hinweis

Die Laufwerkszuordnung für den Zugriff auf lokale Ressourcen wird in der jeweiligen Anwendungsdefinition vorgenommen. Für Citrix-Anwendungen siehe Citrix Software-Standardeinstellungen, für RDP-Anwendungen siehe Erweiterte RDP-Einstellungen.

5.13. Register Drucker

Der eLux Druckservice unterstützt das Drucken aus lokalen Anwendungen heraus sowohl zu einem lokal angeschlossenen Drucker als auch zu Netzwerkdruckern. Darüber hinaus können andere Systeme oder Server innerhalb des Netzwerks einen lokal am Thin Client angeschlossenen Drucker nutzen. Der Drucker muss dafür LPR und TCP Direktdruck unterstützen.

In Scout Enterprise unter **Konfiguration > Drucker > Neu** können Sie lokale Drucker mit logischen Namen definieren und konfigurieren. Auf diese Drucker kann dann innerhalb des Netzwerks zugegriffen werden.

Die Option **Druckdienst aktiviert** legt fest, dass der Druckdienst am Client gestartet werden soll.

5.13.1. Drucker als Standarddrucker auswählen

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevante OU oder Gerät die **Erweiterte Einstellungen > Drucker**.
2. Wählen Sie aus der Dropdownliste **Standarddrucker auswählen** einen Drucker aus.

   *Alle bereits definierten Drucker für dieses Element werden in der Liste angeboten. Sollte ein Drucker nicht angezeigt werden, definieren Sie ihn zunächst im Register **Drucker** der Basiskonfiguration oder einer übergeordneten OU.*

5.13.2. Definieren eines Netzwerkdruckers

1. Aktivieren Sie den Windows LPD Dienst (Line Printer Demon).

   Der TCP/IP-Druckerserverdienst wird installiert und gestartet. Dies ist Voraussetzung für die Ansteuerung des Druckers.
2. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Geräte die **Gerätekonfiguration > Drucker**. In eLux öfnnen Sie die Systemsteuerung und **Setup > Drucker**.
3. Klicken Sie auf die Schaltfläche **Neu**.

   *Der Dialog **Drucker definieren** öffnet.*
4. Geben Sie einen **Namen** für den Netzwerkdrucker ein.
5. Wählen Sie im Feld **Druckeranschluss** den Wert `Netzwerk`.
6. Wählen Sie im Feld **Filter** eine der folgenden Optionen:

Option	Beschreibung
Kein	Ermöglicht Drucken aus einer Remote-Session. Die fertigen Druckdaten aus der Session werden ungefiltert im RAW-Format an den Drucker weitergeleitet.
Text	Ermöglicht Drucken aus einer lokalen Shell.
PCL2	ermöglicht das Drucken von Webseiten, die mit dem lokalen Firefox aus eLux geöffnet werden, sowie das Drucken von PDF-Dateien aus eLux. Der angeschlossene Drucker muss eine der folgenden Sprachen unterstützten: **PCL2**, **PS** (Postscript) oder **PDF**.

Hinweis

Wenn ein Drucker lokal am Thin Client definiert wurde, kann direkt aus eLux gedruckt werden, beispielsweise Text aus einer lokalen Shell oder ein PDF-Dokument aus Firefox. Ebenfalls kann aus einer Remote Session gedruckt werden. Wird aus der Citrix-Session gedruckt, so wird automatisch der Filter `Kein` verwendet. Durch diese automatische Filter-Erkennung kann eLux die in der Session bereits vorverarbeiteten Daten direkt an den entsprechenden Drucker weiterleiten. Weitere Informationen finden Sie im Scout Enterprise Handbuch unter Citrix auto-created Printers im Scout Enterprise-Handbuch.

7. Geben Sie im Feld **Druckeradresse** die IP-Adresse des Servers ein.
   Oder:
   Geben Sie einen Namen aus der lokalen Host-Datenbasis des Clients ein. Diese finden Sie unter **Setup > Netzwerk > Erweitert**.
8. Geben Sie in das Feld **Druckerqueue** den Freigabenamen des Druckers ein.
9. Geben Sie im Feld **Treibernamen** den Treibernamen für den Drucker ein.

Achtung

Der eingetragene Druckertreiber-Name muss genau mit dem auf dem Server installierten Treibernamen übereinstimmen. Überprüfen Sie den Namen auf der Liste der installierten Druckertreiber auf dem Server. Achten Sie auf Groß-/Kleinschreibung sowie Leerzeichen.

10. Bestätigen Sie mit **OK**.
11. Bestätigen Sie die Einstellungen im Register **Drucker** mit der Schaltfläche **Übernehmen**.

5.13.3. Citrix auto-created Printers

Citrix XenApp bietet die Möglichkeit, Drucker automatisch einzurichten ("autocreated printer" oder "dynamic printer mapping"). Das bedeutet, dass beim Anmelden über ICA automatisch eine Druckerdefinition am XenApp Server erstellt wird. Diese Druckerdefinition gilt nur für die Dauer der ICA-Sitzung, d.h. sie wird mit der Abmeldung gelöscht und steht nur dem angemeldeten Benutzer zur Verfügung.

XenApp kann lokale Drucker erstellen, die am Client-Rechner angeschlossen sind oder einen universellen Citrix-Drucker, der nicht an ein bestimmtes Gerät gebunden ist.

Lokalen Drucker clientseitig für die automatische Druckereinrichtung konfigurieren

1. Geben Sie unter **Konfiguration > Drucker** einen oder mehrere Drucker an.
2. Geben Sie im Dialog **Drucker** im Feld **Name** den Microsoft Windows-Druckernamen genauso ein, wie er in der Treiber-Liste am Server angegeben ist. Achten Sie auf Groß-/Kleinschreibung.

*Wird eine ICA-Verbindung zum Citrix XenApp Server gestartet, sieht der Benutzer im Drucker-Dialog (**Start > Einstellungen > Drucker**) Symbole für die automatisch erstellten Client-Drucker in folgendem Format:*

`Client\`*<Hostname>#\<Drucker>*

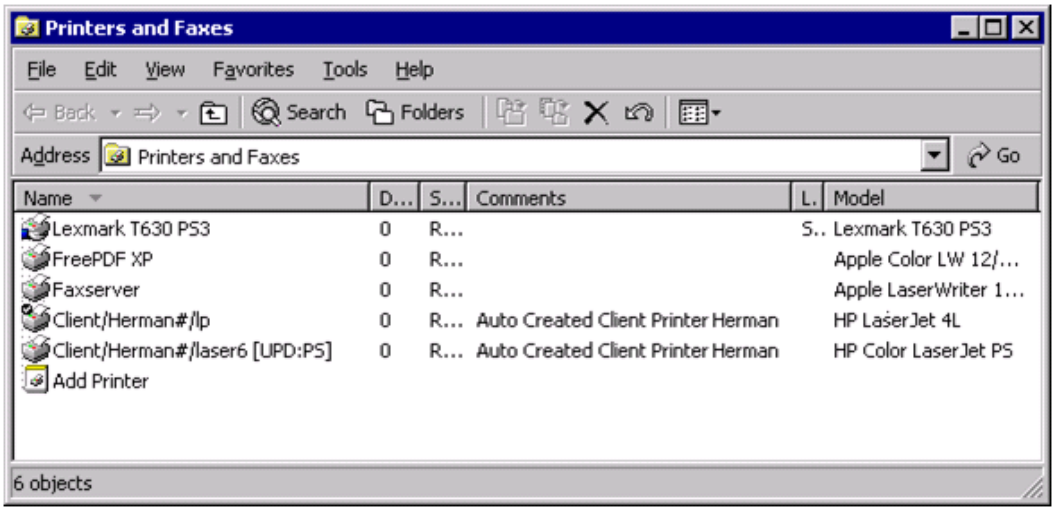
<Hostname> ist der Hostname des Thin Client und <Drucker> der Name des in Scout Enterprise definierten Druckers.
Sollte der spezifische Treiber nicht am Anwendungsserver installiert sein oder ist der Name nicht identisch, dann wird der Client-Drucker nicht erstellt. In diesem Fall wird der universelle Citrix-Drucker genutzt.

Universellen Citrix-Drucker am XenApp-Server konfigurieren

Dieses Feature setzt den aktuellen Citrix ICA-Client für Linux am Thin Client voraus. Der generische Treiber ist der XenApp Universaltreiber.

1. Melden Sie sich als Administrator am XenApp Server an
2. Öffnen Sie die Managementkonsole für XenApp.
3. Wählen Sie im Kontextmenü der **Druckerverwaltung** den Eintrag **Eigenschaften**.
4. Klicken Sie im linken Fensterbereich auf **Drucker** und konfigurieren Sie die automatische Erstellung von Client-Druckern. Weitere Informationen entnehmen Sie bitte der Citrix-Dokumentation.
5. Klicken Sie im linken Bereich auf **Treiber** und konfigurieren Sie den Treiber:

Option	Beschreibung
Nur native Treiber	Ein Client-Drucker wird mit dem in Scout Enterprise definierten nativen Treiber erstellt. Wenn der Treiber nicht am XenApp Server installiert ist, wird der Client-Drucker nicht erstellt.
Nur universeller Treiber	Ein Client-Drucker wird erstellt. Der in Scout Enterprise definierte Druckertreiber wird durch den universellen Treiber ersetzt.
Universellen Treiber nur verwenden, wenn nativer Treiber nicht verfügbar ist	Ein Client-Drucker wird mit dem in Scout Enterprise definierten nativen Treiber erstellt. Wenn der native Treiber nicht am XenApp Server installiert ist, wird der universelle Treiber verwendet.
Universelle und native Treiber	Für jeden Client-Drucker werden zwei Versionen erstellt, eine mit dem universellen Treiber und eine mit dem in Scout Enterprise definierten nativen Treiber.
Native Treiber für automatisch erstellte Client- und Netzwerkdrucker automatisch installieren	Native Druckertreiber werden auf XenApp Servern selbsttätig installiert, wenn die **Automatische Erstellung** aktiv ist..



Wenn Sie einen universellen Treiber nutzen, wird der Druckername um den folgenden Text ergänzt:

`[UPD:<generic driver name>]`, wobei `<generic driver name>` im Beispiel der Text `PS` ist.

In obiger Abbildung wurde der Clientdrucker `Client/Herman#/lp` mit dem nativen Treiber `HP LaserJet 4L` erstellt. Dagegen wurde der Clientdrucker `Client/Herman#/laser6 [UPD:PS]` mit dem generischen Treiber für PostScript erstellt, da der angegebene Treiber `HP LaserJet PS` nicht auf dem Anwendungsserver installiert ist.

Mehr Informationen zu serverseitigen Druckereinstellungen finden Sie in der **Citrix Product Documentation** für XenApp.

5.13.4. TCP-Direktdruck

Sie haben die Möglichkeit, direkt via TCP/IP auf die parallele Schnittstelle bzw. die USB-Schnittstelle Druckdaten zu schicken. In diesem Fall werden die Daten nicht mehr für den Druck aufbereitet und keine Protokolldaten zum fernen Spoolsystem gesendet. Die Flusskontrolle übernimmt TCP/IP.

- Aktivierien Sie unter **Konfiguration > Drucker** den TCP-Direktdruck.
- Geben Sie die Portnummer zur Kommunikation an (Standard ist Port 9101 für USB-Drucker und Port 9100 für Parallelport-Drucker).
- Wenn Sie aus einer Windowssitzung drucken wollen, wählen Sie als Druckeranschluss einen "Standard TCP/IP Port" und geben Sie die IP-Adresse des Thin Clients sowie den TCP/IP-Port an, den Sie im vorherigen Schritt gewählt haben; als Protokoll in Windows wählen Sie "Raw".

5.13.5. ThinPrint

ThinPrint von der Firma Cortado AG in Deutschland ermöglicht optimiertes Drucken im Netzwerk auf verschiedenen Plattformen. Die Software beinhaltet eine Server-Komponente und eine Client-Komponente. Die Server-Komponente bereitet die Druckdaten für den Zieldrucker auf und sendet sie in komprimierter Form an den Client. Der Client empfängt die Druckjobs vom Server, dekomprimiert sie und leitet sie an den ausgewählten Drucker weiter. ThinPrint-Server und -Client sind per TCP/IP verbunden. ThinPrint ist ein Druckprotokoll, das im Gegensatz zu TCP-Direktdruck, LPR oder CUPS eine Begrenzung der Bandbreite erlaubt. Es empfiehlt sich daher zum Einsatz in Netzwerken mit geringer Bandbreite (WAN).

ThinPrint konfigurieren:

1. Installieren Sie den ThinPrint-Client auf dem Thin Client.
2. Schließen Sie einen Drucker an.
3. Wenn Sie Windows CE Clients einsetzen, legen Sie in **Setup > Drucker** unter **ThinPrint** das relevante Protokoll fest.
4. Definieren Sie den Drucker unter **Setup > Drucker > Neu** und aktivieren Sie die Option **ThinPrint**. Fügen Sie optional einen Klassennamen mit max. 7 Zeichen Länge ein.
5. Konfigurieren Sie den ThinPrint-Server. Für weitere Informationen siehe die ThinPrint Dokumentation auf www.thinprint.com.

5.13.6. CUPS

Das Common UNIX Printing System™ (CUPS™) ist ein Produkt von Easy Software Products. Es bietet eine allgemein übliche Druckschnittstelle innerhalb eines lokalen Netzwerks sowie die dynamische Druckererkennung und Gruppierung. Der Vorteil von CUPS ist, dass die gesamte Konfiguration am CUPS-Server vorgenommen wird, und nicht lokal am Client.

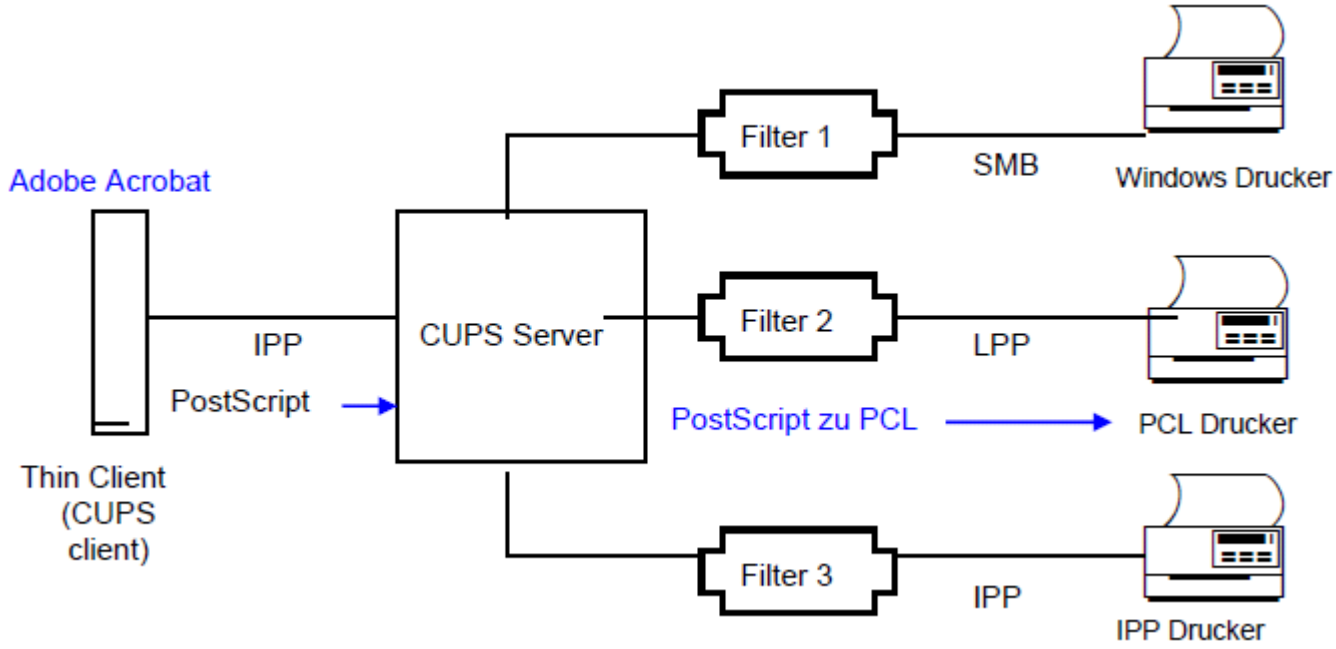
Der CUPS-Server enthält eine Liste von Ausgabeschnittstellen (Backends) inklusive seriellen und parallelen Ports, USB und Netzwerk (LPD).

Wenn der CUPS-server installiert ist, ersetzt er das lokale LPD Drucksystem am Client.

CUPS-Client und -Server sind kostenfrei. Add-ons und Support für den CUPS Server sindbei Easy Software Products gegen Entgelt erhältlich.

CUPS ist optimal geeignet zum Drucken aus lokalen Anwendungen am Thin Client (beispielsweise aus Adobe Acrobat oder einem Browser). Diese lokalen Anwendungen haben das Ausgabeformat PostScript. Ist kein PostScript-Drucker vorhanden, müssen Sie am CUPS-Server einen Filter installieren (Beispiel: PostScript zu PCL).

CUPS Ablauf



1. Das Programm (Adobe Acrobat) generiert eine Ausgabedatei (PostScript Format) und sendet diese an den CUPS Server via IPP.
2. CUPS konvertiert PostScript zu PCL unter Verwendung des vorinstallierten Filters.
3. CUPS sendet den Druckjob an den Drucker unter Verwendung des vorinstallierten Backends (parallel, seriell, Netzwerk etc.).

CUPS-Client am Thin Client installieren

Voraussetzung
Das Paket **Print Environment (CUPS) (baseprinter)** muss auf dem eLux Client installiert sein.

1. Installieren Sie den CUPS-Server auf einem beliebigen Computer und konfigurieren Sie den CUPS-Server.

   Eine Anleitung zur Installation und Konfiguration des CUPS-Servers finden Sie auf www.-cups.org.

2. Definieren Sie folgende Umgebungsvariablen in Scout Enterprise:

Variable	Beschreibung
CUPS_SERVER	Hostname oder IP-Adresse des CUPS-Servers.
CUPS_OPTIONS (optional)	Damit werden benutzerspezifische Druckoptionen vorbesetzt. Diese Optionen sind in der Druckerdatei `.ppd` file definiert. Fragen Sie Ihren CUPS-Administrator nach dem Parameter. Beispiel: CUPS_OPTIONS=-o OutputBin=Bin2. Tipp: Wenn Sie LDAP oder AD verwenden, können Sie anstelle der in Scout Enterprise definierten Umgebungsvariable CUPS_OPTIONS die Benutzervariable ELUX_PRINTEROPTIONS verwenden, die am LDAP- oder AD-Server definiert ist. Informationen zur Definition von LDAP-Benutzervariablen finden Sie im Kapitel Benutzervariablen.

3. Übertragen Sie die Umgebungsvariablen auf den Thin Client.

Drucken aus einem lokalen Browser

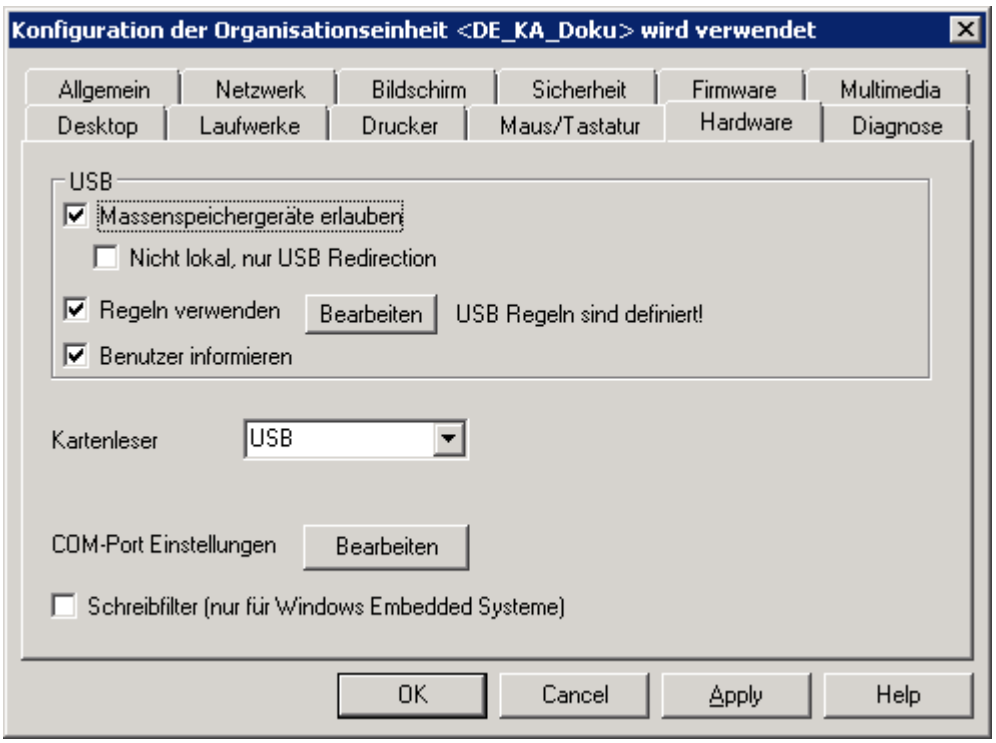
1. Starten Sie am Thin Client den Browser **Firefox**.
2. Öffnen Sie eine beliebige Webseite.
3. Wählen Sie **Datei > Drucken**.

   Der Browser-Dialog **Drucken** *öffnet.*
4. Ändern Sie hier keine Einstellungen, klicken Sie nur auf **OK**.

   Der CUPS-Dialog **Drucken** *öffnet.*
5. Wählen Sie im Listenfeld **Name** den relevanten Drucker (die Auswahl ist abhängig von serverseitigen Einstellungen).
6. Wenn gewünscht, setzen Sie weitere Optionen.
7. Bestätigen Sie mit **OK**.

   Der Druckvorgang beginnt.
8. Bestätigen Sie nach dem Druckvorgang mit **OK**, um den Dialog **Druckinformation** zu schließen.

5.14. Register Hardware



5.14.1. USB-Massenspeicher und Kartenleser

Option	Beschreibung
Massenspeichergeräte erlauben	Erlaubt die Verwendung angeschlossener USB-Massenspeichergeräte grundsätzlich
Nicht lokal, nur USB Redirection[1]	Beschränkt die Verwendung von USB-Massenspeichergeräten auf die USB-Geräteumleitung (USB Redirection) innerhalb einer Verbindung zu einem Backend. Es steht kein Mount-Point zur lokalen Nutzung auf dem eLux-Client zur Verfügung.
Regeln verwenden	Beschränkt die Verwendung von USB-Massenspeichergeräten gemäß definierter USB-Regeln: Die Verwendung von USB-Massenspeichergeräten kann auf Geräte mit einer bestimmten VID (Vendor ID) und/oder PID (Product ID) eingeschränkt werden, beispielsweise auf ein bestimmtes USB-Stick-Modell. Darüber hinaus können die USB-Regeln für andere USB-Geräteklassen wie Smartcard-Reader verwendet werden.
Bearbeiten	Öffnet den Dialog USB-Regeln: Definieren Sie Regeln, um bestimmte Geräte-Modelle explizit zu erlauben oder verweigern.

[1] ab eLux RP 5.4

Option	Beschreibung
Kartenleser	Aktiviert einen Kartenleser auf dem ausgewählten Anschluss
Benutzer informieren	Beim Anschließen eines USB-Massenspeichergerätes wird eine Systray-Meldung angezeigt
COM-Port Einstellungen	Einstellen einzelner COM-Port-Parameter wie Geschwindigkeit, Parität, Stopbits
Schreibfilter (nur Windows Embedded)	Der Benutzer darf keine lokalen Dateien auf seinem Windows Embedded-Client speichern.

Hinweis
Wenn Sie definierte USB-Regeln nutzen, wird die Option **Hardware > USB-Massenspeichergeräte** für Thin Clients mit eLux RP 4 (ab eLux RP Version 4.1) aktiviert und die Nutzung von USB-Massenspeichergeräten ermöglicht. Dies gilt auch, wenn die USB-Regeln ausschließlich Einträge für andere USB-Geräteklassen (beispielsweise Smartcard-Reader) enthalten. Um die Nutzung von USB-Massenspeichergeräten dennoch zu unterbinden, verwenden Sie die USB-Regel: `DENY: CLASS=8`.

Wenn Sie USB-Regeln für eLux 5.4-Clients mit Scout Enterprise Version 14.7 oder älter verwenden möchten, muss die `terminal.ini` einen Eintrag erhalten:

- Definieren Sie für die relevanten Clients in **Erweiterte Konfiguration > Erweiterte Dateieinträge** folgenden Eintrag:

Datei	`/setup/terminal.ini`
Abschnitt	`Global`
Eintrag	`USBUseRules`
Wert	`true`

Für weitere Informationen siehe Erweiterte Dateieinträge.

5.14.2. USB-Regeln definieren

1. Öffnen Sie für die relevante OU oder Gerät **Konfiguration > Hardware > USB > Bearbeiten**.
2. Wählen Sie ein Regelset aus dem Listenfeld unten als Vorlage.
3. Doppelklicken Sie auf die jeweilige Zeile oder markieren Sie die Zeile und drücken F2.
4. Passen Sie die Regel an. Verwenden Sie die Beschreibung der Beispielregeln unten.

   Die Werte für die Hersteller/Vendor-ID (`VID`) und die Produkt-ID (`PID`) finden Sie im **USB-Geräte Info**-Dialog der Taskleiste.

5. Bestätigen Sie mit **OK**.

Beispiele für Regeln

Regel	Code
Nur ein bestimmtes USB-Stick-Modell zulassen	`ALLOW: VID=0781 PID=5151` # USB-Stick-Modell zulassen (Beispiel: SanDisk Cruzer Micro) `DENY: CLASS=08` # Alle Geräte der Klasse MASSENSPEICHER verweigern
Nur ein bestimmtes Smartcard-Modell verweigern	`DENY: VID=18a5 PID=0302` # Smartcard-Modell verweigern (Beispiel: Omnikey CardMan 3821) `ALLOW: CLASS=0B` # Alle Geräte der Klasse SMARTCARD zulassen

Regel	Code
Alle Drucker, Massenspeicher und Smartcard-Geräte verweigern	`DENY: CLASS=07` # Alle Gerate der Klasse DRUCKER verweigern `DENY: CLASS=08` # Alle Geräte der Klasse MASSENSPEICHER verweigern `DENY: CLASS=0B` # Alle Geräte der Klasse SMARTCARD verweigern
Alle Geräte verweigern	`DENY:` # Alle Geräte verweigern

Die Syntax der USB-Regeln entspricht derjenigen der Citrix USB-Richtlinienregeln.

Achtung

Die USB-Regeln wirken auf alle USB-Geräteklassen und somit auch auf die Klasse `03 HID` (Human Interface Devices). Eine Verweigerung der Klasse `03 HID` deaktiviert Tastatur und Maus. Eine Verweigerung aller Klassen (`DENY: # Alle Geräte verweigern`) betrifft am Client auch interne USB-Hubs und Geräte mit herstellerspezifischen Geräteklassen, wie z.B. WLAN-Module. Dies kann bei bestimmten Hardware-Konstellationen zu Problemen in der Startphase des Clients führen. Testen Sie diese Regeloption vor dem Einsatz.

USB-Geräteumleitung konfigurieren

Für Citrix Receiver ab Version 13.x und für VMware Horizon ab Version 4.1 können Sie USB-Filterregeln für die USB-Geräteumleitung definieren.

1. Erfassen Sie die relevanten USB-Filterregeln in den entsprechenden Konfigurationsdateien:

   Citrix USB-Filterregeln:

Konfigurationsdatei	Code (Beispiel)
/setup/ica/usb.conf	`ALLOW: VID=0781 PID=5151` `DENY: CLASS=08`

   VMware USB-Filterregeln:

Konfigurationsdateien	Code (Beispiel)
/setup/elux/.vmware/default-config /setup/elux/.vmware/config /setup/elux/.vmware/view-userpreferences	`viewusb.ExcludeFamily = "storage"` `viewusb.IncludeVidPid = "vid-0781_pid-5151"`

   Die VMware-Filterregeln müssen in allen drei Konfigurationsdateien enthalten sein.

2. Um die Konfigurationsdateien zum Client zu übertragen, verwenden Sie die Scout Enterprise-

Funktion **Konfigurierte Dateiübertragung**. Für weitere Informationen siehe Erweiterte Konfiguration > Dateien.

Nach dem nächsten Neustart der relevanten Clients ist die USB-Geräteumleitung aktiv.

5.14.3. Tastenkombination zum sicheren Entfernen von USB-Geräten

Eingesteckte USB-Massenspeicher-Geräte sollten immer mit der Funktion **Sicher entfernen** entfernt werden, um sicherzustellen, dass alle Daten auf dem USB-Gerät gesichert sind.

Um dem Benutzer diese Funktion zu erleichtern, können Sie eine Tastenkombination definieren, die alle eingesteckten USB-Massenspeicher sicher entfernt:

ALT+WINDOWS-TASTE+S

Die Tastenkombination definieren Sie Sie mit Hilfe der Funktion **Erweiterte Dateieinträge** in der Scout Enterprise-Konsole für die Datei `terminal.ini`:

Datei	`/setup/terminal.ini`
Abschnitt	`Layout`
Eintrag	`UsbUnmountHotKey`
Wert	`<Alt><Mod4><Hyper>s`

Für weitere Informationen siehe Erweiterte Dateieinträge.

5.15. Register Diagnose

Im Register **Diagnose** können Sie die erweiterte Protokollierung am Client ein- oder ausschalten.

Die erweiterte Protokollierung bewirkt, dass im Zuge der Gerätediagnose vordefinierte Skript-Befehle auf dem Client ausgeführt werden und Konfigurations- und Logdateien in größeren Umfang vom Client angefordert werden.

Falls Sie den technischen Support von Unicon benötigen, schalten Sie diese Option ein, bevor Sie Diagnosedateien anfordern.

Die Gerätediagnose wird über ein Online-Kommando ausgeführt, Informationen zur Durchführung erhalten Sie unter Gerätediagnose.

Hinweis
Verwenden Sie die eingeschaltete Protokollierungsstufe ausschließlich als temporäre Gerätekonfiguration. Andernfalls laufen Sie Gefahr, an die Flashspeicher-Kapazitätsgrenze des Thin Clients zu stoßen.

5.16. Problembehandlung

Fehler / Problem	Ursache	Lösung
Bei der Nutzung von USB-MultiMedia-Komponenten (Headset, Webcam) friert der Desktop ein oder das Fenster kann nicht mehr fokussiert werden.	Die Bedienelemente (Einstellknöpfe) der USB-MultiMedia-Komponenten registrieren sich im System als Tastatur- oder Mauskomponenten.	Verhindern Sie die Registrierung als Tastatur- oder Mauskomponenten durch einen Eintrag in der `terminal.ini`. Verwenden Sie die Funktion Erweiterte Dateieinträge der Scout Enterprise-Konsole: Datei: `/setup/terminal.ini` Abschnitt: `Xorg` Eintrag: `IgnoreUsbInput` Wert: `VendorID_1:ProductID_1,VendorID_2:ProductID_2` Beispiel: `0b0e:034c,047f:c01e` Die grundsätzliche Funktionalität der Bedienelemente wird dadurch nicht beeinträchtigt.

Fehler / Problem	Ursache	Lösung
Die Tonwiedergabe von Multimedia-USB-Geräten, die über DisplayPort angeschlossen sind, funktioniert nicht.	Die Tonwiedergabe über DisplayPort ist deaktiviert.	Aktivieren Sie die Tonwiedergabe durch einen Eintrag in der `terminal.ini`. Verwenden Sie die Funktion Erweiterte Dateieinträge der Scout Enterprise-Konsole: Datei: `/setup/terminal.ini` Abschnitt: `Screen` Eintrag: `Radeon.Audio` Wert: `true` Alternativ verwenden Sie ein eigenes Audio-Kabel.
Bei der Nutzung eines Monitors mit Touch-Funktion wird die Position beim Tippen mit dem Finger nur ungenau erkannt.	Der Monitor ist nicht exakt kalibriert.	Um eine Kalibrierung des Monitors durchzuführen, konfigurieren Sie eine benutzerdefinierte Anwendung mit Parameter `calibrator` und starten die Anwendung.
Probleme bei der Grafikdarstellung	Das Feature-Paket für die Hardwarebeschleunigung **HwVideoAccDrivers**[1]) ist nicht installiert.	Aktivieren Sie das **HwVideoAccDrivers**-FPM[2] innerhalb des **XOrg**-Paketes in der Imagedefinitions-Datei.

[1]für eLux RP 5.5 und frühere Versionen: **HwVideoAcc Libraries and Drivers**-FPM
[2]für eLux RP 5.5 und frühere Versionen: **HwVideoAcc Libraries and Drivers**-FPM

Fehler / Problem	Ursache	Lösung

	Die Hardwarebeschleunigung (installiert mit dem **HwVideoAccDrivers**-FPM[1]) wird vom Gerät nicht unterstützt und führt zu Problemen.	Um einzelne Gerätetypen von der Hardwarebeschleunigung auszuschließen[2], erstellen Sie eine Blacklist, die Sie mit der Scout Enterprise-Funktion Dateien auf die Clients übertragen und lokal speichern:
		`/setup/hwaccBlacklist`
		Listen Sie in der Textdatei `hwaccBlacklist` die relevanten Gerätetypen, ein Gerätetyp pro Zeile. Die Bezeichnung für den Gerätetyp muss der Zeichenfolge entsprechen, die im Eigenschaften-Fenster in der Scout Enterprise-Konsole unter **Hardwareinformation > Inventar > Typ** angezeigt wird.
		Beispiel:
		`FUTRO S920`
		`D3314-B1`
		`HP t620 Dual Core TC`
		Für alle in der Blacklist aufgeführten Gerätetypen wird die Hardwarebeschleunigung deaktiviert.

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

[1] für eLux RP 5.5 und frühere Versionen: **HwVideoAcc Libraries and Drivers**-FPM
[2] für eLux RP 5.6 und spätere Versionen

6. Erweiterte Konfiguration

Die Einstellungen der Geräte-Konfiguration, die Sie entweder in der Basis-Konfiguration oder für bestimmte OUs bzw. Geräte festgelegt haben, können Sie in der **Erweiterten Konfiguration**

- für einzelne Geräte oder OUs überschreiben
- um weitere spezifische Optionen ergänzen.

Erweiterte Konfiguration aufrufen

- Wählen Sie im Scout Enterprise-Menü **Optionen > Erweiterte Optionen**, um die Konfiguration für alle Geräte zu überschreiben oder zu ergänzen.
- Öffnen Sie das Kontextmenü für die relevante OU oder Gerät und wählen Sie den Eintrag **Erweiterte Einstellungen...**, um die Konfiguration dieser OU/dieses Geräts zu überschreiben oder zu ergänzen.

Hinweis
Auch die Erweiterte Konfiguration verwendet das Vererbungsprinzip. Die Option **Übergeordnete Erweiterte Konfiguration verwenden** ist standardmäßig aktiv, kann jedoch für einzelne Register innerhalb einer Ebene deaktiviert werden.

6.1. Geräte

– nur global für alle Geräte (**Optionen > Erweiterte Optionen**) verfügbar –

Option	Beschreibung
Maximale Pingzeit (Millisekunden)	Maximale Antwortzeit des Clients auf einen `ping`-Befehl
Maximale Suchzeit (Sekunden)	Maximale Gesamtdauer für die zu suchenden Geräte, bis Discovery abgebrochen wird.
Nur gesperrte Felder werden am Client aktualisiert	Nicht gesperrte Felder sind zur lokalen Benutzerkonfiguration freigegeben und werden nicht von Scout Enterprise überschrieben. Beim nächsten Laden der Konfiguration werden nur die über **Setup > Sicherheit** gesperrten Felder aktualisiert. Für weitere Informationen siehe Individuelle Konfiguration schützen.
	Hinweis Nach fehlerhafter Konfiguration des Benutzers können Sie dennoch alle Konfigurations-Werte überschreiben lassen, indem Sie in der Scout Enterprise-Konsole ein Flag für dieses Gerät setzen. Für weitere Informationen siehe Individuelle Konfiguration schützen.

Option	Beschreibung
Standard-OU	OU, in die neue Geräte standardmäßig eingeordnet werden
OU von Geräten durch OU-Filter festlegen	Aktiviert den OU-Filter für neue Geräte Klicken Sie auf die Schaltfläche **...**, um den OU-Filter zu konfigurieren. Der OU-Filter hat Priorität gegenüber anderen Verfahren, kann aber für einzelne Geräte ignoriert werden. Für weitere Informationen siehe OU-Filter.
Neue Geräte deaktivieren	Deaktiviert neu hinzugefügte Clients
Automatischen Gruppenwechsel von Geräten erlauben	Erlaubt die automatische Zuordnung von Geräten über DHCP
Nur bekannte Geräte akzeptieren	Der Scout Enterprise-Server nimmt nur neue Geräte mit bekannter MAC-Adresse an. Für weitere Informationen siehe Geräteprofil reservieren.
Immer den Client-Hostnamen als Gerätenamen übernehmen	Der Gerätename kommt vom Client und kann in Scout Enterprise-Konsole nicht (dauerhaft) geändert werden.
Bei doppelten Namen den existierenden Eintrag ändern	Bei der Eintragung eines neuen Gerätes mit gleichem Namen, wird der Name des vorhandenen Gerätes und nicht der Name des neuen Gerätes geändert.
Namensschablone	Namensschablone für neu hinzugefügte Clients Kann für einzelne OUs überschrieben werden (**Erweiterte Konfiguration > Management**)
Namensschablone nur für neue Geräte anwenden	Namensschablone wird nicht beim Verschieben oder Umziehen von Geräten angewendet

6.2. Update

– nicht für einzelne Geräte verfügbar –

Option	Beschreibung
Maximale Anzahl paralleler Updates	Beschränkung der Geräte die gleichzeitig aktualisiert werden (Performance)
Maximale Dauer für den Verbindungsaufbau	Zeit für den Verbindungsaufbau, bevor das nächste Gerät herangezogen wird

Hinweis
Die optimalen Werte sind systemspezifisch.

6.3. Wake On LAN

– nur global für alle Geräte (**Optionen > Erweiterte Optionen**) verfügbar –

Mit Wake On LAN können ausgeschaltete Thin Clients über Scout Enterprise eingeschaltet werden.

Hierzu sendet der Scout Enterprise-Server ein sogenanntes Magic Packet, welches von der Netzwerkkarte der ausgeschalteten Thin Clients entsprechend erkannt wird (Voraussetzung: Wake On LAN wird vom Thin Client unterstützt und ist im Geräte-BIOS konfiguriert).

Der Versand des Magic Packet für Wake On LAN erfolgt als Broadcast (UDP, eLux Port 20000 eingehend/ausgehend) innerhalb des eigenen Netzsegments und kann nicht über Subnetzgrenzen hinweg erfolgen. Um trotzdem Thin Clients in entfernten Subnetzen einschalten zu können, stehen die folgenden Alternativen zur Verfügung:

Integrierter eLux RP Wake On LAN-Server

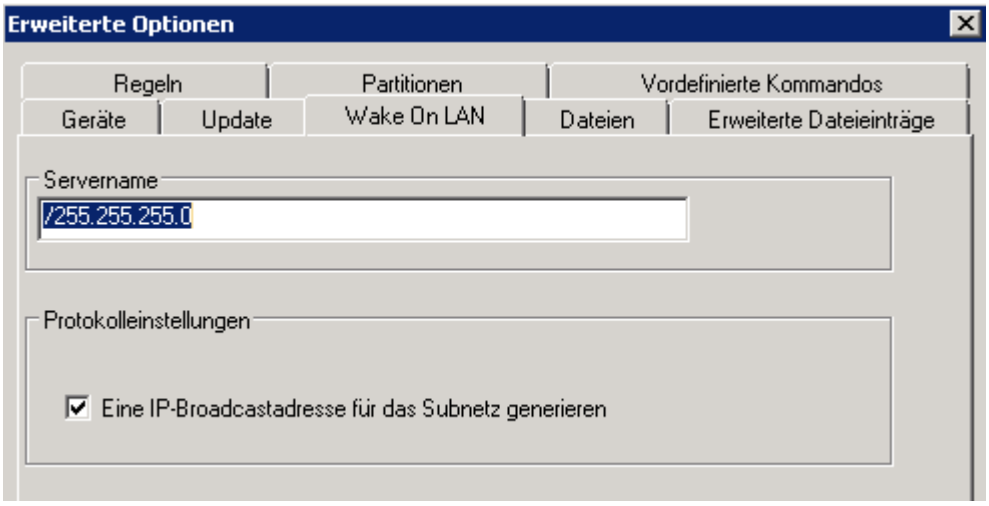
Der Scout Enterprise-Server prüft immer, ob im Subnetz des einzuschaltenden Thin Clients ein eingeschalteter Thin Client vorhanden ist. In diesem Fall übermittelt der Scout Enterprise-Server einen Wake On LAN-Auftrag mit der MAC-Adresse des einzuschaltenden Thin Clients via IP an den eingeschalteten Thin Client. Dieser agiert als Wake On LAN-Server, erstellt ein entsprechendes Magic Packet mit der MAC-Adresse des einzuschaltenden Thin Clients und versendet das Magic Packet für Wake On LAN als Broadcast (UDP) innerhalb seines Subnetzes.

Die Funktionalität des Wake On LAN-Servers ist integraler Bestandteil von eLux RP und muss nicht gesondert konfiguriert werden.

Gerichteter Subnetz-Broadcast

Über einen gerichteten Subnetz-Broadcast kann das zugehörige Subnetz des einzuschaltenden Thin Clients direkt via IP mit dem Broadcast adressiert werden. Die Ermittlung der IP-Broadcastadresse des Subnetzes erfolgt aus der IP-Adresse des Thin Clients über eine zu konfigurierende Subnetzmaske. Das Magic Packet für Wake On LAN wird ausschließlich innerhalb des adressierten Subnetzes als Broadcast (UDP) versendet.

Die Nutzung einer IP-Broadcastadresse für das Subnetz muss als globale Einstellung konfiguriert werden.



Diese Option ist nur in der Erweiterten Basiskonfiguration verfügbar.

Option	Beschreibung
Servername	Subnetzmaske für gerichtete Subnetz-Broadcasts (für frühere Versionen: IP-Adresse des Wake On LAN-Servers –auch verfügbar in den Erweiterten Optionen für Geräte und OUs)
Eine IP-Broadcastadresse für das Subnetz generieren (nur global konfigurierbar)	Das Paket wird an das zugehörige Subnetz (dedicated subnet) geschickt. Die Option erfordert die Eingabe der Subnetzadresse in das Feld **Servername** im Format `/255.255.255.0` (Beachten Sie den führenden Slash). Beispiel: Um ein Gerät mit der IP-Adresse `192.168.10.44` aufzuwecken, tragen Sie `/255.255.255.0` in das Feld **Servername** ein. Daraus generiert Scout Enterprise die IP-Broadcastadresse `192.168.10.255` für das Subnetz. Standardmäßig ist die Option deaktiviert.

6.4. VPN

– nur für einzelne Geräte verfügbar –

Hinweis

Das Register **VPN** ist nur in den **Erweiterten Einstellungen** eines Gerätes und nicht für ganze OUs verfügbar.

Scout Enterprise unterstützt die folgenden VPN (Virtual Private Network)-Clients zur Kommunikation über eine sichere Verbindung:

- Cisco AnyConnect
- VPNC (nur für eLux RP Version 4)
- OpenVPN

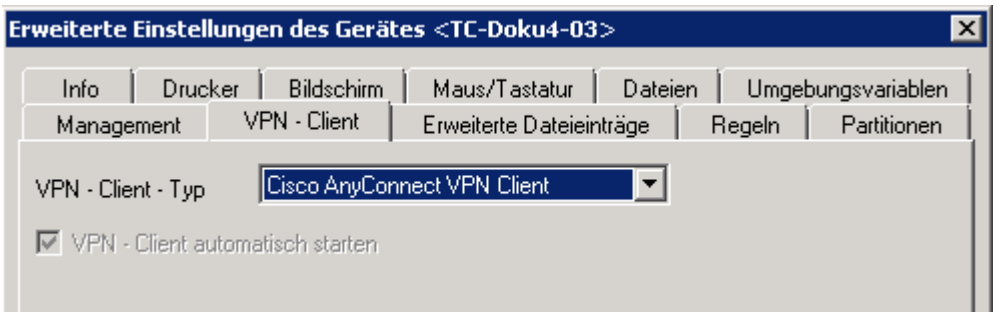
Abhängig vom eingesetzten VPN-Client muss eine entsprechende Konfigurationsdatei auf dem Client vorhanden sein. Die Konfigurationsdatei können Sie über die Scout Enterprise-Funktion Erweiterte Dateieinträge bearbeiten.

6.4.1. Cisco AnyConnect einrichten

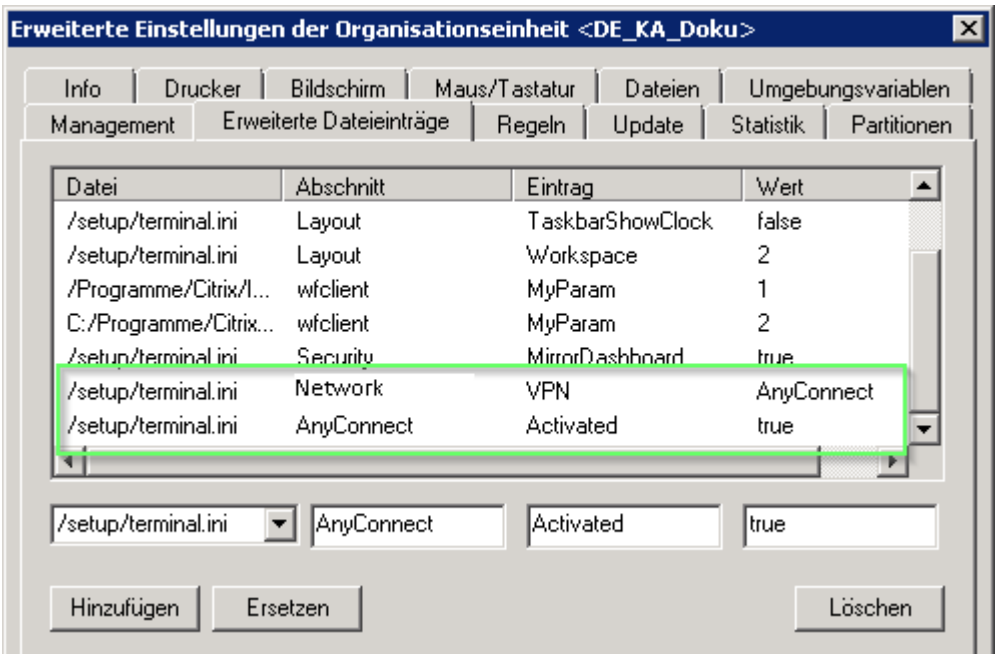
Voraussetzung

Die IDF-Datei muss das Software-Paket **vpnsystem-***x* enthalten und im Paket muss die Komponente **Cisco AnyConnect** aktiviert sein. Für weitere Informationen siehe IDF erstellen im ELIAS-Handbuch.

1. Wenn Sie Cisco AnyConnect für ein einzelnes Gerät konfigurieren möchten, klicken Sie mit der rechten Maustaste auf das relevante Gerät, wählen **Erweiterte Einstellungen > VPN-Client** und wählen `Cisco AnyConnect VPN Client` aus dem Listenfeld.



2. Wenn Sie Cisco AnyConnect für eine OU konfigurieren möchten, öffnen Sie für die relevante OU **Erweiterte Einstellungen > Erweiterte Dateieinträge**, und setzen folgende Einträge für die `terminal.ini`:



Die Clients der relevanten OU erhalten die Cisco AnyConnect-Konfiguration über die `terminal.ini`.

3. Um die Übertragung der benötigten Zertifikate zu konfigurieren, öffnen Sie für den Client oder die OU **Erweiterte Einstellungen > Dateien**. Tragen Sie Quelldatei und Zieldatei mit Zielpfad `/setup/cacerts/ca` ein.

Hinweis
Die Zertifikate, die vom VPN-Server übertragen werden, liegen unter `/setup/cacerts/client`.

4. Führen Sie zweimal einen Neustart der relevanten Clients durch. (Die Clients benötigen einen zweiten Neustart, um die VPN-Konfiguration lokal zu aktivieren.)

   Der Cisco AnyConnect-Dialog öffnet. Der Dialog kann auch aus einer Shell über `vpnui` oder als lokale benutzerdefinierte Anwendung geöffnet werden.

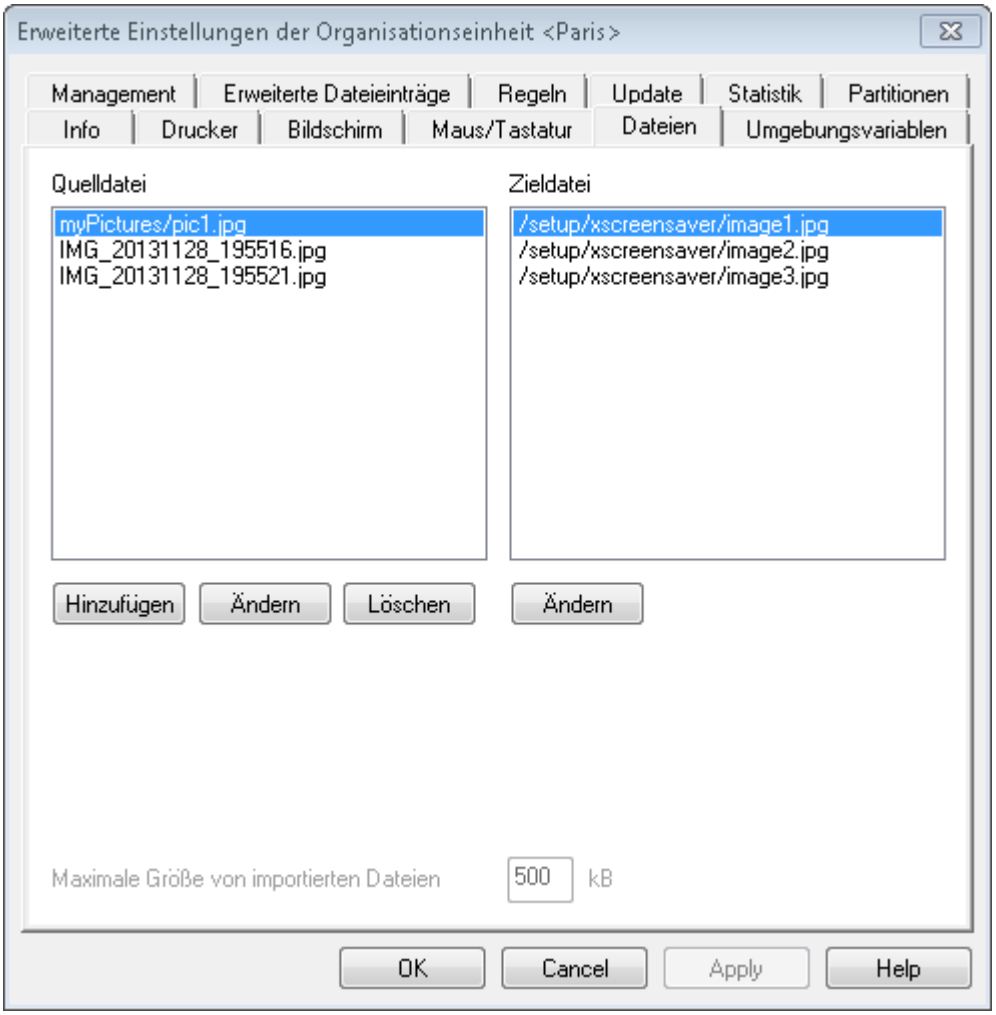
5. Geben Sie die Adresse des Cisco Backends ein und klicken Sie auf **Connect**.

Hinweis
Optional können Sie eine Konfigurationsdatei für AnyConnect erstellen oder von einem Referenz-Client kopieren, die Sie anschließend über die **Dateien**-Funktion der Scout Enterprise-Konsole nach `/setup/elux/.anyconnect` übertragen.

6.5. Konfigurierte Dateiübertragung

Mit dieser Scout Enterprise-Funktion können Sie Dateien auf den Client übertragen. Sie können Dateien für alle Geräte, einzelne Geräte oder OUs definieren, die beim nächsten Neustart in das angegebene Verzeichnis auf den Client übertragen werden.

Die Quelldateien können im Dateisystem referenziert werden oder in die Scout Enterprise-Datenbank importiert werden.



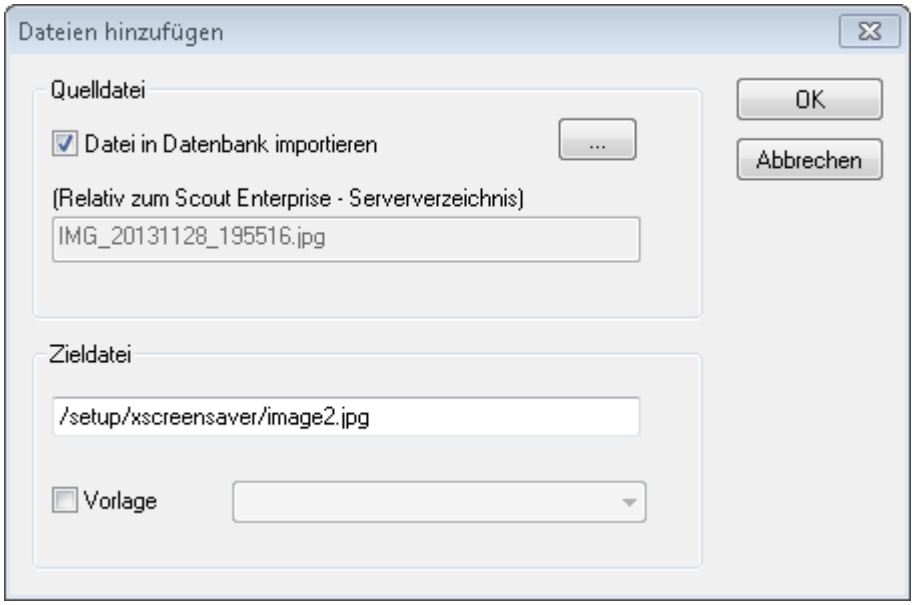
Beispiel: Sie möchten eine oder mehrere Bilddateien als Bildschirmschoner auf die Clients kopieren.

Dateien für den Transfer definieren

1. Wenn Sie Dateien für alle Geräte definieren möchten (globale Dateiliste), wählen Sie **Optionen > Erweiterte Konfiguration**.
   Wenn Sie Dateien für eine OU oder ein Gerät definieren möchten (individuelle Dateiliste), öffnen Sie für die relevante OU oder Gerät das Kontextmenü und wählen Sie den Eintrag **Erweiterte Konfiguration...**

Hinweis
Eine individuelle Dateiliste dominiert die globale Dateiliste.

2. Wählen Sie das Register **Dateien**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.



*Der Dialog **Dateien hinzufügen** öffnet.*

4. Schalten Sie unter **Quelldatei** die Option **Datei in Datenbank importieren** ein, klicken Sie auf die Schaltfläche **...** und wählen Sie die relevante Datei aus dem Dateisystem.
   Oder:
   Geben Sie den Dateinamen der Quelldatei inklusive Pfad relativ zum Scout Enterprise Server-Verzeichnis (`...\UniCon\Scout\Server`) in das Textfeld unter **Quelldatei** ein.

Hinweis
In die Datenbank importierte Dateien werden automatisch beim SQL-Datenbank-Backup mitgesichert.
Für im Dateisystem referenzierte Dateien besteht die Möglichkeit, den Inhalt der Dateien unter Beibehaltung des Namens dynamisch zu ändern.

5. Passen Sie unter **Zieldatei** Pfad und Dateinamen an, so wie die Datei am Client gespeichert werden soll.

   Der Dateiname auf dem Thin Client muss nicht mit dem der Quelldatei identisch sein.

6. Bestätigen Sie mit **OK**.

Quelle und Ziel sind definiert. Der Dateitransfer erfolgt beim nächsten Bootvorgang der Clients.

Ein erneuter Dateitransfer erfolgt nur, wenn sich an der Konfiguration der Dateien oder den Dateien selbst etwas ändert.

6.6. Erweiterte Dateieinträge

Mit Hilfe des Registers **Erweiterte Dateieinträge** können Sie Parameter definieren, die nicht über eine graphische Oberfläche gesetzt werden können, z.B. spezielle Parameter für Citrix ICA Client-Konfigurationsdateien.

Voraussetzung ist, dass die Konfigurationsdatei im Format `.ini` vorliegt.
Desweiteren stellt der `INI`-Dateieditor in Scout Enterprise folgende Anforderungen:

- Eine .ini-Datei besteht aus mindestens einem Abschnitt. Jeder Abschnitt besteht aus null oder mehreren Schlüsselwörtern. Diese enthalten wiederum null oder mehrere Werte.
- Ein Abschnitt wird durch einen symbolischen Namen, der in eckige Klammern gefasst ist, eingeleitet.
- Jedes Schlüsselwort und der zugehörige Wert stehen in jeweils einer Zeile. Schlüsselwort und Wert sind durch ein Gleichheitszeichen (=) voneinander getrennt.
  Ein Schlüsselwort kann mehr als einen Wert haben.
- Wenn ein Abschnittsname in einer Datei mehrfach verwendet wird, oder wenn ein Schlüsselwort in einem Abschnitt mehrfach verwendet wird, dominiert der letzte Eintrag.

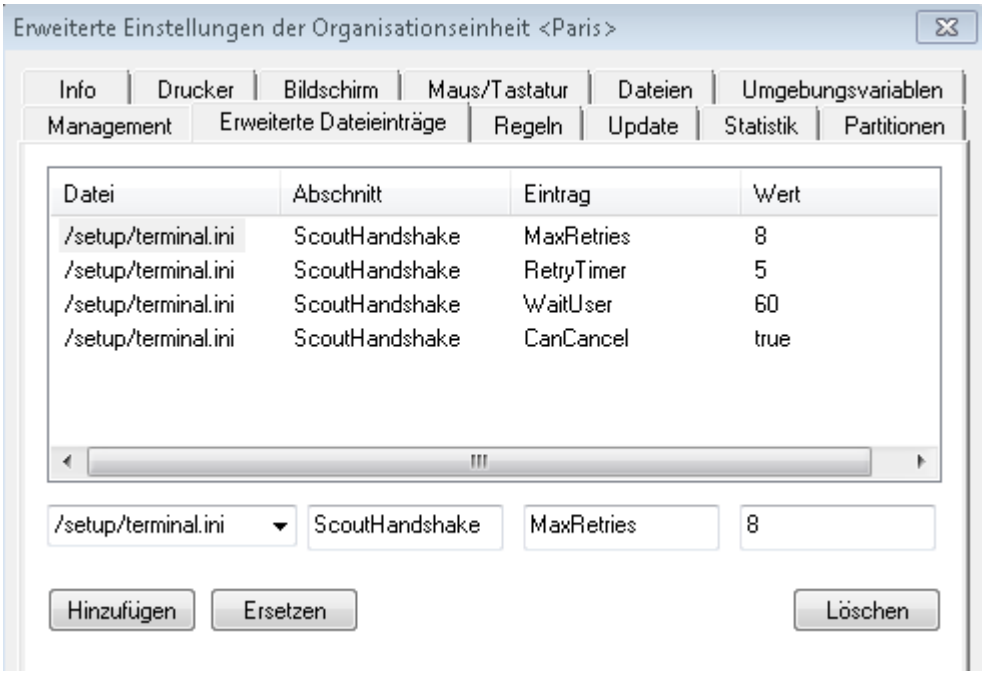
6.6.1. Individuelle Dateieinträge festlegen

1. Wählen Sie in der Scout Enterprise-Konsole **Optionen > Erweiterte Optionen**.
   Oder:
   Öffnen Sie für die entsprechende OU bzw. Gerät das Kontextmenü und wählen Sie **Erweiterte Einstellungen ...**
2. Wählen Sie das Register **Erweiterte Dateieinträge**.
3. Füllen Sie die Felder folgendermaßen aus:

Option	Beschreibung
Datei	Tragen Sie den vollständigen Pfad und Namen der zu bearbeitenden Datei ein oder wählen Sie aus der Dropdown-Liste: Citrix ICA: `/setup/ica/wfclient.ini` und `/setup/ica/appsrv.ini` Terminal: `/setup/terminal.ini`
Abschnitt	Abschnittsüberschrift ohne Klammern
Eintrag	Schlüsselwort
Wert	Der dem Schlüsselwort zuzuordnende Wert. Leerzeichen, Trennzeichen und mehrfache Werte sind erlaubt. Beispiel: `WertA,WertB,WertC;Kommentar`

4. Klicken Sie auf **Hinzufügen**.

Die neuen Einträge werden beim nächsten Neustart in die .ini-Datei des Clients geschrieben.



6.6.2. Werte für individuelle Dateieinträge ändern

1. Markieren Sie in **Erweitere Konfiguration > Erweiterte Dateieinträge** den Eintrag, deren Wert Sie ändern möchten.
2. Ersetzen Sie unten im Feld **Wert** den vorhanden Wert.
3. Klicken Sie auf **Ersetzen**.

Die neuen Werte werden beim nächsten Neustart in die .ini-Datei des Clients geschrieben.

6.6.3. Individuelle Dateieinträge löschen

1. Definieren Sie in **Erweitere Konfiguration > Erweiterte Dateieinträge** einen neuen Eintrag: Geben Sie **Datei**, **Abschnitt** und **Eintrag** des zu löschenden Eintrages ein, aber lassen Sie das Feld **Wert** leer.
2. Klicken Sie auf **Hinzufügen**.

Der "leere" Dateieintrag überschreibt frühere Anweisungen. Der Eintrag wird beim nächsten Neustart des Clients aus dem entsprechenden Abschnitt gelöscht.

Hinweis
Wenn Sie eine markierte Zeile mit der Schaltfläche **Löschen** aus der Liste löschen, bedeutet das lediglich, dass Scout Enterprise diesen Eintrag nicht mehr am Client aktualisiert.

6.6.4. Gesamte Abschnitte löschen

1. Definieren Sie in **Erweitere Konfiguration > Erweiterte Dateieinträge** einen neuen Eintrag: Geben Sie **Datei** und **Abschnitt** des zu löschenden Abschnitts ein, aber lassen Sie die Felder **Eintrag** und **Wert** leer.
2. Klicken Sie auf **Hinzufügen**.

Der "leere" Abschnitt überschreibt frühere Anweisungen. Der komplette Abschnitt wird beim nächsten Neustart des Clients aus der Datei gelöscht, unabhängig davon ob er Dateieinträge enthalten hat.

6.7. Regeln

In diesem Register definieren Sie Regeln, die beim Beenden der letzten Anwendung oder beim ersten Kontakt mit Scout Enterprise ausgeführt werden.

Option	Beschreibung
Nach dem Beenden der letzten Anwendung folgende Aktion durchführen	Wählen Sie eine Option aus dem Listenfeld
Am Gerät eine Meldung für [] einblenden	Geben Sie eine Zeitspanne in Sekunden ein, um den Beutzer zu informieren
Beim ersten Kontakt mit dem Manager folgende Aktion durchführen	Wählen Sie `Update durchführen`, um sicherzustellen, dass neue Geräte sofort auf dem aktuellen Software-Stand sind

Hinweis
Für OUs und Geräte ist die Option `Übergeordnete Aktion verwenden` standardmäßig aktiv.

6.8. Umgebungsvariablen

– nur für einzelne Geräte und OUs verfügbar –

Umgebungsvariablen können lokal am Client eingesetzt werden und enthalten Zeichenketten.

Umgebungsvariable definieren

1. Klicken Sie auf die Schaltfläche **Neu**.
2. Geben Sie eine Variable in folgendem Format ein:
   `Variablenname=Wert`
   und bestätigen Sie mit **OK**.

   Die neue Variable wird in der Liste angezeigt.
3. Wenn Sie den Wert der Variable verschlüsseln möchten, klicken Sie mit der rechten Maustaste auf die Variable und wählen im Kontextmenü **Wert verschlüsseln**.

Hinweis
Bei Verwendung der Variablen muss der Variablenname mit einem Dollarzeichen eingeleitet werden: `$<Variablenname>`.

7. Anwendungsdefinition

Den Clients können folgende Anwendungen zur Verfügung gestellt werden:

- Anwendungen zur Anbindung an ein Backend-System
- lokale Anwendungen

Anwendungsdefinitionen und Software werden unabhängig voneinander bereitgestellt. Mit der Anwendungsdefinition definieren Sie die dem Anwender zur Verfügung gestellten Anwendungen. Damit der Anwender diese nutzen kann, müssen die entsprechenden Software-Pakete auf dem Client über das in ELIAS konfigurierte IDF installiert sein. Für weitere Informationen siehe IDF erstellen im ELIAS-Handbuch.

Hinweis
Der Begriff **Anwendungen** bezeichnet im folgenden Anwendungsdefinitionen.
Der Begriff **Software** bezeichnet die erforderlichen Software-Pakete.

Anwendungen können von oben nach unten vererbt werden. Die niedrigste Ebene zur Definition einer Anwendung ist eine OU, die höchste Ebene ist ganz oben oberhalb der Top-Level-OUs (Basis-Anwendungen).

7.1. Allgemeines

7.1.1. Anwendung hinzufügen

1. Klicken Sie in der Organisationsstruktur unterhalb der gewünschten OU mit der rechten Maustaste auf **Anwendungen**.
2. Wählen Sie im Kontextmenü **Hinzufügen...**.

*Der Dialog **Anwendungs-Eigenschaften** öffnet. Der Dialog enthält für jeden Anwendungstyp ein eigenes Register.*

Folgende Optionen sind in den **Anwendungseigenschaften** vieler Anwendungen verfügbar:

Option	Beschreibung
Name dieser Anwendung	Name für die Anwendung, wird in der Scout Enterprise-Konsole angezeigt **Hinweis** Anwendungen werden durch ihren Namen identifiziert. Sie müssen eindeutig sein, um Konflikte zu vermeiden.

Option	Beschreibung
Anzeigename (optional)[1]	Name für die Anwendung, wird am Client angezeigt (Systemsteuerung, Startmenü)
Server	Name des Servers, mit dem sich die Anwendung verbindet
Anmeldung	Die Anmeldung des Benutzers am Terminal-Server erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).
Passthrough-Anmeldung	Die Werte der lokalen Benutzervariablen `$ELUXUSER`, `$ELUXPASSWORD` und `$ELUXDOMAIN` werden zur Anmeldung am Authentifizierungsserver verwendet. Dadurch können die Anmeldedaten einer AD-Anmeldung auf dem eLux Desktop zur automatischen Anmeldung für die konfigurierten Anwendungen genutzt werden (Single Sign-On). Für weitere Informationen siehe Benutzervariablen.
Dauerbetrieb	Die Anwendung wird sofort wieder gestartet, nachdem sie unerwartet oder durch einen Benutzer beendet wurde.
Automatisch starten nach	Die Anwendung wird automatisch gestartet, nachdem eLux hochgefahren ist. Optional können Sie die Anzahl der Sekunden angeben, um die der Anwendungsstart verzögert werden soll.
Desktop-Symbol	Für die Anwendung wird eine zusätzliche Verknüpfung auf dem Desktop angelegt (Symbol und Anzeigename). Ausnahme: PNAgent
Freie Parameter	Individuelle Parameter zum Starten einer Anwendung

Hinweis
Sie können Anwendungsdefinitionen außerdem

- zwischen OUs kopieren
- aus einer OU in eine Datei exportieren und in eine andere OU importieren (Kontextmenü > **Bearbeiten**).

7.1.2. Anwendungseigenschaften bearbeiten

- Öffnen Sie für die relevante Anwendung das Kontextmenü und wählen Sie **Eigenschaften...**.

*Der **Anwendungseigenschaften**-Dialog für diese Anwendung öffnet. Je nach Anwendung sind unterschiedliche Eigenschaften konfigurierbar.*

Hinweis
Die Eigenschaften einer markierten Anwendung können Sie in der Scout Enterprise-Konsole im **Eigenschaften**-Fenster (**Ansicht > Fenster > Eigenschaften**) anzeigen, aber nicht bearbeiten.

[1] ab Scout Enterprise Management Suite Version 14.7

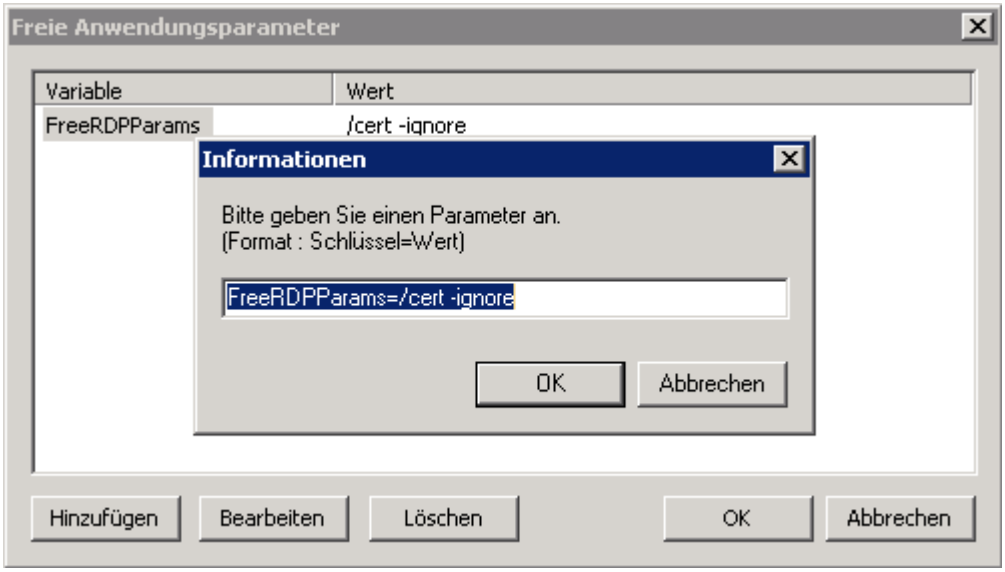
7.1.3. Freie Anwendungsparameter definieren

Freie Anwendungsparameter sind individuelle Parameter, die zum Starten einer Anwendung verwendet werden können. Freie Anwendungsparameter können Sie für alle Anwendungen außer SAP-GUI und Emulation definieren.

1. Öffnen Sie die **Anwendungseigenschaften** der relevanten Anwendung.
2. Klicken Sie auf die Schaltfläche **Freie Parameter**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**, geben Sie den relevanten Parameter im vorgegebenen Format ein und bestätigen Sie mit **OK**.

   Der neue Parameter wird gespeichert und im Dialog angezeigt.
4. Um einen weiteren Parameter zu definieren, wiederholen Sie den letzten Schritt.
5. Bestätigen Sie mit **OK**.

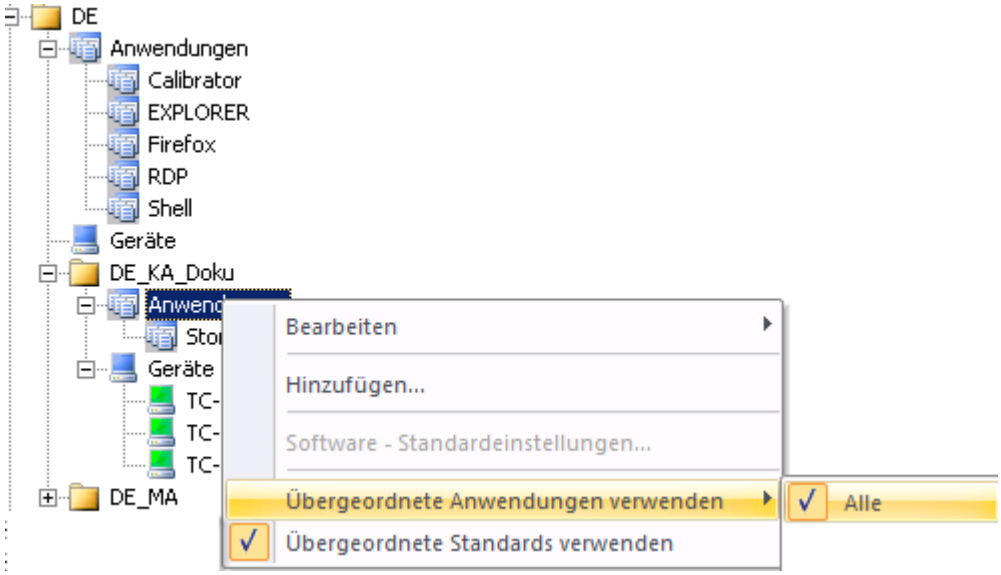
Scout Enterprise fügt die definierten Parameter in die `\setup\sessions.ini`*-Datei für die entsprechende Anwendung ein.*



7.1.4. Verwendung übergeordneter Anwendungen

Standardmäßig werden Anwendungen in untergeordnete OUs vererbt. Damit können Sie Anwendungen an wenigen Stellen zentral definieren.

Für die untergeordneten OUs ist in der Baumstruktur im **Anwendungen**-Kontextmenü die Option **Übergeordnete Anwendungen verwenden > Alle** eingeschaltet (Haken gesetzt). Damit sind alle Anwendungen aktiv, die in einer übergeordneten OU oder auf oberster Ebene definiert wurden. Zusätzlich können für die OU selbst Anwendungen definiert werden, die in dieser OU (und in untergeordneten OUs) aktiv sind.



Vererbung von Anwendungen ausschalten

1. Öffnen Sie für die OU, die keine Anwendungen von oben erhalten soll, das Kontextmenü.
2. Wählen Sie **Übergeordnete Anwendungen verwenden > Alle**, um den Haken zu entfernen.

Die OU verwendet keine übergeordneten Anwendungen und kann keine übergeordneten Anwendungen weitervererben. Nur Anwendungen, die innerhalb der OU definiert sind, sind aktiv.

Vererbung auf bestimmte Anwendungen beschränken

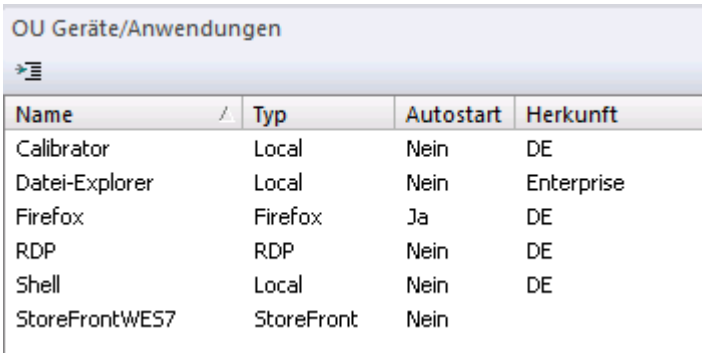
1. Öffnen Sie für die OU, die einen Teil der Anwendungen von oben erhalten soll, das Kontextmenü.
2. Stellen Sie sicher, dass die Option **Übergeordnete Anwendungen verwenden > Alle** ausgeschaltet ist (kein Haken).
3. Wählen Sie im Untermenü **Übergeordnete Anwendungen verwenden** unterhalb von **Alle** die Anwendung, die Sie von oben übernehmen möchten.

Die gewählte Anwendung erhält im Untermenü einen Haken und die Anwendungsdefinition wird den Clients dieser OU nach dem nächsten Neustart zur Verfügung gestellt.

Definierte Anwendungen für eine OU anzeigen

1. Wählen Sie **Ansicht > Fenster > OU Geräte/Anwendungen**, um das entsprechende Fenster anzuzeigen.
2. Markieren Sie in der Baumstruktur das **Anwendungen**-Symbol unterhalb einer OU.

*Für die gewählte OU werden alle definierten Anwendungen gelistet. In der Spalte **Herkunft** wird die OU angezeigt, aus der eine Anwendung vererbt wird. Basis-Anwendungen auf der obersten Ebene zeigen den Wert* `Enterprise`.



Name	Typ	Autostart	Herkunft
Calibrator	Local	Nein	DE
Datei-Explorer	Local	Nein	Enterprise
Firefox	Firefox	Ja	DE
RDP	RDP	Nein	DE
Shell	Local	Nein	DE
StoreFrontWES7	StoreFront	Nein	

In der Abbildung hat die ausgewählte OU eine eigene Anwendung (kein Eintrag bei **Herkunft**, vier Anwendungen aus der übergeordneten OU **DE** und eine Basis-Anwendung.

Hinweis
Auch die Standardeinstellungen können über das Anwendungen-Kontextmenü mit **Übergeordnete Standards verwenden** vererbt werden.

7.1.5. Standardeinstellungen für Anwendungen setzen

Standardeinstellungen können für alle Anwendungen eines Typs zentral oder wahlweise pro OU definiert werden. Standardeinstellungen sind für die Citrix-Anwendungen (Citrix Receiver) und für die Browser[1] verfügbar.

Wir empfehlen, die Standardeinstellungen auf der obersten Ebene (Basis-Anwendungen) zu setzen und weiter zu vererben.

1. Öffnen Sie in der Baumstruktur für die relevante Ebene das Kontextmenü der **Anwendungen** und wählen Sie den Eintrag **Software-Standardeinstellungen...**.

   Hinweis
   Wenn die Vererbung eingeschaltet ist, können Sie nur die **Software-Standardeinstellungen...** der übergeordneten (vererbenden) Instanz öffnen und anpassen. Um die Vererbung aufzubrechen, muss im **Anwendungen**-Kontextmenü die Option **Übergeordnete Standards verwenden** ausgeschaltet werden.

2. Wählen Sie im Listenfeld die gewünschte Software und klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie die relevanten Optionen im jeweiligen Register und bestätigen Sie mit **Übernehmen**.

7.1.6. Anwendungen von Client zu Scout Enterprise hochladen

Die Anwendungsdefinitionen eines Referenz-Clients mit aktueller eLux-Version können in die Scout Enterprise-Konsole hochgeladen und einer beliebigen OU zugeordnet werden.

[1] ab Scout Enterprise Management Suite Version 15.0

Achtung

Wenn Sie Anwendungen in eine OU hochladen, werden alle vorher definierte Anwendungen in der OU gelöscht.

Upload von beliebigem Client

1. Wählen Sie in Scout Enterprise den Menübefehl **Datei > Anwendungs-Upload...**.

   *Der Dialog **Anwendungs-Upload** öffnet.*

2. Geben Sie IP-Adresse oder Namen des Thin Clients ein, dessen Anwendungsdefinitionen Sie hochladen möchten.
3. Wählen Sie die **Ziel**-OU, in die die Anwendungsdefinitionen kopiert werden sollen.
4. Klicken Sie auf **Start**.

Die Anwendungsdefinitionen des angegebenen Clients (bzw. seiner OU) werden in die ausgewählte OU hochgeladen. Bereits vorhandene Anwendungen werden gelöscht.

Upload von verwaltetem Client in Scout Enterprise Management Suite

1. Markieren Sie in der Scout Enterprise-Konsole den Thin Client, dessen Anwendungsdefinitionen Sie hochladen möchten.
2. Wählen Sie den Menübefehl **Datei > Anwendungs-Upload...**.

   *Der Dialog **Anwendungs-Upload** öffnet. Die IP-Adresse des ausgewählten Gerätes wird bereits im Feld **IP-Adresse oder Name des Gerätes** angezeigt.*

3. Wählen Sie die **Ziel**-OU, in die die Anwendungsdefinitionen kopiert werden sollen.
4. Klicken Sie auf **Start**.

Die Anwendungsdefinitionen des angegebenen Clients (bzw. seiner OU) werden in die ausgewählte OU hochgeladen. Bereits vorhandene Anwendungen werden gelöscht.

7.1.7. Anwendungssymbol definieren

Sie können eigene Anwendungssymbole definieren, um sie am Client-Desktop anzuzeigen. Als Symboldateien werden Dateien vom Typ `XPM`, `ICO` und `GIF` unterstützt.

1. Öffnen Sie in der Baumstruktur das **Anwendungen**-Kontextmenü der obersten Ebene.
2. Wählen Sie den Eintrag **Anwendungssymbole definieren...**
3. Klicken Sie auf **Hinzufügen** und wählen Sie die relevante Symboldatei aus dem Dateisystem.
4. Bestätigen Sie mit **Öffnen** und **OK**.

Das neue Anwendungssymbol wird im Dialog angezeigt. Das Symbol ist definiert, aber noch nicht zugewiesen.

Anwendungssymbol zuweisen

7.1.8. Benutzerdefiniertes Anwendungssymbol zuweisen

Voraussetzung

Bevor Sie ein benutzerdefiniertes Anwendungssymbol zuweisen können, muss es in Scout Enterprise definiert sein. Für weitere Informationen siehe Anwendungssymbol definieren.

1. Öffnen Sie für die relevante Anwendung das Kontextmenü und wählen Sie **Eigenschaften...**
2. Aktivieren Sie die Option **Desktopsymbol**.
3. Klicken Sie auf die Schaltfläche **...** und markieren Sie das gewünschte Symbol.
4. Bestätigen Sie mit **OK** und **Übernehmen.**

Das Anwendungssymbol wird beim nächsten Client-Neustart für die ausgewählte Anwendung angezeigt.

7.2. Verbindung zu einer Citrix-Farm

Benutzer können sich zu Sitzungen verbinden, die auf einem Citrix-Backend laufen. Sobald die Verbindung hergestellt ist, kann der Benutzer veröffentlichte Desktops und Anwendungen verwenden.

Die Verbindung vom Thin Client zu einem Citrix-Backend erfolgt über eine Anwendung:

- über eine StoreFront-Anwendung auf einen StoreFront-Server
- über die Citrix Self-Service-Benutzeroberfläche auf einen StoreFront-Server
- per Browser-Sitzung auf einen StoreFront-Server oder einen Webinterface-Server
- über eine PNAgent-Anwendung auf einen StoreFront-Server (XenApp Services Support muss auf der Citrix-Farm aktiviert sein) oder einen Webinterface-Server
- über eine ICA-Anwendung auf einen virtuellen Desktop oder veröffentlichte Anwendungen

Hinweis
Der Zugriff über den Anwendungs-Typ **ICA** ist veraltet und wird nur bis XenApp 6.x von Citrix unterstützt.

Voraussetzungen

- Das Software-Paket **Citrix Receiver for Linux 13.x** muss auf den Clients installiert sein.
- Für eine Verbindung via HTTPS beim Anwendungs-Typ **Storefront**, **Self Service** und **PNagent** müssen die entsprechenden Root- und Intermediate-Zertifkate auf den Clients vorhanden sein.
  - Root-Zertifikate müssen nach `/setup/cacerts` übertragen werden.
  - Intermediate-Zertifkate müssen nach `/setup/cacerts/intcerts` übertragen werden.

  Für weitere Informationen zur Konfiguration der Zertifikate siehe Zertifikate.
- Für eine Verbindung via HTTPS beim Anwendungs-Typ **Browser** müssen die entsprechenden Root- und Intermediate-Zertifkate auf den Clients vorhanden sein.
  - Firefox: Root-Zertifikate und Intermediate-Zertifkate müssen nach `/setup/cacerts/firefox` übertragen werden.
  - Chromium: Root-Zertifikate und Intermediate-Zertifkate müssen nach `/setup/cacerts/browser` übertragen werden.
- Die eLux-Taskleiste sollte auf den Clients aktiv sein, wenn veröffentlichte Anwendungen als **seamless applications** zur Verfügung gestellt werden. Seamless applications verhalten sich wie lokale Anwendungen und können aus der minimierten Fenstergröße nur über die Taskleiste wiederhergestellt werden. Für weitere Informationen siehe Erweiterte Desktop-Einstellungen.

7.2.1. StoreFront-Anwendung

Mit dem Anwendungs-Typ **StoreFront** können sich Benutzer zu einem StoreFront-Server verbinden. Virtuelle Desktops und veröffentlichte Anwendungen werden über einen Store zur Verfügung gestellt. Als Citrix-Produkte kommen hauptsächlich Citrix XenApp und Citrix XenDesktop zum Einsatz. Der Zugriff auf StoreFront-Seiten kann über HTTP oder HTTPS erfolgen.

Mit der StoreFront-Integration in die Modern UI von eLux RP können die Citrix-Ressourcen eines oder mehrerer Stores gemeinsam mit anderen konfigurierten eLux-Anwendungen wie **RDP**- oder **Browser**-Sitzungen über eine gemeinsame Benutzeroberfläche, das eLux Modern User Interface, genutzt werden. Für weitere Informationen siehe eLux Modern UI.

StoreFront-Anwendung definieren

Hinweis
Für HTTPS-Verbindungen müssen die entsprechenden SSL-Zertifikate am Client vorhanden sein.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **StoreFront**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung, wird in der Scout Enterprise-Konsole angezeigt
Stores	Geben Sie die URL eines oder mehrerer Stores ein: ▶ Klicken Sie auf die Schaltfläche **Hinzufügen** und ändern den automatisch erzeugten Vorgabewert auf Ihren individuellen Wert ab (Doppelklick oder F2). Beispiel: `https://CtrXd76.mastertec-01.-com/Citrix/Store33/discovery`
Anmeldung	Die Anmeldung des Benutzers am Store erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).
Passthrough-Anmeldung	Die Anmeldung des Benutzers am Store erfolgt via Single Sign-On. Die Werte der AD-Benutzeranmeldung werden verwendet. Wenn die AD-Benutzeranmeldung über SmartCard erfolgt, darf bei Verwendung von Citrix Receiver for Linux 13.4 oder höher die Authentifizierungs-Methode **Domain pass-through** am Citrix-Server nicht aktiviert sein.

Option	Beschreibung
	Hinweis Für die Passthrough-Anmeldung muss das eLux-Paket **Citrix Receiver Extensions** und das hierin enthaltene Feature-Paket **Dialog Extension** auf den Clients installiert sein.
Letzten Benutzer anzeigen[1]	Im StoreFront-Anmeldedialog werden die Anmeldedaten (außer Kennwort) der letzten Anmeldung angezeigt. Diese Option hat keine Auswirkung, wenn Sie unter **Anmeldung** feste Anmeldedaten zur automatischen Anmeldung eintragen.
Autostart	Geben Sie die Namen der StoreFront-Anwendungen ein, die automatisch gestartet werden sollen. Achten Sie auf die korrekte Schreibweise gemäß Anwendungsnamen in StoreFront. Mehrere Anwendungsnamen müssen durch Semikolon getrennt werden. Beispiel: `MyApp1;MyApp2`
Dauerbetrieb automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen
Freie Parameter (optional)	Individuelle Parameter für den Anwendungsstart siehe Freie Anwendungsparameter definieren

3. Wenn Sie einen Eintrag aus der **Stores**-Liste löschen möchten, markieren Sie den Eintrag und klicken auf **Löschen**.
4. Für weitere Einstellungen klicken Sie auf die Schaltfläche **Erweitert** und bearbeiten folgende Felder:

Option	Beschreibung
Fenstereigenschaften	Desktops können im Vollbild-Modus oder im Fenster-Modus gestartet werden.
Zeitgesteuertes Abmelden	Für eine automatische Abmeldung vom StoreFront-Server aktivieren Sie die Option **Abmelden nach** und geben die relevante Verzögerung in Sekunden an. Dies gilt nicht für den gestarteten Desktop. Alternativ kann eine automatische Abmeldung nach dem Beenden der letzten StoreFront-Anwendung konfiguriert werden.

[1] ab Scout Enterprise Management Suite Version 14.7

Option	Beschreibung
Wiederverbinden von Anwendungen	Legen Sie fest, was beim Wiederverbinden zum StoreFront-Server passieren soll. **Nicht wiederverbinden**: Die Verbindung zum Desktop bzw. zu den veröffentlichten Anwendungen wird nicht wiederhergestellt (Standard). **Nur getrennte Sitzungen**: Die Verbindung zu einer getrennten Sitzung wird wiederhergestellt.. **Aktive und getrennte Sitzungen**: Die Verbindung zu einer getrennten oder aktiven Sitzung wird wiederhergestellt
Manuelles Abmelden	Legen Sie fest, was bei der Abmeldung am StoreFront-Server passieren soll. **Nur Server abmelden**: Eine Abmeldung erfolgt nur vom StoreFront-Server. **Server und Anwendungen abmelden**: Eine Abmeldung erfolgt vom StoreFront-Server und vom virtuellen Desktop oder den veröffentlichen Anwendungen. **Server abmelden und Anwendungen trennen**: Eine Abmeldung erfolgt vom StoreFront-Server, aber am virtuellen Desktop wird nur eine Sitzungs-Trennung durchgeführt. Dadurch ist ein späteres Wiederverbinden zu diesem Desktop möglich.

5. Bestätigen Sie mit **Übernehmen** und **OK**.

SmartCard-Authentifizierung für StoreFront

Wenn Sie die SmartCard-Authentifizierung für StoreFront nutzen, können Sie das Verhalten beim Ziehen der SmartCard konfigurieren.

Hinweis

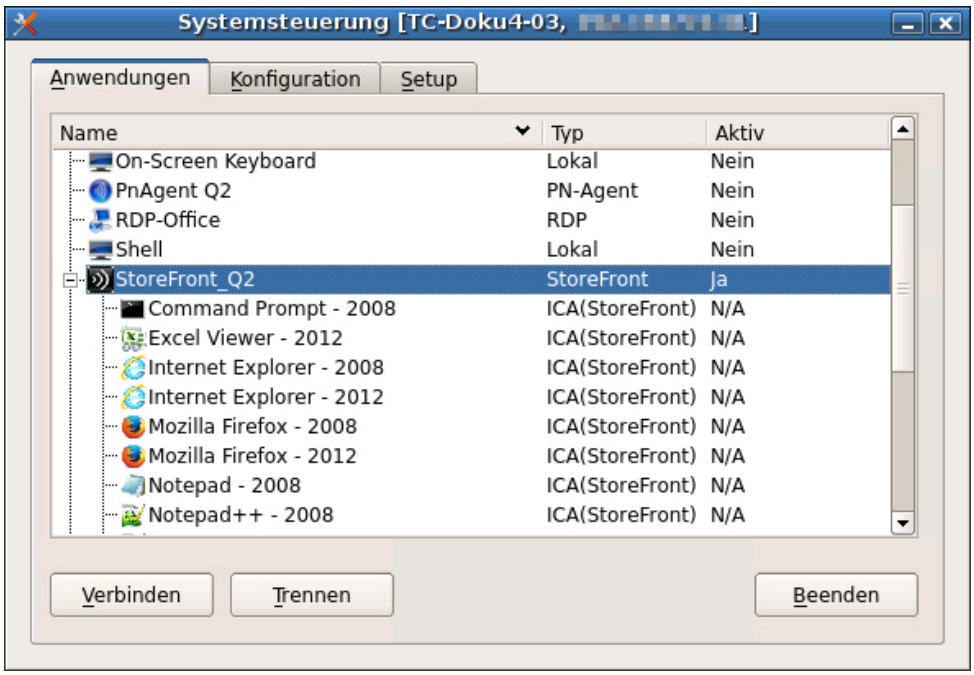
Die entsprechende Smartcard-Middleware muss auf den Clients installiert sein. Weiterhin muss die Smartcard-Authentifizierung auf der Citrix-Farm aktiviert sein. Wenn Citrix Receiver für Linux auf dem Client eine Smartcard-Middleware findet, hat die Smartcard-Anmeldung Vorrang gegenüber der Anmeldung mit Benutzername und Passwort.

- Definieren Sie mit Hilfe der Scout Enterprise-Funktion Erweiterte Dateieinträge folgenden Eintrag:

Datei	`/setup/sessions.ini`
Abschnitt	`ICADefaults`
Eintrag	`SmartcardRemovalAction`
Wert	`noaction` | `forcelogoff` (Default: `noaction`)

Zugriff auf veröffentlichte Ressourcen

Nach der Anmeldung an einem StoreFront-Store oder einem Webinterface-Server kann der Benutzer die verfügbaren Ressourcen über das eLux-Startmenü öffnen oder über die Systemsteuerung und das Register **Anwendungen**: Der **StoreFront**-Knoten kann erweitert werden, um die am Server verfügbaren Ressourcen anzuzeigen.



7.2.2. Self-Service-Benutzeroberfläche

Die Self-Service-Benutzeroberfläche ersetzt die Konfigurationsverwaltung **wfcmgr** und erlaubt den Zugriff auf Citrix-Dienste, die veröffentlichte Ressourcen bereitstellen. Benutzer, für die ein Konto eingerichtet wurde, können Desktops und Anwendungen abonnieren und dann starten.

Citrix Self-Service als lokale Anwendung definieren

Hinweis
Das eLux-Paket **Citrix Receiver for Linux** und das hierin enthaltene Feature-Paket **Self-service** muss auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie `Benutzerdefiniert`.
Parameter (erforderlich)	Geben Sie folgenden Programmnamen zum Aufruf ein: `selfservice`

3. Bestätigen Sie mit **Übernehmen** und **OK**.

Hinweis
Die Anwendung `selfservice` verwendet die Standard-Konfiguration. Wenn Sie weitere Konfigurationsmöglichkeiten wünschen, verwenden Sie alternativ die Self-Service-Benutzeroberfläche mit Erweiterungen (`ucselfservice`).

7.2.3. Self-Service-Benutzeroberfläche mit Erweiterungen

Die Citrix Self-Service-Benutzeroberfläche kann um weitere Funktionalitäten ergänzt werden:[1]

- Konfiguration der aufzurufenden Stores
- Verbindungsoptionen
- Dialog- und Fenstereigenschaften

Citrix Self-Service mit erweiterter Funktionalität definieren

Hinweis
Das eLux-Paket **Citrix Receiver for Linux V13.5.x** muss installiert sein.
Das eLux-Paket **Citrix Receiver Extensions V2.x** muss installiert sein.
Je nach gewünschter Funktionalität müssen folgende enthaltene Feature-Pakete auf den Clients installiert sein:
Self-service wrapper
Dialog Extension (für Änderungen des Citrix-Dialog-Designs)
Self-service dialog themes (für Änderungen des Citrix-Dialog-Designs)

Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie `Benutzerdefiniert`.
Parameter (erforderlich)	Geben Sie folgenden Programmnamen zum Aufruf ein: `ucselfservice`
Freie Parameter	Definieren Sie Parameter und Werte für aufzurufende Stores, Fenstereigenschaften und Verbindungsoptionen gemäß untenstehender Tabelle **Parameter für die Self-Service-Erweiterung**. Für weitere Informationen siehe Freie Anwendungsparameter definieren.

3. Bestätigen Sie mit **Übernehmen** und **OK**.
4. Wenn Sie das Design der Citrix-Dialoge für alle Citrix-Verbindungen ändern möchten, verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole, um folgende

[1] ab eLux RP 5.6

Einträge zu setzen:

Datei	Abschnitt	Eintrag	Wert
/setup/sessions.ini	ICADefaults	UiDialogTheme	`ucselfservice`
/setup/sessions.ini	ICADefaults	UiDialogDecorated	`<true|false>`
/setup/sessions.ini	ICADefaults	UiDialogKeepAbove	`<true|false>`
/setup/sessions.ini	ICADefaults	UiDialogKeepBelow	`<true|false>`
/setup/sessions.ini	ICADefaults	UiDialogColorHover	<*color*> Beispiel `#b0b0b0`
/setup/sessions.ini	ICADefaults	UiDialogColorUnselected	<*color*> Beispiel: `#a0a0a0`
/setup/sessions.ini	ICADefaults	UiDialogColorSelected	<*color*> Beispiel: `#c0c0c0`

Für weitere Informationen siehe Erweiterte Dateieinträge.

Hinweis

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

Parameter für die Self-Service-Erweiterung

Parameter	Beschreibung	Herkunft
`StoreUrl1=`<*URL to store1*>	Storefront-URL	Citrix/Unicon
`StoreUrl2=`<*URL to store2*>	Storefront-URL	Citrix/Unicon
`StoreUrl3=`<*URL to store3*>	Storefront-URL	Citrix/Unicon
`SharedUserMode=`<*true|false*>	Im **Shared User Mode** wird ein Systemkonto für mehrere Benutzer verwendet. Beim Abmelden oder Schließen der Benutzeroberfläche werden die Benutzerdaten entfernt.	Citrix
`FullscreenMode=`<*0|1|2*>	0 kein Vollbildmodus 1 Vollbildmodus 2 maximiert und ohne Rahmen, Taskleiste bleibt sichtbar Kann für die Verwendung von **seamles applications** sinnvoll sein Default: 0 (kein Vollbildmodus)	Citrix

Parameter	Beschreibung	Herkunft
`SelfSelection=<true|false>`	Wird zur Deaktivierung des Suchfeldes und der Self-Selection-Leiste verwendet Das Deaktivieren verhindert, dass Benutzer weitere Anwendungen abonnieren können. Default: false	Citrix
`StoreGateway=<store gateway>`	Angabe eines Gateways, falls erforderlich	Citrix
`ReconnectOnLogon=<true|false>`	Versucht, direkt nach der Anmeldung an einem Store alle Sitzungen für diesen Store wiederzuverbinden	Citrix
`ReconnectOnLaunchOrRefresh=<true|false>`	Versucht alle Sitzungen wiederzuverbinden, sobald eine Anwendung gestartet oder der Store aktualisiert wird	Citrix
`SessionWindowedMode=<true|false>`	true: Desktops werden im Fenstermodus angezeigt false: Desktops werden full-screen angezeigt	Citrix
`UseLogoffDelay=<0|1>`	Automatisches Abmelden aktivieren mit `UseLogoffDelay=1`	Unicon
`LogoffDelay=<seconds>`	Verzögerung in Sekunden beim automatischen Abmelden	Unicon
`ForcedLogoff=<1|2>`	1 Logoff-Timer wird mit der Anmeldung gestartet 2 Logoff-Timer wird nach Beenden der letzten Citrix-Anwendung gestartet	Unicon
`LogoffInfoTimeout=<seconds>`	Während der Abmeldung (Self-Service-Neustart) kann für einige Sekunden ein Info-Dialog angezeigt werden.	Unicon

7.2.4. Browser-Sitzung zum Zugriff auf veröffentlichte Ressourcen

Benutzer können von einem lokalen Browser auf Anwendungen und Desktops zugreifen, die über einen Store auf dem Citrix StoreFront-Server oder über das Citrix Webinterface veröffentlicht wurden.

Browser-Anwendung zum Zugriff auf Citrix-Ressourcen konfigurieren

Hinweis
Damit eine Browser-Anwendung direkt am Client genutzt werden kann, muss das entsprechende Software-Paket für Firefox oder Chromium auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

Hinweis
Für HTTPS-Verbindungen müssen die entsprechenden SSL-Zertifikate am Client vorhanden sein.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Browser**.
2. Bearbeiten Sie die folgende Felder:

Option	Beschreibung
Name	Name für die Browser-Sitzung
Browsertyp	Firefox oder Chromium

Aufzurufende Seite	URL zum Aufruf der Webinterface-Startseite oder des StoreFront-Stores.
	Beispiele:
	`https://<Servername>/Citrix/StoreWeb`
	`https://<Servername>/Citrix/XenApp`

3. Konfigurieren Sie die weiteren Parameter, siehe Browser-Anwendung definieren.

Der lokale Benutzer startet den Browser und gelangt automatisch zur definierten Startseite. Nach erfolgreicher Anmeldung am Storefront-Server oder am Webinterface-Server werden die verfügbaren veröffentlichten Anwendungen, Desktops und Inhalte im Browser-Fenster angezeigt.

7.2.5. PNAgent-Anwendung

Eine Anwendung vom Typ **PNAgent** (Program Neighborhood Agent) ermöglicht Benutzern, über einen Server, auf dem eine XenApp Services-Site ausgeführt wird, auf veröffentlichte Ressourcen zuzugreifen. Veröffentlichte Ressourcen können veröffentlichte Anwendungen, veröffentlichte Server-Desktops oder veröffentlichte Inhalte (Dateien) sein.

Einstellbare Optionen für alle Benutzer sind in der Konfigurationsdatei `config.xml` definiert, die auf dem Webinterface-Server (standardmäßig im Verzeichnis `//I-netpub/wwwroot/Citrix/PNAgent`) gespeichert ist. Wenn ein Benutzer eines der veröffentlichten Programme startet, liest es die Konfigurationsdaten vom Server. Die Konfigurationsdatei kann so konfiguriert werden, dass Einstellungen und Benutzerschnittstelle regelmäßig aktualisiert werden.

Die Datei `config.xml` gilt für alle Verbindungen, die von der XenApp Services-Site definiert werden. Für weitere Informationen siehe die Citrix eDocs unter http://support.citrix.com.

PNAgent konfigurieren

Hinweis
Für HTTPS-Verbindungen müssen die entsprechenden SSL-Zertifikate am Client vorhanden sein.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **PNAgent**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung

Server	Geben Sie die Adresse der Konfigurationsdatei am Webinterface-Server an (URL).
	Wenn das Standardverzeichnis und Port 80 genutzt werden, genügt die Angabe des Servers.
	
	Beispiele:
	`https://CtrXd.mastertec-01.-de/Citrix/PNAgent/config.xml`
	`https://192.168.10.11:81`

Anmeldung	Die Anmeldung des Benutzers am Webinterface erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).

Option	Beschreibung
Passthrough-Anmeldung	Die Anmeldung des Benutzers am Webinterface erfolgt via Single Sign-On. Die Werte der AD-Benutzeranmeldung werden verwendet. Hinweis: Die Authentifizierung über Kerberos wird für Citrix Receiver für Linux 13.x nicht mehr unterstützt.
Autostart Anwendung/Verzeichnis	Geben Sie die Namen der Anwendungen an, die automatisch gestartet werden sollen. Alternativ können Sie einen Autostart-Ordner angeben, der veröffentlichte Anwendungen enthält. Der Ordner muss am Citrix Webinterface-Server angelegt sein.
Letzten Benutzer anzeigen[1]	Im PNAgent-Anmeldedialog werden die Benutzerdaten (außer Kennwort) der letzten Anmeldung angezeigt. Diese Option hat keine Auswirkung, wenn Sie Benutzerdaten zur automatischen Anmeldung eintragen.
Abbrechen erlauben	Erlaubt dem Benutzer, den PNAgent-Anmeldedialog zu schließen
Dauerbetrieb automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen
Freie Parameter (optional)	Individuelle Parameter für den Anwendungsstart Beispiel: `PNATimeout=60` führt dazu, dass der Citrix Receiver 60 Sekunden lang versucht die veröffentlichten Anwendungen und Desktops zu enumerieren. Um Dual-Monitorbetrieb einzurichten, können Sie ebenfalls die Freien Parameter verwenden, siehe unten. Für weitere Informationen siehe Freie Anwendungsparameter definieren

3. Für weitere Einstellungen klicken Sie auf die Schaltfläche **Erweitert** und bearbeiten folgende Felder:

Option	Beschreibung
Fenstereigenschaften	Wählen Sie für Auflösung/Fenstergröße, Farbtiefe und Audio-Qualität entweder den Standard- Wert (Server-Einstellungen) oder einen Wert aus dem Listenfeld.

[1] ab Scout Enterprise Management Suite Version 14.7

Option	Beschreibung
Zeitgesteuertes Abmelden	Für eine automatische Abmeldung vom Webinterface-Server aktivieren Sie die Option **Abmelden nach** und geben die relevante Verzögerung in Sekunden an. Dies gilt nicht für den gestarteten Desktop. Alternativ kann eine automatische Abmeldung nach dem Beenden der letzten PNAgent-Anwendung konfiguriert werden.
Wiederverbinden von Anwendungen	Legen Sie fest, was beim Wiederverbinden zum Webinterface-Server passieren soll. **Nicht wiederverbinden**: Die Verbindung zum Desktop oder zu den veröffentlichten Anwendungen wird nicht wiederhergestellt (Standard). **Nur getrennte Sitzungen**: Die Verbindung zu einer getrennten Sitzung wird wiederhergestellt. **Aktive und getrennte Sitzungen**: Die Verbindung zu einer getrennten oder zu einer aktiven Sitzung wird wiederhergestellt.
Manuelles Abmelden	Legen Sie fest, was nach einem Abmelden am Webinterface-Server passieren soll. **Nur Server abmelden**: Eine Abmeldung erfolgt nur vom Webinterface-Server. **Server und Anwendungen abmelden**: Eine Abmeldung erfolgt vom Webinterface-Server und vom virtuellen Desktop bzw. den veröffentlichen Anwendungen **Server abmelden und Anwendungen trennen**: Eine Abmeldung erfolgt am Webinterface-Server, aber am virtuellen Desktop wird nur eine Sitzungs-Trennung durchgeführt. Dadurch ist ein späteres Wiederverbinden zu diesem Desktop möglich.

4. Bestätigen Sie mit **Übernehmen** und **OK**.

Program Neighborhood-Variablen

Variablen können beispielsweise zur Definition eines eindeutigen Client-Namens für eine Citrix XenApp-Sitzung verwendet werden. Bei der Anmeldung am Webinterface-Server mit Program Neighborhood stehen die folgenden Variablen im Dialog zur Verfügung:

`$ICAUSER`	Benutzername
`$ICADOMAIN`	Domain für diesen Anwender
`$ICAAPPLICATION`	Name der Anwendungsdefinition im PNAgent

Domänenliste erstellen

Sie können für PNAgent-Anwendungen eine Domänenliste erstellen zur Auswahl für den Anwender.

1. Erstellen Sie die Textdatei `icadomains` ohne Dateinamenserweiterung.
2. Tragen Sie die relevanten Domänen ein, eine Domäne pro Zeile.
3. Speichern Sie die Datei im Scout Enterprise-Installationsverzeichnis.
4. Übertragen Sie die Datei in das Verzeichnis `/Setup` am Thin Client mit Hilfe der Scout Enterprise-Funktion Dateien.

Wenn in der Konfiguration nicht alle Informationen angegeben wurden, öffnet sich beim Start einer PNAgent- Anwendung ein Anmelde-Dialog für das Citrix Webinterface. Die Domänen werden als Drop-down-Liste angeboten.

Hinweis
In der PNAgent-Anwendungsdefinition können Sie zusätzlich eine Domäne voreinstellen.
Beispiel: `work.mastertec-01.com`

Einstellungen für Dual-Monitor-Betrieb

Für PNAgent-Sitzungen können Sie den Dual-Monitorbetrieb mit einer der folgenden Methoden einrichten. Die Citrix-Sitzung kann auf den ersten Monitor, den zweiten Monitor oder beide Monitore übertragen werden.

Methode 1:

- Verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole, um die ICA Software-Standardeinstellungen zu bearbeiten:

Datei	`/setup/sessions.ini`
Abschnitt	`ICADefaults`
Eintrag	`Xinerama`
Wert	`-1|0|1`

  Für weitere Informationen siehe Erweiterte Dateieinträge.

Methode 2:

- Definieren Sie in der Scout Enterprise-Konsole in der Anwendungsdefinition folgende **Freie Parameter**:

```
Key = Xinerama
Value = -1|0|1
```

  Für weitere Informationen siehe Freie Anwendungsparameter.

Die Werte haben folgenden Effekt:

-1	beide Monitore
0	erster Monitor
1	zweiter Monitor

7.2.6. ICA-Anwendung definieren

Hinweis
Der Zugriff über den Anwendungs-Typ **ICA** ist veraltet und wird nur bis XenApp 6.x von Citrix unterstützt.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **ICA**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die ICA-Anwendung
Veröffentlichte Anwendung	Konfiguriert direkten Zugriff auf eine veröffentlichte Anwendung Um Zugriff auf komplette Desktops zu konfigurieren, deaktivieren Sie die Option.
Server	IP-Adresse oder Name des Citrix-Servers (Terminal Server)
Anwendung	Nur relevant, wenn Sie die Option **Veröffentlichte Anwendung** aktiviert haben Name der Windows-Anwendung mit Pfad (siehe Citrix-Server) Hinweis: Die Schaltfläche **Durchsuchen** bezieht sich auf die verwendete Citrix-Farm, die Funktion wird jedoch nicht mehr unterstützt.
Arbeitsverzeichnis (optional)	Nur relevant, wenn Sie die Option **Veröffentlichte Anwendung** aktiviert haben. Arbeitsverzeichnis für die Anwendung
Anmeldung	Die Anmeldung des Benutzers am Citrix-Server erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).
Passthrough-Anmeldung	Die Anmeldung des Benutzers am Citrix-Server erfolgt via Single Sign-On. Die Werte der AD-Benutzeranmeldung werden verwendet. Hinweis: Die Authentifizierung über Kerberos wird für Citrix Receiver für Linux 13.x nicht mehr unterstützt.

Option	Beschreibung
Smartcard-Anmeldung	Der Client verwendet eine Smartcard zum Anmelden.
Dauerbetrieb automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen
Freie Parameter (optional)	Individuelle Parameter für den Anwendungsstart Für weitere Informationen siehe Freie Anwendungsparameter definieren
Verbindungs-Optionen Erweitert (eLux)	Öffnet den Konfigurations-Dialog des Citrix Receiver für Linux (`wfcmgr`) Bearbeiten Sie die gewünschten Optionen. Die Citrix Receiver-Konfiguration wird in der Datei `/setup/ica/wfclient.ini` auf dem Client gespeichert und kann über die Scout Enterprise-Funktion **Diagnosedateien** eingesehen werden.

3. Bestätigen Sie mit **Übernehmen** und **OK**.

Eine veröffentlichte Anwendung wird wie eine lokale Anwendung am eLux-Client angezeigt.

7.2.7. Citrix Software-Standardeinstellungen

Für Citrix-Anwendungen können Sie in der Scout Enterprise-Konsole Citrix Receiver-Standardeinstellungen festlegen, die für alle Citrix-Verbindungen und alle Geräte in dieser OU wirksam sind und je nach Einstellung weiter nach unten vererbt werden.

Folgende Standardeinstellungen stehen zur Verfügung:

- Client-Laufwerkszuordnung
- Zuordnung von COM-Anschlüssen
- Firewall-Einstellungen
- Citrix-Tastenkombinationen
- Fenstereigenschaften
- Verbindungsoptionen
- Bitmap-Caching

Zum Aufruf siehe Standardeinstellungen für Anwendungen setzen.

Einige Citrix Receiver-Standardeinstellungen werden im folgenden beschrieben.Weitere Informationen entnehmen Sie bitte der Dokumentation von Citrix.

Register Allgemein

Option	Beschreibung
TW2StopwatchMinimum	Bildlaufgeschwindigkeit für Remote Anwendungen (beispielsweise für Adobe Acrobat Reader, Excel) Je höher der Wert, desto langsamer die Geschwindigkeit beim Scrollen Hinweis für Excel: Ein niedriger Wert erhöht die Bildlaufgeschwindigkeit, aber verzögert sie, sobald eine Markierung in der Excel-Tabelle außerhalb des unteren Bildschirmrandes gezogen wird. Standardwert = 25
ClientName – Vorlage	Definition des Client-Namens in der Citrix-Sitzung Hinweis: Sie können die Program Neighborhood-Variablen `$ICANAME` und `$ICADOMAIN` nutzen, um einen eindeutigen Client-Sitzungsnamen zu setzen. Für Citrix-Roaming und einige XenApp-Programme ist dies Voraussetzung. Für weitere Informationen siehe PNAgent-Anwendung.

Register Laufwerkszuordnung

Option	Beschreibung
A-Z	Die Buchstaben A-Z stellen die logischen Laufwerksnamen auf dem Terminalserver dar. Im Feld rechts daneben können Sie einem Laufwerk eine lokale Ressource zuordnen, die in der Citrix-Sitzung dargestellt werden soll. Tragen Sie den Mountpoint ein, der dem Pfad zum lokalen Zugriff auf die Ressource entspricht. Die Mountpoints werden von eLux zur Verfügung gestellt, beispielsweise `/media/usbdisk` oder `/media/cdrom`.
Attribute E / R / W	bezeichnen die Art des Zugriffsrechts: • E = aktivieren (enable) • R = lesen (read) • W = schreiben (write)
Laufwerkszuordnung erlauben	Nur bei eingeschalteter Option werden die definierten Laufwerkszuordnungen durchgeführt.
Dynamische Zuordnung aktiveren	Eventuell vorhandene Massenspeicher werden dem nächsten freien Laufwerksbuchstaben zugeordnet.

Für weitere Informationen siehe Mountpoints.

Register COM-Ports

Zur Verbindung an einen COM-Port muss der Gerätename des COM-Anschlusses am Thin Client bekannt sein.

Der COM-Port-Gerätename beginnt immer mit `/dev`. Groß- und Kleinschreibung ist bei den Gerätenamen relevant.

Beispiele:

Port-Gerätename	COM Port
`/dev/ttyS0`	COM1
`/dev/ttyS1`	COM2

Die Verfügbarkeit der COM-Ports hängt von der Hardwareplattform ab.

Hinweis
Die Client-Ports müssen entsprechend auf der Citrix-Ressource (zum Beispiel Desktop) abgebildet werden, beispielsweise über ein `net use`-Kommando.
Beispiel: `net use com1: \\Client\COM2: /persistent:yes`

7.2.8. Citrix Connection Center

Das Citrix Connection Center zeigt die aktuell vorhandenen Serververbindungen an. Der Benutzer oder Administrator kann eine Verbindung schließen, trennen oder abmelden, ohne die Anwendung zu bedienen. Außerdem wird die Übertragungsstatistik angezeigt, was beispielsweise bei langsamen Verbindungen hilfreich sein kann.

Das Connection Center wird als Systray-Icon in der Taskleiste angezeigt.

Citrix Connection Center konfigurieren

Hinweis

Das eLux-Paket **Citrix Receiver Extensions** und das hierin enthaltene Feature-Paket **Connection Center** muss auf den Clients installiert sein.

Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie `ICA Connection Center`.

3. Bestätigen Sie mit **Übernehmen** und **OK**.

7.3. Zusätzliche Software für Citrix-Umgebungen

7.3.1. HDX RealTime Optimization Pack installieren

Die HDX RealTime Optimization Pack ermöglicht eine bessere Audio- und Videoqualität bei VOIP und Videochat.

1. Laden Sie das Paket `citrix_hdxrtme` herunter.
2. Importieren Sie das Paket mithilfe von ELIAS in Ihren Container.
3. Fügen Sie das Paket in ELIAS Ihrer `IDF`-Datei hinzu und speichern Sie die neue `IDF`-Datei.
4. Führen Sie ein eLux-Update auf die neue `IDF`-Datei durch.
5. Konfigurieren Sie Microsoft Lync oder Skype for Business in der Backend-Umgebung.

7.3.2. Adobe Flash Player konfigurieren

Ab eLux RP 5.4 werden für Adobe Flash Player zwei Versionen bereitgestellt. Ein Paket beinhaltet die von Citrix unterstützte Version für HDX MediaStream Flash Redirection, das andere Paket ist die aktuellste Version.

- Bearbeiten Sie die Datei `mms.cfg` und verwenden Sie anschließend die Scout Enterprise-Funktion **Dateien**, um die Konfigurationsdatei in das Zielverzeichnis `/setup/adobe/` am Client zu übertragen.

  Für weitere Informationen siehe Dateien.

7.3.3. Cisco VXME installieren

Cisco Virtualization Experience Media Edition (VXME) erweitert die Cisco Collaboration-Funktionalität auf virtuelle Umgebungen. Benutzer können in Verbindung mit dem Cisco Jabber Kommunikationsdienst für Windows Telefonanrufe auf ihrem Hosted Virtual Desktop (HVD) tätigen und entgegennehmen. Die VXME-Software routet alle Audio- und Video-Streams direkt von einem Thin Client zum anderen oder zu einem Telefon - ohne über den HVD zu gehen.

1. Laden Sie das `Cisco VXME`-Paket von der Cisco-Webseite herunter.
2. Laden Sie das Paket `VXME_utils` von unserem Portal www.myelux.com herunter.
3. Importieren Sie das Paket mithilfe von ELIAS in Ihren Container.
4. Fügen Sie das Paket in ELIAS Ihrer `IDF`-Datei hinzu und speichern Sie die neue `IDF`-Datei.
5. Führen Sie ein eLux-Update auf die neue `IDF`-Datei durch.
6. Folgen Sie dem Cisco Deployment and Installation Workflow auf der Cisco-Webseite, um die VXME-Systemumgebung zu konfigurieren.

Für weitere Informationen siehe

VXME 11.5 eLux Edition

VXME 11.5 eLux Edition Release Notes

7.3.4. Lumension-Paket installieren

1. Laden Sie das Paket "Lumension Endpoint Security Agent Control" von myelux.com > Software Packages für die betreffende eLux-Version herunter.
2. Fügen Sie das Paket mithilfe von ELIAS einem Container hinzu.
3. Fügen Sie das Paket zu Ihrer `IDF`-Datei hinzu und speichern Sie die neue `IDF`-Datei.
4. Führen Sie ein eLux-Update auf die neue `IDF`-Datei durch.
5. Wechseln Sie auf den Server, auf dem die serverseitige Lumension-Software läuft.
6. Beenden Sie den Dienst **Lumension Endpoint Security Command and Control**.
7. Kopieren Sie die Datei **LDI64.dll** in das Verzeichnis **Program Files\Lumension\Endpoint**.
8. Starten Sie den Dienst **Lumension Endpoint Security Command and Control** neu.

Die Protokolldatei befindet sich nun unter **%windir%\Temp\ldi.log**

Weitere Informationen finden Sie auf der Homepage von Lumension.

7.3.5. CenterTools DriveLock installieren

CenterTools DriveLock bietet Endpoint-Security für USB-Schnittstellen am Thin Client.

1. Laden Sie das Paket `DriveLock` von unserem Portal www.myelux.com herunter.
2. Importieren Sie das Paket mithilfe von ELIAS in Ihren Container.
3. Fügen Sie das Paket in ELIAS Ihrer `IDF`-Datei hinzu und speichern Sie die neue `IDF`-Datei.
4. Führen Sie ein eLux-Update auf die neue `IDF`-Datei durch.
5. Konfigurieren. Sie die DriveLock Backend-Umgebung.

7.4. RDP

Dieser Verbindungstyp entspricht in vieler Hinsicht der ICA-Funktionalität, nutzt jedoch das Microsoft Remote Desktop Protocol (RDP) zur Verbindung mit einem Microsoft Terminalserver. Zur Verfügung steht der **eLuxRDP**-Client basierend auf der freien Implementierung **FreeRDP**.

Zwei Konfigurationsmöglichkeiten stehen zur Verfügung:

- Windows Desktop: Eine Remote Desktop-Sitzung greift auf den Desktop eines Terminalservers zu. Der Anwender kann jede auf dem Desktop verfügbare Anwendung in beliebiger Reihenfolge nutzen.
- Einzelanwendung / Seamless application: Der Anwender kann nur auf eine bestimmte Anwendung des Terminalservers zugreifen.

7.4.1. RDP-Sitzung als Windows Desktop definieren

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **RDP**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die RDP-Anwendung
Server	IP-Adresse oder Name des Servers
Anwendung	Lassen Sie das Feld leer.
Arbeitsverzeichnis	Lassen Sie das Feld leer.
Anmeldung	Die Anmeldung des Benutzers am Server erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).
Passthrough-Anmeldung	Die Werte der AD-Benutzeranmeldung werden verwendet.
Freie Parameter	Erlaubt die Definition aller Parameter, die eLuxRDP zulässt, im Format: `FreeRDPParams=<Parameter>` Beispiel: `FreeRDPParams=/cert -ignore` Eine Liste der Parameter erhalten Sie durch Eingabe des Kommandos `eluxrdp` in einer Shell.
Dauerbetrieb automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen

3. Bestätigen Sie mit **Übernehmen** und **OK**.

Hinweis
Eine Server-unabhängige RDP-Sitzung können Sie als lokale versteckte Anwendung mit Namen `RDP_TEMPLATE` definieren. Diese Anwendung können Sie als Muster ohne Backend konfigurieren. Der Benutzer startet `rdpconnect` in der Shell und gibt anschließend den Server an, zu dem verbunden werden soll. Voraussetzung ist das Software-Paket **RDPConnect**.

7.4.2. RDP-Anwendung definieren

Für die Konfiguration einer Einzelanwendung über RDP müssen Sie zusätzlich zu den für die Windows Desktop-Konfiguration definierten Daten die relevante Anwendung angeben.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **RDP**.
2. Bearbeiten Sie die folgende Felder:

Option	Beschreibung
Name	Name für die RDP-Anwendung
Server	IP-Adresse oder Name des Servers
Anwendung	Name der Windows-Anwendung einschließlich Pfadangabe. Systemvariablen sind zulässig Beispiel: `c:\Programme\Microsoft Office\Office\EXCEL.EXE %SystemRoot%\system32\notepad.exe`
Arbeitsverzeichnis (optional)	Arbeitsverzeichnis der Windows-Anwendung
Anmeldung	Die Anmeldung des Benutzers am Server erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).
Passthrough-Anmeldung	Die Werte der AD-Benutzeranmeldung werden verwendet.
Dauerbetrieb automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen

3. Bestätigen Sie mit **Übernehmen** und **OK**.

Für den Benutzer läuft die Anwendung im Vollbildmodus im Remote-Sitzungs-Fenster.

7.4.3. Erweiterte RDP-Einstellungen

- Um zu den erweiterten RDP-Einstellungen zu gelangen, klicken Sie in den Anwendungseigenschaften einer RDP-Anwendung auf die Schaltfläche **Erweitert**.

Register Anzeige

Option	Beschreibung
Fenstergröße	Vollbild oder eine bestimmte Auflösung
Vollbild auf Monitor	Wenn Sie die Fenstergröße `Vollbild` gewählt haben, können Sie wählen, ob auf alle oder einen bestimmten Monitor ausgegeben werden soll.
Farben	Farbtiefe der RDP-Sitzung (8-32 Bit)

Hinweis
Wenn mehrere Bildschirme angeschlossen sind und wenn Sie auf einen einzelnen Monitor auszgeben möchten, muss in der Gerätekonfiguration die Option **Desktop > Erweiterte Desktop-Einstellungen > Windowmanager > Maximieren/Vollbild auf einzelnen Monitor** einschaltet sein.

Register Lokale Ressourcen

Das Register **Lokale Ressourcen** bietet zusätzliche Einstellungsmöglichkeiten für Terminalserver, die die RDP-Protokollversion V5.2 oder höher unterstützen.

Hinweis
– für Terminalserver, die die RDP-Protokollversion V5.2 oder höher unterstützen –
Die Einstellungen werden nur dann wirksam, wenn im Register **Erweitert** das **Protokoll** nicht auf `RDP V4` gesetzt ist.

Option	Beschreibung
Laufwerke	Wählen Sie Laufwerk, Mountpoint und den Laufwerksbuchstaben, der in der RDP-Sitzung dargestellt werden soll. Die Mountpoints entsprechen dem lokalen Zugriffspfad auf die Ressource und werden von eLux zur Verfügung gestellt. Für USB-Sticks lauten die Mountpoints `/media/usbdisk`, `/media/usbdisk0` usw. Für weitere Informationen siehe Mountpoints.

Option	Beschreibung
Drucker	Bis zu vier Druckerdefinitionen für eine Sitzung können automatisch erstellt werden. Die Drucker müssen im Register Drucker der eLux-Systemsteuerung eingerichtet sein und einen für den Server gültigen Treibernamen haben (Groß- / Kleinschreibung ist hier von Bedeutung). Es werden die ersten vier Profile mit Treibern genutzt. Zur Definition eines Standarddruckers aktivieren Sie die Option **Standard** in den eLux-**Druckereinstellungen**.
Sound	Mit der Option **Lokal abspielen** wird der Ton lokal am Client wiedergegeben. **Remote abspielen** bewirkt die Wiedergabe am entfernten Server.
Anschlüsse	Macht die definierten Schnittstellen von der RDP-Sitzung aus zugänglich.
Kartenleser	Smartcards können zur Anmeldung auf Basis eines Zertifikats verwendet werden.

Register Erweitert

Option	Beschreibung
Protokoll	Ermöglicht die Einstellung auf Protokoll 4 oder 5. Standardmäßig wird das Protokoll automatisch erkannt.
Tastatursprache	Definiert das Tastaturlayout innerhalb einer RDP-Sitzung. Die Standardeinstellung `Auto` entspricht der Einstellung der Tastatursprache in der eLux Systemsteuerung.
	Achtung Wenn Sie eine bestimmte Tastatursprache einstellen, muss diese identisch mit der in der eLux-Systemsteuerung eingetragenen Tastatursprache sein.
Deaktiviere Window-Manager Dekorationen	Die Rahmen der eLux-Fenster werden ausgeblendet.
Deaktiviere Verschlüsselung	Der Server akzeptiert keine verschlüsselten Sitzungen. Diese Option können Sie setzen, um die Performance zu erhöhen. Standardmäßig ist die Option deaktiviert.
Deaktiviere Mausbewegungsereignisse	Informationen zur Mauszeigerposition werden nur jeweils bei Mausklick zum Server geschickt. Das erhöht die Systemleistung bei Verbindungen mit geringer Bandbreite. Standardmäßig ist diese Option deaktiviert.
Verbindungsleiste bei Vollbild anzeigen	Zeigt die Verbindungsleiste im Vollbildmodus an.
Bandbreite	Wählen Sie zwischen `Standard`, `Modem`, `Breitband`, `LAN`.

7.4.4. RemoteFX konfigurieren

Microsoft® RemoteFX™ ist eine Funktion, die in Windows Server 2008 R2 mit Service Pack 1 (SP1) enthalten ist. RemoteFX bietet eine umfassende Funktionalität für Virtual Desktop Infrastructure (VDI) durch die Bereitstellung eines virtuellen 3D-Adapters, intelligenter Codecs, sowie der Möglichkeit, USB-Geräte an virtuelle Maschinen weiterzuleiten.

Hinweis

RemoteFX kann nur in der RDP Sitzung verwendet werden, wenn das Server-Backend dies unterstützt und entsprechend dafür konfiguriert ist. Einzig die Bandbreite muss für den Client eingestellt werden.

1. Öffnen Sie die Eigenschaften Ihrer RDP-Anwendung und klicken Sie auf die Schaltfläche **Erweitert**.

   *Der Dialog **Erweiterte RPD-Einstellungen** öffnet.*

2. Wählen Sie das Register **Erweitert**.
3. Wählen Sie im Feld **Bandbreite** die Option `LAN`.
4. Bestätigen Sie mit **Übernehmen** und **OK**.

7.5. Virtual Desktop

Als **virtuellen Desktop** können Sie für Citrix-Verbindungen oder VMware-Verbindungen einen Virtual Desktop Broker definieren.

Für Citrix XenDesktop werden die Anmeldedaten analog zu einer ICA-Verbindung definiert.

7.5.1. Virtuellen Desktop definieren

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Virtueller Desktop**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
VD Broker	Wählen Sie den relevanten Broker aus der Liste
Server	Geben Sie die IP-Adresse (oder Name) des Servers ein.
Anmeldung	Die Anmeldung des Benutzers am Store erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).
Passthrough-Anmeldung	Die Werte der AD-Benutzeranmeldung werden verwendet.
Protokoll (nur VMware View)	Wählen Sie zwischen `RDP` und `PCOIP`

3. Für weitere Einstellungen klicken Sie auf die Schaltfläche **Erweitert**. Für weitere Informationen siehe je nach gewähltem Broker oder. Protokoll
   - Erweiterte XenDesktop-Einstellungen oder
   - Erweiterte RDP-Einstellungen
4. Bestätigen Sie mit **Übernehmen** und **OK**.

7.6. Browser

Unterstützte Browser sind Mozilla Firefox und Google Chromium.[1]

Hinweis
Wenn Sie Chromium einsetzen, empfehlen wir mindestend 2 GB RAM für die Thin Clients.

7.6.1. Browser-Anwendung definieren

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Browser**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für den Browser, wird in der Scout Enterprise-Konsole angezeigt
Browsertyp	Wählen Sie `Firefox` oder `Chromium`[2].
Startseite	Webseite (URL), die im Browser als Startseite hinterlegt wird, öffnet beim Klick auf **Home**
Aufzurufende Seite	Webseite (URL), die unmittelbar nach dem Starten des Browsers öffnet

Proxy-Einstellung	**Kein Proxy** : Keine Proxy-Einstellung für den Browser
	Manuell (Proxy:Port): Proxy-Server und Portnummer
	Beispiel: `proxy.mastertec-01.de:3800`
	Für die manuelle Proxy-Einstellung, können Sie eine Ausnahmeliste[3] in den **Erweiterten Browser-Einstellungen** pflegen.
	Auto (URL): Proxy-Konfigurationsdatei
	Beispiele:
	`http://www.proxy.mastertec-01.com/proxy.pac`
	`http://www.wpad.mastertec-01.com/wpad.dat`

Dauerbetrieb Automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen
Freie Parameter (optional)	Individuelle Parameter für den Anwendungsstart siehe Freie Anwendungsparameter

3. Um bei der manuellen Proxy-Einstellung Ziele zu definieren, auf die nicht per Proxy zugegriffen

[1] Chromium ist ab Scout Enterprise Management Suite Version 14.8 verfügbar
[2] Chromium ist ab Scout Enterprise Management Suite Version 14.8 verfügbar
[3] ab Scout Enterprise Management Suite Version 14.8

werden soll, wählen Sie **Erweitert > Proxy-Ausnahmeliste** und geben die relevanten Adressen ein.

4. Um den Kiosk-Modus einzuschalten, siehe Kiosk-Modus konfigurieren.
5. Bestätigen Sie mit **Übernehmen** und **OK**.

Hinweis
Alle Browserdateien (Cache, History, Lesezeichen usw.) werden standardmäßig temporär auf dem Flashspeicher gespeichert, sind aber nach einem Neustart nicht mehr verfügbar. Wir empfehlen, ein Netzlaufwerk als Browser-Homeverzeichnis zu definieren. Für weitere Informationen siehe Speicherort für Browserdateien.

Weitere Browser-spezifische Voreinstellungen können Sie mit Hilfe von Richtlinien-Dateien (Chromium) oder Einträgen in der Konfigurationsdatei (Firefox) definieren. Für weitere Informationen siehe im Scout Enterprise-Handbuch.

Voreinstellungen Chromium

Voreinstellungen Firefox

SSL-Zertifikate für den Browser bereitstellen

Für den Zugriff via HTTPS müssen entsprechende Root-Zertifikate und Intermediate-Zertifikate für den Browser importiert werden.

- Verwenden Sie die Scout Enterprise-Funktion **Konfigurierte Dateiübertragung**, um die Zertifikat-Dateien in das erforderliche Zielverzeichnis am Client zu übertragen:

Mozilla Firefox	`/setup/cacerts/firefox`
Google Chromium	`/setup/cacerts/browser`

  Für weitere Informationen siehe Erweiterte Konfiguration > Dateien.

Beachten Sie, dass ein zweiter Neustart des Clients erforderlich ist, um die während des ersten Neustarts übertragenen Zertifikate in den Zertifikatsspeicher des Browsers zu übernehmen.

7.6.2. Voreinstellungen Chromium

Mit Hilfe von Richtlinien können Sie für den Chromium-Browser obligatorische (managed) und empfohlene (recommended) Voreinstellungen setzen. Obligatorische Voreinstellungen setzen feste, nicht-änderbare Vorgabewerte. Empfohlene Voreinstellungen setzen änderbare Vorgabewerte (Default-Werte). Für weitere Informationen siehe https://www.chromium.org/administrators/.

- Verwenden Sie die Scout Enterprise-Funktion **Konfigurierte Dateiübertragung**, um Richtlinien-Dateien (`.json`) in das erforderliche Zielverzeichnis am Client zu übertragen:

Feste Vorgabewerte	`/setup/chromium/managed`
Änderbare Vorgabewerte	`/setup/chromium/recommended`

Für weitere Informationen siehe Erweiterte Konfiguration > Dateien.

7.6.3. Voreinstellungen Firefox

Firefox-spezifische Voreinstellungen, die über die Konfigurationsmöglichkeiten der Anwendungsdefinition hinausgehen, können Sie ab Firefox Version 38.5.2.1 mit Hilfe der Konfigurationsdatei `/setup/firefox/user.ini` am Client festlegen.

Zur Verfügung stehen alle Optionen, die im Mozilla Konfigurationseditor für Firefox (Seite `about:config`) verfügbar sind. Eine Option wird mit dem relevanten Eintrag und dem gewünschten Wert mit Hilfe der Scout Enterprise-Funktion **Erweiterte Dateieinträge** zum Client übertragen.

Voreinstellungen für Firefox aus about:config definieren

1. Rufen Sie in Firefox die Seite `about:config` auf. Die unter **Einstellungsname** / **Preference Name** gelisteten Optionen liefern die Basis für die Zeichenfolgen, die Sie im nächsten Schritt unter **Abschnitt** und **Eintrag** angeben.
   Für weitere Informationen siehe Konfigurationseditor für Firefox auf der Mozilla Support-Seite.
2. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Konfiguration > Erweiterte Dateieinträge**.
3. Definieren Sie folgenden Eintrag:

Datei	`/setup/firefox/user.ini`
Abschnitt	*<Einstellungsname, wie im Konfigurationseditor angegeben –Zeichenfolge links vom letzten Punkt>*
Eintrag	*<Einstellungsname, wie im Konfigurationseditor angegeben – Zeichenfolge rechts vom letzten Punkt>*
Wert	*<gewünschter Wert>*

Beispiel:
Sie möchten den Wert für die Option **browser.tabs.closeWindowWithLastTab** auf den Wert `false` setzen.

Datei	`/setup/firefox/user.ini`
Abschnitt	`browser.tabs`
Eintrag	`closeWindowWithLastTab`
Wert	`false`

Für weitere Informationen siehe Erweiterte Dateieinträge.

7.6.4. Speicherort für Browserdateien

Alle Browser-Einstellungen werden standardmäßig temporär auf dem Flashspeicher gespeichert, sind aber nach einem Neustart nicht mehr verfügbar.

Wenn Sie ein Browser-Homeverzeichnis auf dem Netzwerk angeben, können Browser-Einstellungen wie beispielsweise Bookmarks nach jeder Sitzung gespeichert und dem Benutzer nach einem Neustart wieder zur Verfügung gestellt werden. Verwenden Sie dafür ein Netzlaufwerk, das Sie für den Zugriff konfiguriert haben:

Voraussetzung

Der Zugriff auf ein Windows-Netzlaufwerk ist konfiguriert (Definiertes Laufwerk). Für weitere Informationen siehe Netzlaufwerk definieren.

Speicherort für Firefox-Dateien festlegen

- Geben Sie im Register **Laufwerke** unter **Browser-Homeverzeichnis** ein als Laufwerk definiertes Freigabeverzeichnis aus der linken Liste ein. Der Name muss demjenigen aus der Liste entsprechen. Beispiel: `/smb/share`

Firefox legt die Einstellungsdaten im angegebenen Windows-Verzeichnis im Ordner `mozilla` ab.

Speicherort für Chromium-Dateien festlegen

Voraussetzung

- eLux RP 5.4 oder höher
- Das Netzwerkverzeichnis muss `SMB 2.1` unterstützen (Windows Server 2008 R2 oder höher).

- Definieren Sie mit Hilfe der Funktion die **Erweiterte Konfiguration > Erweiterte Dateieinträge** folgenden Eintrag:

Datei	`/setup/terminal.ini`
Abschnitt	`Chromium`
Eintrag	`Home`
Wert	`<Definiertes Laufwerk>*`

*Samba-Share, wie in Konfiguration > Laufwerke in der Liste angegeben. Beispiel: `/smb/share`

Für weitere Informationen siehe Erweiterte Dateieinträge.

Chromium legt die Einstellungsdaten direkt im angegebenen Windows-Verzeichnis ab.

7.6.5. Kiosk-Modus

Hinweis
Der Kiosk-Modus wird zur Zeit nur für Firefox unterstützt.

Im Kiosk-Modus wird der Browser als Fullscreen-Anwendung geöffnet. Der Benutzer kann keine weiteren Fenster öffnen und den Browser nicht beenden.

Das Browser-Fenster wird standardmäßig ohne Adressleiste und Navigations-Schaltflächen angezeigt. Damit ist der Benutzer gezwungen, auf der freigegebenen vorkonfigurierten Webseite zu bleiben und kann nicht "ausbrechen".

Der Kiosk-Modus ist geeignet, wenn Benutzer nur eine definierte Webseite sehen und keine anderen Programme bedienen sollen. Für diese Funktion ist es sinnvoll, den Browser automatisch zu starten und alle weiteren Zugriffsrechte für den Client einzuschränken. Für weitere Informationen siehe Sicherheit.

Kiosk-Modus konfigurieren

1. Klicken Sie in den Anwendungseigenschaften Ihrer Browser-Anwendung auf die Schaltfläche **Erweitert**.
2. Bearbeiten Sie auf dem Register **Kiosk-Modus** folgende Felder:

Option	Beschreibung
Kiosk-Modus einschalten	Aktiviert den Kiosk-Modus
Navigationsleiste einblenden	Erlaubt die Verwendung von Browser-Tabs trotz aktiviertem Kiosk-Modus Der Benutzer kann mehrere Seiten der definierten Webseite gleichzeitig öffnen.
Druck-Schaltfläche hinzufügen	Erlaubt die Verwendung von Browser-Tabs und stellt eine **Drucken**-Funktion trotz aktiviertem Kiosk-Modus zur Verfügung
Adressleiste hinzufügen	Erlaubt die Verwendung von Browser-Tabs und stellt die Adressleiste mit Navigations-Schaltflächen trotz aktiviertem Kiosk-Modus zur Verfügung

3. Bestätigen Sie mit **Übernehmen** und **OK**.

Beim nächsten Client-Neustart wird der Browser im Kiosk-Modus ausgeführt.

7.7. Lokale und benutzerdefinierte Anwendungen

Der Definition lokaler Kommandos kommt eine besondere Bedeutung zu. Damit ist es möglich, Anwendungen zu definieren, die auch innerhalb einer Shell aufgerufen werden können. Vorausgesetzt werden Kenntnisse über die Kommandos, die ein durchschnittlicher Anwender möglicherweise nicht hat.

Hinweis
Beachten Sie die Berechtigung zum Start der jeweiligen Anwendung. Alle Kommandos werden vom Unix-Benutzer **eLux** ausgeführt (UID = 65534).

Einige lokale Anwendungen sind vordefiniert. Wenn die gewünschte Anwendung in der Liste fehlt, können Sie mit der Option `Benutzerdefiniert` im Listenfeld **Lokale Anwendung** eigene Anwendungen und Kommandos definieren.

Fehlermeldungen werden nicht angezeigt. Wenn das eingegebene Kommando keine X-fähige Anwendung aufruft, wird bei der Ausführung nichts angezeigt. Deshalb empfehlen wir, das Kommando zuerst innerhalb einer XTerm-Sitzung auszuführen und zu testen, um gegebenenfalls Fehlermeldungen zu erhalten.

7.7.1. Vordefinierte lokale Anwendung definieren

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie einen vordefinierten Anwendungstyp aus dem Listenfeld.
Parameter (optional)	Kommandozeilenparameter für den Programmstart
Dauerbetrieb Automatisch starten Desktop-Symbol	siehe Anwendung hinzufügen
Freie Parameter (optional)	Individuelle Parameter für den Anwendungsstart siehe Freie Anwendungsparameter

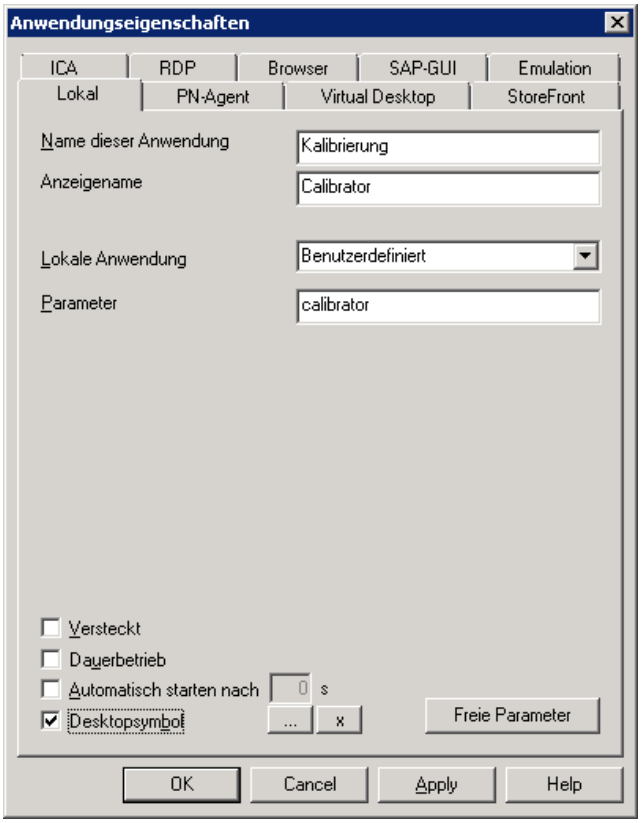
3. Bestätigen Sie mit **Übernehmen** und **OK**.

7.7.2. Benutzerdefinierte Anwendung definieren

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie `Benutzerdefiniert`.
Parameter (erforderlich)	Geben Sie den Programmnamen zum Aufruf der Anwendung ein. Wenn gewünscht, geben Sie zusätzlich Parameter ein, mit denen die Anwendung gestartet werden soll. Beispiel: `calibrator` ruft die Anwendung **Calibrator** auf. `squid` ruft die Anwendung **Squid** auf. `squid /tmp/mycache` ruft **Squid** mit einem bestimmten Cache-Verzeichnis auf.
Versteckt	Die Anwendung wird am Client nicht im Register **Anwendungen** angezeigt. Aktivieren Sie entweder die Option **Automatisch starten** oder die Option **Dauerbetrieb**.
Dauerbetrieb Automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen
Freie Parameter (optional)	Individuelle Parameter für den Anwendungsstart siehe Freie Anwendungsparameter

3. Bestätigen Sie mit **Übernehmen** und **OK**.



Die Abbildung zeigt die Anwendungsdefinition für das Kalibrierungstool **Calibrator**. Nach dem nächsten Neustart steht das Tool **Calibrator** auf dem Client zur Verfügung und kann über die Systemsteuerung, über das Startmenü oder über das Desktop-Symbol aufgerufen werden (vorausgesetzt, das **Calibrator**-Tool ist Bestandteil der Image-Datei).

7.7.3. Ekiga SIP Softphone konfigurieren

Ekiga ist eine freie Software für Audio- und Video-Telefonie (VoIP), die das SIP-Protokoll unterstützt. Die Konfiguration basiert auf einem SIP-Konto.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie in den **Anwendungs-Eigenschaften** das Register **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Frei wählbarer Name
Anwendung	`Benutzerdefiniert`
Parameter	`ekiga`

3. Klicken Sie auf **Freie Parameter** und dann auf **Hinzufügen**, um folgende freie Parameter zu definieren:

Variable	Wert
account	*<Name des SIP-Kontos>*
server	*<ServerURL>*
user	*<SIP Benutzername>*
password	<freies Kennwort>
outbound_proxy	*<ProxyURL >*

Beispiel: `password=424242`
Für weitere Informationen siehe Freie Anwendungsparameter.

4. Klicken Sie im Dialog **Freie Anwendungsparameter** mit der rechten Maustaste auf den Parameternamen `password` und wählen Sie im Kontextmenü **Verschlüsseln**.
5. Bestätigen Sie mit **Übernehmen** und **OK**.

7.8. Emulation

Folgende Emulationen sind verfügbar:

Emulation	Beschreibung
PowerTerm InterConnect	PowerTerm InterConnect der Firma Ericom Software ist ein Terminal-Emulator für Windoes und ermöglicht die Anbindung an IBM Mainframe, IBM AS/400,Unix, VAX/Alpha OpenVMS,Tandem (NSK), HP-3000 und Data General. Das **PowerTerm InterConnect** (powerterm)-Paket muss installiert sein. Die Software ist lizenzpflichtig und ist bei unseren Vertriebspartnern erhältlich.
eterm	eterm ist eine Terminalemulationssuite, die folgende Emulationen enthält: Siemens 97801 (7 & 8 Bit), ANSI, AT386, BA-80, VT320. Das **Eterm 97801 terminal emulation** (eterm)-Paket muss installiert sein. eterm ist kostenfrei in der eLux Lizenz enthalten. Konfigurationshinweise und eine Beschreibung der Tastaturbelegungsdatei zur Erzeugung von Sonderzeichen entnehmen Sie dem eterm Administrationshandbuch im Archiv der Download-Seite.
Virtual Network Computing	Virtual Network Computing (VNC) ist ein Remote Display System. Sie können damit den Desktop und die Umgebung Ihres Computers nicht nur auf dem System anzeigen, auf dem es installiert ist, sondern die Anzeige ist auch über das Intranet oder auch Internet und von einer Vielzahl von Architekturen möglich. Auf dem anzuzeigenden remote-System muss ein VNC Server installiert sein, das lokale Gerät muss einen VNC Viewer haben. Der Dialog **Emulationen** dient zur Konfiguration des VNC Viewers, der als Open Source Komponente kostenlos in die eLux Software integriert ist. Das **VNC client**-Paket des eLux-Pakets **Mirror eLux Desktop** muss installiert sein. Für weitere Informationen siehe Spiegelung im Scout Enterprise-Handbuch.
XDMCP	Das X Display Manager Control Protocol (XDMCP) wird von X Terminals benutzt (wie auch von X Servern im allgemeinen), um eine X-Sitzung mit einem entfernten System über das Netzwerk aufzubauen. Diese Funktionalität ist im BaseOS erhalten. Standardmäßig läuft eine XDMCP-Sitzung auf der eigenen Konsole. Zur Aktivierung des Sounds wählen Sie **Setup > Multimedia** und aktivieren die Option **In XDMCP-Sitzungen Audio verwenden**. Hinweis: Die Anwendung muss kompatibel zum e-sound System sein.
X11	Das X Window System (X11) ist das Standard-Grafiksystem für UNIX und LINUX Betriebssysteme. Es stellt die übliche Windows-Umgebung zur Verfügung und überbrückt damit heterogene Plattformen, unabhängig von Betriebssystem und Hardware. Der X11-Server von The XFree86 Project, Inc. (http://www.xfree86.org) ist im **Xorg**-Paket enthalten und ist Teil des BaseOS.

Emulation	Beschreibung
Tarantella	Tarantella ermöglicht dem Benutzer den Zugriff auf seine Anwendung über eine Web-basierende Schnittstelle. Das **Tarantella Client** (tarantella)-Paket muss installiert sein. Der Server ist lizenziert, der Client nicht. Für weitere Informationen siehe www.tarantella.com.

Für weitere Informationen zur Konfiguration siehe PowerTerm InterConnect konfigurieren und X11-Anwendung konfigurieren im Scout Enterprise-Handbuch.

7.8.1. X11-Anwendung definieren

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **Emulation**.
2. Wählen Sie im Listenfeld **Emulationstyp** den Eintrag `X11`.
3. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung, wird in der Scout Enterprise-Konsole angezeigt
Serveradresse	IP-Adresse oder Name des Unix-Servers
Benutzername	Name des auf dem Unix-System eingetragenen Benutzers
Anwendung	Anwendung mit kompletter Pfadangabe
SSH benutzen	Startet die X11-Sitzung via SSH Berechtigung ist nur über den öffentlichen Schlüssel möglich

4. Bestätigen Sie mit **Übernehmen** und **OK**.

7.8.2. PowerTerm InterConnect konfigurieren

Die Konfiguration von PowerTerm InterConnect erfolgt in zwei Schritten:

- Konfigurieren der PowerTerm-Anwendung auf einem Referenz-Client und Übertragen der erzeugten Konfigurationsdateien
- Konfigurieren der PowerTerm-Anwendung für alle Clients unter Verwendung der Konfigurationsdateien des Referenz-Clients

PowerTerm InterConnect-Anwendung für Referenz-Client definieren

Auf dem Referenz-Client muss das PowerTerm-Paket installiert sein.

1. Definieren Sie lokal oder in der Scout Enterprise-Konsole eine PowerTerm-Anwendung auf dem Referenz-Client, die lediglich den Anwendungsnamen enthält. (Details siehe unten).
2. Starten Sie PowerTerm auf dem Referenz-Client und konfigurieren Sie die Anwendung manuell.

   Die Konfiguration wird im lokalen Verzeichnis `/setup/PowerTerm/` *in folgenden vier Dateien gespeichert:*
   `ptdef.pts`
   `ptdef.ptc`
   `ptdef.ptk`
   `ptdef.ptp`
3. Schließen Sie PowerTerm.
4. Kopieren Sie die vier Konfigurationsdateien mittels Netzwerk oder USB-Stick und stellen Sie sie der Scout Enterprise-Konsole zur Verfügung.
   Oder:
   Übertragen Sie die Konfigurationsdateien remote über **Diagnosedateien anfordern** mittels einer individuellen Vorlage vom Client zur Scout Enterprise-Konsole, siehe Gerätediagnose anpassen.

Die Konfigurationsdateien für die eigentliche PowerTerm-Konfiguration stehen zur Verfügung. Der zweite Schritt kann erfolgen.

PowerTerm InterConnect-Anwendung für beliebige Clients definieren

1. Fügen Sie in der Scout-Enterprise-Konsole für die relevante OU eine neue Anwendung hinzu.
2. Wählen Sie das Register **Emulation** und im Listenfeld **Emulationstyp** den Eintrag `PowerTerm`.
3. Bearbeiten Sie folgende Felder:

Feld	Beschreibung
Name dieser Anwendung	Geben Sie einen beliebigen Namen (ohne Leerzeichen) ein.

Feld	Beschreibung
Parameter	Optionale Aufruf-Parameter für die PowerTerm-Anwendung: `-fullscreen` Vollbild `-maximize` Maximiertes Fenster `-no-menu-bar` keine Menüleiste `-no-tool-bar` keine Toolbar `[myName].pts` Name einer individuellen PowerTerm-Konfigurationsdatei des Clients Beispiel 1: `-fullscreen -no-menu-bar -no-tool-bar` Beispiel 2: `-fullscreen ptconfig001.pts`
Terminal-konfigurationsdatei	Wählen Sie die zu übertragende `.pts`-Datei des Referenz-Clients aus dem Dateisystem.
Kommunikations-datei	Wählen Sie die zu übertragende `.ptc`-Datei des Referenz-Clients aus dem Dateisystem.
Tastaturdatei	Wählen Sie die zu übertragende `.ptk`-Datei des Referenz-Clients aus dem Dateisystem.
Power PAD-Datei	Wählen Sie die zu übertragende `.ptp`-Datei des Referenz-Clients aus dem Dateisystem.
Schaltfläche **x**	Löschen Sie ggf. eine ausgewählte Konfigurationsdatei aus der Scout Enterprise-Datenbank. Zum Löschen der Datei am Client ist der Grundzustand (Factory Reset) des Clients erforderlich.

4. Bestätigen Sie mit **Übernehmen** und **OK**.

PowerTerm InterConnect ist für die Clients der entsprechenden OU ab dem nächsten Start verfügbar.

7.9. SAP GUI

Zur Nutzung dieses Features muss die Software **SAP R/3 client PlatinGUI** (**sapplatingui**) und **IBMJAVA2** installiert sein.

eLux ab Version RL2.10 unterstützt den SAP/R3 Client von SAP AG. Allerdings ist dieses Feature nicht für alle Hardwareplattformen verfügbar. Bitte prüfen Sie im jeweiligen eLux-Container auf www.myelux.com, ob der SAP R/3 Client verfügbar ist.

Systemanforderungen:

- min. 96 MB freier Festplattenspeicher
- min. 128 MB RAM

7.9.1. SAP GUI-Anwendung definieren

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie das Register **SAP GUI**.
2. Geben Sie im Feld **Name** einen aussagekräftigen Namen für die Anwendung in der Konsole ein, und geben Sie im Feld **Anzeigename**[1] einen Namen ein, der am Client angezeigt wird.
3. Aktivieren Sie die Option **Klassische Oberfläche**, wenn Sie das klassische Design von SAP verwenden möchten.
4. Bestätigen Sie mit **Übernehmen** und **OK**.

Es bestehen zwei Möglichkeiten zur Konfiguration:

Lokal am Client	Die Konfiguration wird lokal am Thin Client vorgenommen, wenn der Benutzer den SAP Client zum ersten Mal startet.
Konfiguration durch Administrator	Der Administrator kann eine SAP-Konfigurationsdatei oder Messageserverliste auf die Geräte übertragen. Die SAP Client Konfigurationsdatei ist `/setup/sapgui/platin.ini`. Für weitere Informationen zur Dateiübertragung siehe Erweiterte Konfiguration > Dateien.

Hinweis
Weitere Informationen zur lokalen Konfiguration der SAPGUI und zur SAP-Konfigurationsdatei finden Sie in der SAP-Dokumentation.

[1] ab Scout Enterprise Management Suite Version 14.7

8.1. Problembehandlung

Fehler / Problem	Ursache	Lösung
Fehlende Firmware	Die betreffende Software ist nicht auf dem Thin Client installiert	Installieren Sie die Software auf dem Thin Client. Siehe IDF erstellen im ELIAS-Handbuch und Firmware-Update.
Doppelte Namen	Zwei Anwendungen haben denselben Namen. Dies führt zu Konflikten, da Anwendungen über ihren Namen identifiziert werden.	Vergeben Sie eindeutige Namen.
Versteckte Anwendung wird nicht ausgeführt	Möglicherweise sind Anwendungen für den Benutzer nicht sichtbar, weil sie ausgeblendet (versteckt) wurden. Diese Option ist nur für lokale Anwendungen des Typs **Benutzerdefiniert** verfügbar.	Aktivieren Sie die Option **Automatisch starten nach** bzw. **Dauerbetrieb**, um die versteckte Anwendung beim Systemstart zu starten bzw. dauerhaft am Laufen zu halten.

Fehler / Problem	Ursache	Lösung

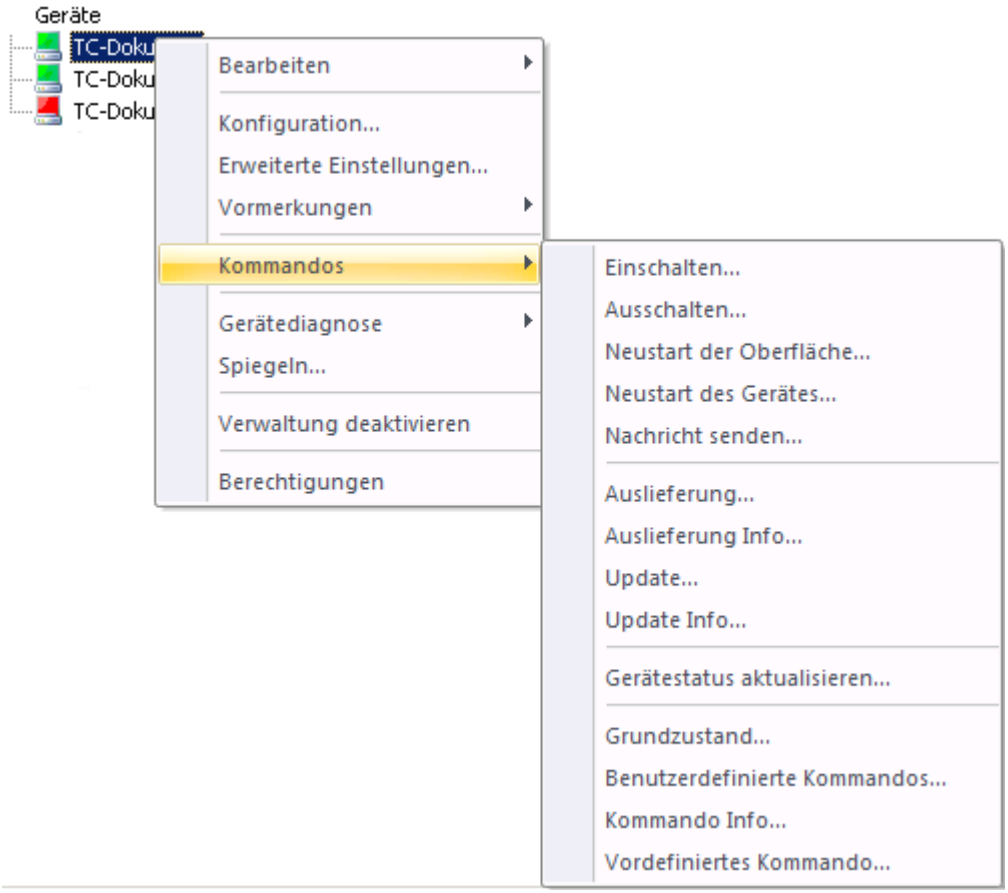
Probleme mit Zertifikaten in Kombination mit VMware View Server	Es liegt ein Server-Problem vor: VMware View Server (>4.5) verwendet nach der Installation ein Self-signed-Zertifikat. Wenn der Client richtig konfiguriert ist, akzeptiert er dieses Zertifikat nicht. Grund: Im CM ist nicht wie für Serverzertifikate zwingend vorgeschrieben, der **FQDN** (fully qualified domain name) eingetragen.	Erstellen Sie ein Serverzertifikat in der Windows-CA mit FQDN.
		In der **MMC** verwenden Sie das Snap-In **Certificates (Local Computer)**.
		
		Der Schlüssel muss exportierbar sein. Die folgenden Schritte hängen von der Version des eingesetzten Servers ab:
		
		A) Ab VMware View Server Version 5.x:
		Der Anzeigenname des Servers muss **vdm** lauten. Im Zertifikatspeicher `Local Computer/Personal` darf nur ein Zertifikat mit diesem Namen existieren.
		
		B) Vor VMware View Server Version 5.x:
		1. Exportieren Sie das Zertifikat einschließlich privatem Schlüssel als: `<Name>.pfx`. Vergeben Sie hierbei ein <*Passwort*>.
		2. Legen Sie die Datei im Verzeichnis: `C:\Programme\VmWare\VmWareView\Server\sslgateway\conf` ab.
		3. Editieren Sie in demselben Verzeichnis die Datei `locked.properties` und fügen die folgenden Zeilen ein:
		`keyfile=<Name>.pfx`
		`keypass=<Passwort>`
		4. Starten Sie den VMware View Connection Server neu.

9. Client-Fernverwaltung durch Kommandos

Mit den Scout Enterprise-Kommandos kann der Administrator den Zustand der Geräte ändern, Updates ausführen und Nachrichten senden. Die Kommandos können sofort oder zu einem definierbaren Zeitpunkt einmalig oder periodisch ausgeführt werden.

Die Kommandos können auf einzelne Geräte, auf OUs oder auf Dynamische Gerätegruppen angewendet werden.

Im Kontextmenü einzelner Geräte finden Sie zusätzlich Kommandos zu Gerätediagnose und Spiegelung.



9.1. Verfügbare Kommandos

Im Kontextmenü für einzelne Geräte, OUs oder Dynamische Gerätegruppen stehen unter **Kommandos** folgende Optionen zur Verfügung, die jeweils den Dialog **Kommando ausführen/einplanen** öffnen:

Kommando	Beschreibung
Einschalten...	Schaltet das Gerät/die Geräte ein
Ausschalten...	Schaltet das Gerät/die Geräte aus

Kommando	Beschreibung
Neustart des Gerätes...	Startet das Gerät/die Geräte neu
Neustart der Oberfläche	Startet die eLux-Oberfläche neu
Nachricht senden...	Sendet eine Nachricht an das Gerät/die Geräte Der Nachrichtentext kann mithilfe von HTML-Tags formatiert werden. Der Titel des Nachrichten-Fensters kann angepasst werden.
Auslieferung...	Liefert Software für ein Firmware-Update aus
Update...	Führt ein Firmware-Update durch
Gerätestatus aktualisieren...	Sendet eine Statusanfrage an das Gerät/die Geräte und aktualisiert den Gerätestatus des Gerätes in der Scout Enterprise-Konsole
Grundzustand...	Setzt das Gerät/die Geräte zurück auf den Grundzustand Die Konfiguration wird gelöscht, die Image-Datei bleibt unverändert. Scout Enterprise-Serveradresse und Lizenzen bleiben am Client erhalten, außer Sie aktivieren die Optionen • Scout Enterprise-Serveradresse am Client löschen (analog Grundzustand lokal am Client) • Am Client gespeicherte Lizenzen löschen (z.B. für den Abverkauf)
Benutzerdefinierte Kommandos...	Sendet ein benutzerdefiniertes Kommando an das Gerät/die Geräte, beispielsweise ein Skript zum BIOS-Update. **Hinweis** Nach der Ausführung eines benutzerdefinierten Kommandos können Sie nach Ablauf von 30 Sekunden ein weiteres benutzerdefiniertes oder Update-Kommando absetzen.
Vordefiniertes Kommando...	Bietet benutzerdefinierte Kommandos, die global vordefiniert wurden. Für weitere Informationen siehe Vordefinierte Kommandos.
Konfigurationslauf...	Bereitet die Client-Konfigurationsinformationen für eine OU oder Dynamische Gerätegruppe vor. Für weitere Informationen siehe Konfigurationslauf. Dieses Kommando kann nicht auf ein einzelnes Gerät angewendet werden.

Folgende Optionen öffnen die jeweilige Protokolldatei:

Kommando	Beschreibung
Auslieferung Info...	Öffnet das Logfile der letzten Software-Auslieferung
Update Info...	Öffnet das Logfile des letzten Firmware-Updates
Kommando Info...	Öffnet das Logfile des letzten Benutzerdefinierten Kommandos

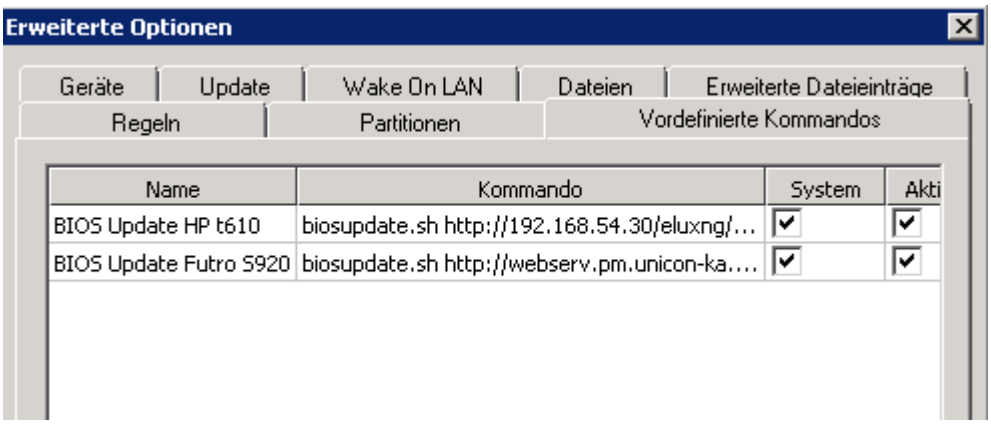
9.2. Vordefinierte Kommandos

Benutzerdefinierte Kommandos können zentral vordefiniert und den Administratoren über **Kommandos > Vordefiniertes Kommando...** zur Verfügung gestellt werden. Beispielsweise können Sie Skripts zum BIOS-Update bestimmter Modelle als Kommando vordefinieren. Diese Kommandos sind anschließend im Listenfeld für vordefinierte Kommandos auswählbar.

Vordefinierte Kommandos definieren

1. Wählen Sie im Scout Enterprise-Menü **Optionen > Erweiterte Optionen > Vordefinierte Kommandos**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Bearbeiten Sie den neuen Eintrag durch Klick in die Felder **Name** und **Kommando**.

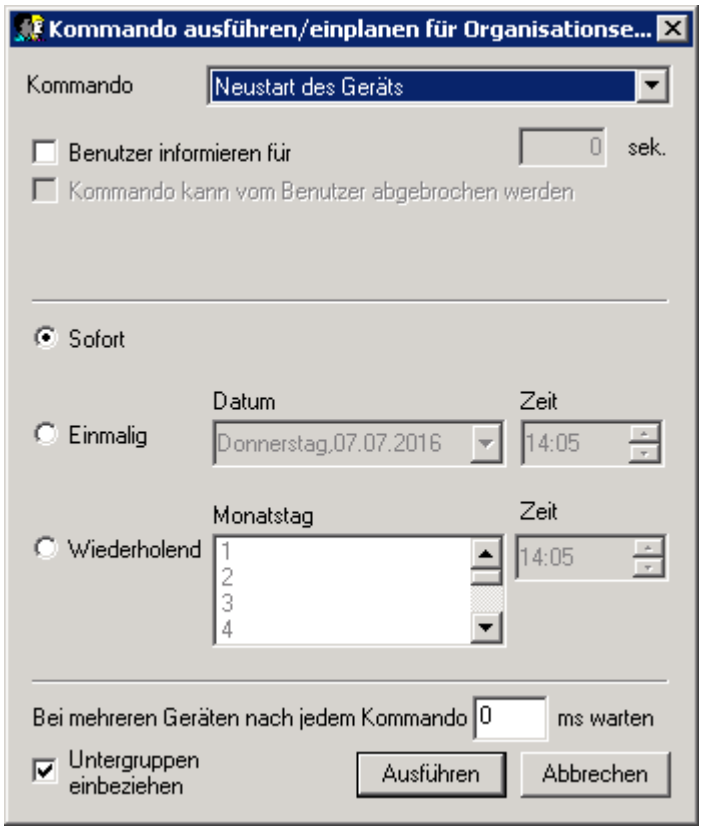
   *Der im Feld **Name** angegebene Kommandoname wird den Administratoren im Kommando-Dialog angezeigt; das eigentliche Kommando wird nicht angezeigt.*
4. Um das Kommando mit Systemrechten auszuführen, lassen Sie die Option **System** aktiv.
5. Um das Kommando im Listenfeld für vordefinierte Kommandos anzuzeigen, lassen Sie die Option **Aktiviert** aktiv.
6. Bestätigen Sie mit **Übernehmen** und **OK**.



*Alle aktiven vordefinierten Kommandos stehen unter **Kommandos > Vordefiniertes Kommando...** im Listenfeld **Auswahl** zur Verfügung und können auf einzelne Geräte, auf OUs oder auf Dynamische Gerätegruppen angewendet werden.*

9.3. Kommando ausführen/einplanen

1. Öffnen Sie für das relevante Gerät, die OU oder die Dynamische Gerätegruppe das Kontextmenü und wählen Sie **Kommandos**.
2. Wählen Sie aus dem Untermenü das gewünschte Kommando.



*Das Fenster **Kommando ausführen/einplanen** öffnet. Je nach ausgewähltem Kommando können die Optionen variieren.*

*Im Listenfeld **Kommando** sind alle Kommandos verfügbar.*

3. Um den Inhalt der Fenstertitelzeile vollständig anzuzeigen, bewegen Sie den Mauszeiger auf die Fenstertitelzeile.
4. Legen Sie fest, ob und wie lang der Benutzer informiert werden soll, und ob der Benutzer das Kommando abbrechen darf.
5. Legen Sie fest, wann das Kommando ausgeführt werden soll und ob es wiederholt werden soll.
6. Wenn mehrere Geräte betroffen sind, können Sie je nach Kommando eine Wartezeit nach jedem abgesetzten Kommando definieren.
7. Wenn eine OU betroffen ist, definieren Sie, ob Sie die **Untergruppen einbeziehen** möchten.
8. Bestätigen Sie mit **Ausführen**.

Das Kommando wird zum definierten Zeitpunkt ausgeführt. Je nach Kommando wird eine Meldung angezeigt, die Sie bestätigen müssen.

9.4. Kommando-Ergebnisse pro Gerät

Rückmeldungen über durchgeführte Update-, Auslieferungs- und benutzerdefinierte Kommandos erhalten Sie sowohl gerätespezifisch im jeweiligen **Eigenschaften**-Fenster als auch geräte-unabhängig im Fenster **Kommandoverlauf**. Alle Vorgänge werden aufgezeichnet, auch wenn das Kommando abgebrochen wurde oder gar nicht ausgeführt wurde, da beispielsweise bei einem Update-Kommando die entsprechende IDF aktuell war. Vollständig durchgeführte Kommandos werden grün gekennzeichnet.

Kommando-Ergebnisse für ein Gerät anzeigen

Hinweis
Die folgende Anleitung bezieht sich auf Update-Kommandos. Die Anzeige für Auslieferungs- und benutzerdefinierte Kommandos funktioniert entsprechend.

1. Zeigen Sie das Eigenschaften-Fenster an: **Ansicht > Fenster > Eigenschaften**.

   *Das **Eigenschaften**-Fenster wird als permanentes Fenster im rechten Bereich angezeigt. Für das markierte Gerät werden relevante Eigenschaften angezeigt. Eigenschaften können über das*  *Icon eingeblendet oder ausgeblendet werden.*

2. Markieren Sie das relevante Gerät in der Baumstruktur.

   *Im **Eigenschaften**-Fenster werden unter **Update** folgende Felder angezeigt:*

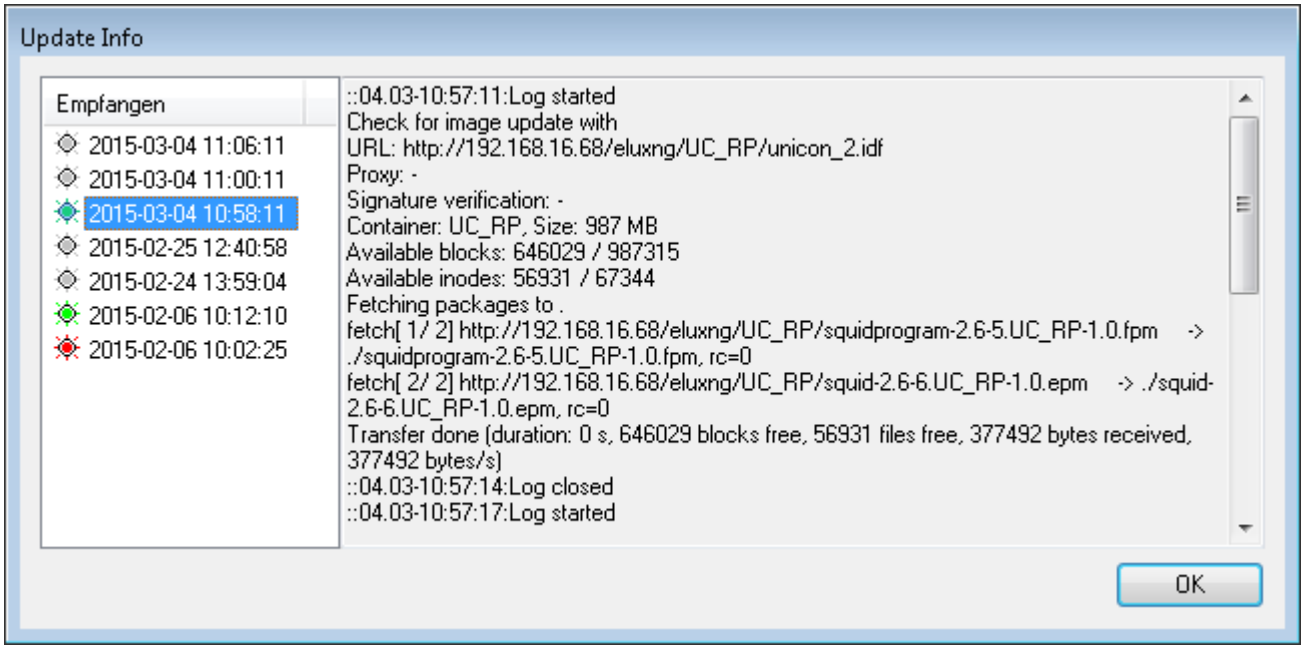
Image	Aktuelle IDF-Datei
Update-Zeitpunkt	Exakter Zeitpunkt der letzten Update-Ausführung
Update-Status	Aktueller Status wie z.B. `Update läuft`, `Update erfolgreich`, `Update nicht erforderlich`
Update-Provider[1]	Herkunft der Software-Pakete (Webserver oder Proxy)
Update-Größe	Größe der übertragenden Software-Pakete im komprimierten Format

3. Doppelklicken Sie auf den Begriff **Update-Status** oder klicken Sie auf **...** am Zeilenende.

   *Der Dialog **Update Info** wird angezeigt. Links werden alle Update-Vorgänge angezeigt. Ein Update-Vorgang kann erfolgreich abgeschlossen, abgebrochen oder nicht durchgeführt sein, da die IDF-Datei aktuell war. Für ein markiertes Update werden rechts alle Protokoll-Informationen*

[1] Ab Scout Enterprise Management Suite Version 14.8

angezeigt, darunter auch die installierten Software-Pakete.



.

Hinweis

Die Information über das letzte Update dieses Gerätes finden Sie alternativ über das Kontextmenü des Gerätes und **Kommandos > Update-Info...**

Alle durchgeführten Kommandos werden unabhängig vom Gerät im Fenster **Kommandoverlauf** angezeigt. Für weitere Informationen siehe Kommandoverlauf.

9.5. Kommandoverlauf

Den Kommandoverlauf für die Kommandos **Update**, **Auslieferung** und **Benutzerdefiniert** können Sie für alle betroffenen Geräte abfragen. Hierbei werden die Berechtigungen der Administratorenverwaltung berücksichtigt.

- Wählen Sie **Ansicht > Kommandoverlauf....**

*Das Fenster **Kommandoverlauf** öffnet und zeigt pro Zeile einen sogenannten Job (Kommando für 1 bis n Geräte) mit folgenden Informationen:*

Feld	Beschreibung
Typ	Objekttyp, auf den das Kommando angewendet wird. Hierbei kann es sich um ein einzelnes Gerät, eine Organisationseinheit mit (OU+) oder ohne untergeordneten OUs (OU) oder um eine Dynamische Gerätegruppe (DGG) handeln.
Name	Objektname (Gerätename, OU-Name oder Name der Dynamischen Gerätegruppe)
Kommando	Ausgeführtes Kommando (Update, Auslieferung oder Benutzerdefiniertes Kommando)
Geräte	Anzahl der betroffenen Geräte
Start	Datum und Uhrzeit der Kommandoübermittlung an die Geräte / Start-Zeitpunkt
Ende	Datum und Uhrzeit der Kommandoübermittlung an die Geräte / Ende-Zeitpunkt Das Job-Ende ist erreicht, wenn alle Geräte `Erfolgreich` oder `Fehler` zurückgemeldet haben, oder wenn die Timeout-Zeit von 5 Minuten für die Rückmeldung abgelaufen ist. Bei Job-Abbruch durch den Administrator wird der Abbruch-Zeitpunkt als Ende des Jobs ausgewiesen.
Erfolgreich	Anzahl der Geräte, die das Kommando erfolgreich verarbeitet haben
Fehler	Anzahl der Geräte, die einen Fehler bei der Kommandoverarbeitung zurückgemeldet haben
Timeout	Anzahl der Geräte, die innerhalb der vorgegebenen Zeit von 5 Minuten kein Resultat der Kommandoverarbeitung zurückgemeldet haben
Fortschritt %	Prozentualer Fortschritt der Kommandoverarbeitung über alle betroffenen Geräte
Administrator	Administrator, der das Kommando ausgeführt hat

Auf die Liste der angezeigten Jobs können Sie folgende Funktionen anwenden:

Funktion	Aktion
Ansicht aktualisieren	Drücken Sie die F5-Taste.
Tabellenzeilen sortieren	Klicken Sie auf die relevante Spaltenüberschrift. *Der erste Klick sortiert die Jobs aufsteigend nach dem ausgewähltem Wert; der zweite Klick sortiert absteigend.* *Klick auf die F5-Taste stellt die Standardsortierung wieder her.*

Auf einen markierten Job können Sie folgende Funktionen anwenden:

Funktion	Aktion
Details einsehen	Klicken Sie auf **Details...**. *Im Fenster **Kommandodetails** werden die Verlaufsinformationen der betroffenen Geräte detailliert dargestellt. Neben dem Start- und Endezeitpunkt finden Sie hier den aktuellen Status und das Ergebnis der Kommandoausführung pro Gerät.*
Objekt in der Baumansicht der Scout Enterprise-Konsole suchen	Klicken Sie mit der rechten Maustaste auf einen Objektnamen und wählen Sie **In Baumansicht suchen**. *Der erste Treffer wird in der Baumansicht markiert.*
Laufenden Job beenden	Markieren Sie den Job mit Status `Läuft` und klicken Sie auf **Beenden**. *Eine Beendigungsanforderung für das Kommando wird an den Scout Enterprise-Server gesendet. Die Übermittlung des Kommandos an die Geräte wird dadurch gestoppt.*

10. Fernwartung

Für Wartung, Benutzer-Support und zur Überprüfung bestimmter Funktionalitäten auf den Clients stehen dem Administrator verschiedene Werkzeuge zur Verfügung

10.1. Spiegelung

Hinweis
Diese Funktion kann nur auf ein einzelnes Gerät angewendet werden.

Der Administrator kann Terminal-Sessions spiegeln, d.h. sich auf die Sitzung eines Benutzers aufschalten (Session Shadowing). Auf dem gespiegelten Computer kann die Kontrolle von Maus und Tastatur an die spiegelnde Person gegeben werden. Dadurch können Support- und Wartungsaufgaben remote durchgeführt werden. Auch Client Updates oder neu installierte Programme können so auf korrekte Funktonalität überprüft werden.

10.1.1. Voraussetzungen

- Auf dem Administrationssystem muss ein VNC-Viewer installiert sein. Dieser wird zur Verfügung gestellt über
  - die Scout Enterprise-Konsole oder
  - die Scout Enterprise Mirror App, um unabhängig von Scout Enterprise zu spiegeln
- Auf dem zu spiegelnden Gerät muss ein VNC-Server installiert sein .
  Für eLux-Clients wird der Spiegelungsserver mit der **VNC Server extension**, einer Komponente des **XOrg**-Paketes installiert. Diese Komponente muss in der IDF-Datei des Clients enthalten sein.
- Für das Zielgerät muss in **Konfiguration > Sicherheit > Spiegelungseinstellungen** die Spiegelung aktiviert und konfiguriert sein. Für weitere Informationen siehe Spiegelung konfigurieren.

10.1.2. Spiegeln mit der Scout Enterprise-Konsole

Während einer Spiegelungssitzung wird der Benutzer durch eine Systemmeldung über die Spiegelung informiert. Die Systemmeldung wird für die Dauer der Spiegelungssitzung auf den Bildschirmen von Benutzer (Gespiegelter) und Administrator (Spiegelnder) angezeigt und erlaubt dem Gespiegelten jederzeit, die Sitzung zu beenden.

Spiegelungssitzung eröffnen

Hinweis

- Bei Clients mit zwei angeschlossenen Monitoren werden beide Monitore gespiegelt, sodass für eine optimale Darstellung auch am Scout Enterprise-PC zwei Monitore mit mindestens derselben Auflösung angeschlossen sein sollten.
- Innerhalb der Spiegelungssitzung wird die Tastaturbelegung des lokalen Systems (PC mit Scout Enterprise) und nicht die des Clients verwendet.

1. Öffnen Sie für das relevante Gerät das Kontextmenü und wählen Sie **Spiegeln...**.

   *Der **Spiegeln**-Dialog öffnet.*

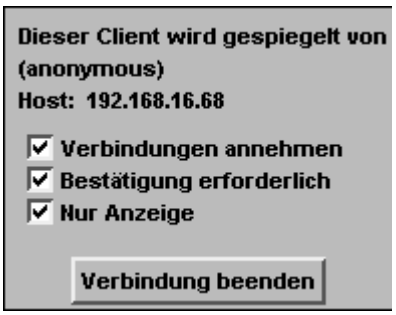
2. Wählen Sie im Feld **Sitzungstyp**, ob Sie den Desktop oder eine bestimmte Sitzung spiegeln möchten:

Option	Beschreibung
Desktop	Spiegelt den eLux Desktop (Display 0)
XDMCP 1	Spiegelt die erste geöffnete XDMCP Sitzung (Display 1)
XDMCP 2	Spiegelt die zweite geöffnete XDMCP Sitzung (Display 2)

3. Bestätigen Sie mit **OK**.
4. Wenn in **Konfiguration > Sicherheit** konfiguriert, geben Sie das erforderliche Kennwort ein. Für weitere Informationen siehe Spiegelung konfigurieren.

   Je nach Konfiguration muss der Benutzer die Spiegelung bestätigen.

Die Spiegelungssitzung startet. Auf dem Client-Bildschirm öffnet für die Dauer der Spiegelungssitzung eine Systemmeldung, die über die Spiegelung informiert und nicht geschlossen werden kann.



Folgende Optionen kann der Benutzer festlegen:

Option	Beschreibung
Verbindungen annehmen	Wenn deaktiviert, kann keine Verbindung vom Spiegelnden mehr hergestellt werden.

Option	Beschreibung
Bestätigung erforderlich	Vor dem Aufbau einer Spiegelungssitzung muss der Benutzer bestätigen. Nach Ablauf von 10 Sekunden wird die Verbindung automatisch verweigert.
Nur Anzeige	Der Administrator darf nur lesend auf das gespiegelte Gerät zugreifen. Maus- und Tastatureingaben des Administrators werden nicht in die gespiegelte Sitzung übertragen.

Die Spiegelungssitzung wird beendet, wenn der Administrator das Sitzungsfenster schließt oder wenn der Benutzer in der Systemmeldung auf die Schaltfläche **Verbindung beenden** klickt.

10.1.3. Spiegeln mit der Scout Enterprise Mirror App

Um eine erhöhte Serverlast zu vermeiden und die Helpdesk-Möglichkeiten zu erweitern, steht eine gesonderte Anwendung zur Verfügung, die die Spiegelung ohne Scout Enterprise-Konsole ermöglicht. Die Berechtigungen der Scout Enterprise-Administratorenverwaltung werden berücksichtigt.

Spiegelung mit der Scout Enterprise Mirror App konfigurieren

1. Aktivieren Sie in der Scout Enterprise-Konsole für die relevanten Clients in **Konfiguration > Sicherheit > Spiegeleinstellungen > Erweitert** die Option **Nur von Scout Enterprise erlauben**.

   Oder lokal am Client:

   Aktivieren Sie in der Systemsteuerung in **Setup > Sicherheit > Spiegeleinstellungen > Erweitert** die Option **Nur von Scout Enterprise erlauben**.

   Das Spiegeln ist von der Scout Enterprise-Konsole und von der Scout Enterprise Mirror App erlaubt, andere Tools sind ausgeschlossen. Dadurch ist die Anwendung der in Scout Enterprise festgelegten Zugriffsrechte sichergestellt.

   Für weitere Informationen zur Konfiguration siehe Spiegelung konfigurieren.

2. Aktivieren Sie in der Scout Enterprise-Konsole im Menü **Sicherheit > Administratoren verwalten > Objektrechte** die entsprechenden Administratoren-Objektrechte: `Spiegelung durchführen` und `Sichtbar`.

3. Stellen Sie sicher, dass im Menü **Sicherheit > Administratoren verwalten > Basisrechte** die Berechtigung für `Scout Enterprise Mirror verwenden` gesetzt ist.

4. Downloaden und installieren Sie das Programm **Scout Enterprise Mirror Application** von www.myelux.com.

Die Scout Enterprise Mirror Application wird an die Scout Enterprise-Datenbank angebunden und zum Aufruf im Startmenü zur Verfügung gestellt.

Spiegeln mit der Scout Enterprise Mirror App

1. Starten Sie die App aus dem Windows-Startmenü.

2. Geben Sie die IP-Adresse, den Host-Namen oder die MAC-Adresse des zu spiegelnden Gerätes an und klicken Sie auf **Starten**.

Für weitere Informationen zum Ablauf der Spiegelungssitzung, siehe Spiegeln mit der Scout Enterprise-Konsole.

10.2. Gerätediagnose

Hinweis
Diese Funktion kann nur auf ein einzelnes Gerät angewendet werden.

Die Gerätediagnose dient zum Ausführen definierter Kommandos auf dem Client und zum Übertragen von Konfigurations- und Protokolldateien vom Client zu Diagnosezwecken. Die angeforderten Client-Dateien unterstützen den Administrator bei der Fehleranalyse und werden beim Anlegen eines Support-Tickets angefragt.

Die Funktion kann auch eingesetzt werden, um frei zu definierende Dateien vom Client anzufordern.

10.2.1. Diagnosedateien anfordern

Hinweis
Vor der Gerätediagnose sollte die erweiterte Protokollierung beim Client temporär eingeschaltet werden. Dadurch werden mehr Dateien und mehr Informationen angefordert. Nach der Gerätediagnose sollte die erweiterte Protokollierung wieder ausgeschaltet werden, um die Flashspeicher-Kapazität des Clients nicht unnötig zu strapazieren.

1. Öffnen Sie für das relevante Gerät das Kontextmenü und wählen Sie **Konfiguration...**.
   Schalten Sie auf dem Register **Allgemein** die Option **Übergeordnete Instanz verwenden** aus.
   Setzen Sie auf dem Register **Diagnose** die Option **Protokollierungsstufe** auf `Ein`.
   Bestätigen Sie und führen Sie einen Neustart des Clients durch.

   Der Protokollierungsparameter am Client wird gesetzt.

2. Öffnen Sie für das relevante Gerät das Kontextmenü und wählen Sie den Eintrag **Gerätediagnose > Dateien anfordern...**.

   *Der Dialog **Diagnosedateien bearbeiten** öffnet.*

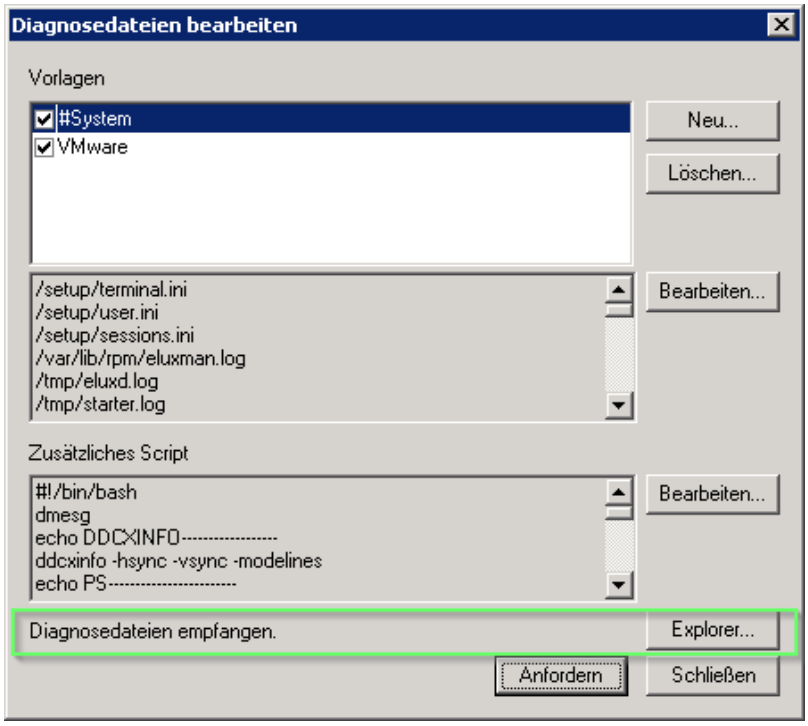
   *Unter **Vorlagen** werden alle definierten Vorlagen angezeigt. Eine Vorlage kann Datei-Listen und Skript enthalten. Nur aktive Vorlagen (mit Haken) werden berücksichtigt. Die vordefinierte Vorlage `#System` ist immer aktiv.*

3. Wenn Sie berechtigt sind, können Sie weitere Vorlagen aus der Liste aktivieren oder deaktivieren.

4. Klicken Sie auf die Schaltfläche **Anfordern**.

   Alle Skripte, die in den aktiven Vorlagen definiert sind, werden ausgeführt.

   Alle Dateien, die in den aktiven Vorlagen definiert sind, werden angefordert und vom Client als ZIP-Datei übertragen. Die ZIP-Datei wird im lokalen Benutzer-Verzeichnis `<user-profile>\Documents\UniCon\Scout\Console\Diag` oder ähnlich gespeichert.



*Scout Enterprise gibt im unteren Bereich des Dialogs Rückmeldung. Wenn die Diagnosedateien empfangen wurden, wird die Schaltfläche **Explorer...** angezeigt.*

5. Klicken Sie auf die Schaltfläche **Explorer**.

   Der Datei-Explorer öffnet mit dem Diagnose-Zielverzeichnis.
   Die aktuelle ZIP-Datei enthält die angeforderten Diagnose-Dateien.

6. Öffnen Sie in Scout Enterprise für das relevante Gerät das Kontextmenü und wählen Sie **Konfiguration...**.
   Setzen Sie im Register **Diagnose** die Option **Protokollierungsstufe** auf `Aus`.
   Schalten Sie auf dem Register **Allgemein** die Option **Übergeordnete Instanz verwenden** ein.

   Die erweiterte Protokollierung ist wieder zurückgesetzt und die Vererbung wiederhergestellt.

Hinweis
Wenn Sie außerhalb der Diagnose frei definierte Dateien über eine eigene Vorlage anfordern möchten, fallen Schritt 1 und 6 weg.

10.2.2. Diagnosedateien konfigurieren

Für die Gerätediagnose über das Kommando **Diagnosedateien anfordern** ist eine Vorlage `#System` vordefiniert. Diese Vorlage enthält eine Datei-Liste mit relevanten Konfigurations- und Protokolldateien sowie Script-Code. Beide Komponenten sind nicht editierbar und werden bei jeder Gerätediagnose über **Anfordern** ausgeführt.

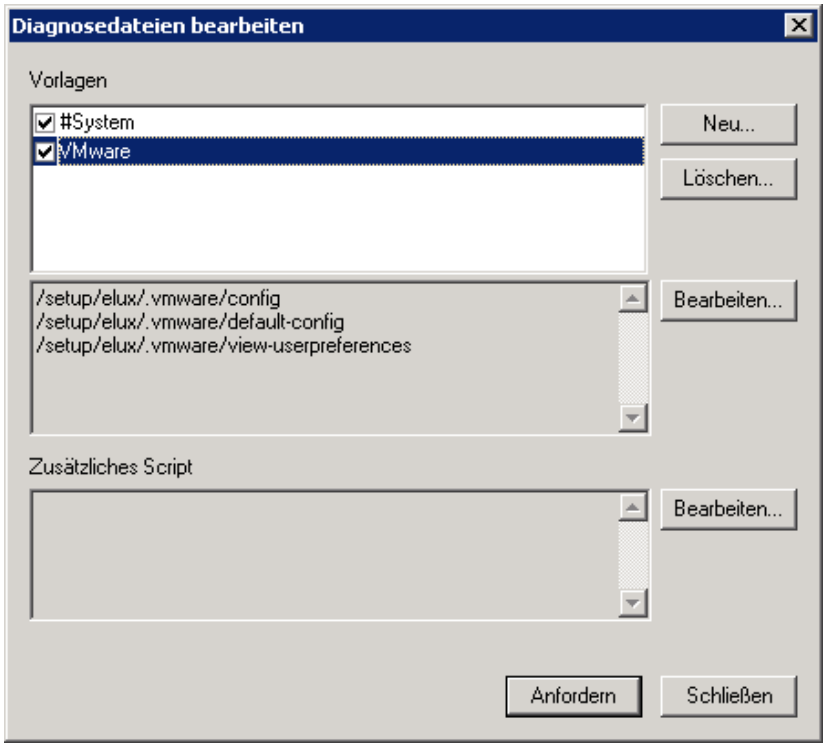
Zusätzlich können Sie eigene Vorlagen definieren, die sowohl Dateien als auch Script enthalten können. Die Vorlagen sind global verfügbar.

Vorlage für Gerätediagnose definieren

1. Öffnen Sie das Kontextmenü eines Gerätes und wählen Sie den Eintrag **Gerätediagnose > Dateien anfordern**.

   *Der Dialog **Diagnosedateien bearbeiten** öffnet. Unter **Vorlagen** wird die vordefinierte Vorlage `#System` angezeigt und ggf. weitere Vorlagen*

2. Klicken Sie auf die Schaltfläche **Neu**, geben Sie Ihrer neuen Vorlage einen Namen und bestätigen Sie mit **OK**.
3. Markieren Sie die neue Vorlage und klicken Sie auf die Schaltfläche **Bearbeiten...** neben der Datei-Liste.
4. Geben Sie im Textfenster die relevanten Dateien mit Pfad zeilenweise ein.
   Bestätigen Sie mit **Speichern**.



5. Um Code zu definieren, der auf dem Client ausgeführt werden soll, klicken Sie neben **Zusätzliches Script** auf die Schaltfläche **Bearbeiten...** und geben Sie im Textfenster den auszuführenden Code ein.
   Bestätigen Sie mit **Speichern**.

Hinweis

Beim Ausführen der Gerätediagnose über **Anfordern** werden alle aktiven Vorlagen berücksichtigt. Ob alle in der Vorlage `#System` definierten Dateien geschrieben und geholt werden, hängt von der eingestellten Protokollierungsstufe ab. Für weitere Informationen siehe Gerätekonfiguration > Register Diagnose.

10.2.3. Konfiguration vergleichen (Soll – Ist)

Hinweis
Diese Funktion kann nur auf ein einzelnes Gerät angewendet werden.

Der Konfigurationsvergleich überprüft, ob die Einstellungen des Clients (IST) identisch mit den am Scout Enterprise-Server definierten Konfigurationen (SOLL) sind.

- Öffnen Sie für das relevante Gerät das Kontextmenü und wählen Sie den Eintrag **Gerätediagnose > Setupvergleich**.
  Oder:
  Markieren Sie das relevante Gerät und verwenden Sie die Tastenkombination STRG-E.

Die Konfiguration des ausgewählten Clients wird mit den aktuell hinterlegten Werten in der Scout Enterprise-Datenbank verglichen. Eigenschaften, deren Werte sich unterscheiden, werden in einem Fenster aufgelistet.

Hinweis
Um die Konfiguration **zwischen** OUs oder Geräten zu vergleichen, blenden Sie das Fenster **Konfigurationsvergleich** ein. Für weitere Informationen siehe Konfiguration zwischen OUs/Geräten vergleichen.

11. Firmware-Update

Die Thin Clients enthalten bei Auslieferung bereits Betriebssystem und Anwendungen wie ICA-Client, RDP-Client, Browser und Emulationen. Die auf dem Flash-Speicher gespeicherte Software, die Firmware, kann aktualisiert werden, wenn neue Software-Versionen vorliegen oder wenn sich die Anforderungen ändern und z.B. Komponenten hinzugefügt oder entfernt werden sollen.

Wesentliche Schritte

- Download der entsprechenden Software-Pakete von myelux.com
- Anpassen der Image-Definitionsdatei am Webserver mit Hilfe von ELIAS
- Überprüfen der Firmware-Konfiguration der relevanten Clients
- Ausführen des Updates
  - Auslieferung der Software
  - Installation der neuen Software am Client

Das Ausführen des Updates kann entweder in einem Schritt als Update-Kommando durchgeführt werden. Dabei werden die Softwarepakete übertragen und automatisch installiert. Alternativ können die beiden Aktionen entkoppelt werden (ab Scout Enterprise Management Suite Version 14.6) und zunächst mit einem Kommando die Software ausgeliefert werden, bevor in einem zweiten Schritt die Installation der Software per Update-Kommando gestartet wird.

Hinweis
Um Bandbreite zu sparen, können Sie zum Updaten bestimmter Clients einen Proxy einsetzen, siehe Update über Proxy-Client..

Auslösen eines Firmware-Updates

Updates können sofort durchgeführt oder zu einem definierten Zeitpunkt automatisch ausgelöst werden:

- Firmware-Updates können mit Hilfe des **Update-Kommando** ausgeführt oder einplant (einmalig oder periodisch) werden.
- Die Geräte können so konfiguriert werden, dass sie automatisch beim Ein- oder Ausschalten der Clients auf eine neue IDF-Version prüfen und ggf. updaten
- Das Setzen einer **Update-Vormerkung** führt zum Ausführen eines Firmware-Updates beim nächstem Einschalten der Clients

Wenn konfiguriert, kann der Benutzer die Durchführung des Updates verschieben.

Updates werden nur dann ausgeführt, wenn die relevante IDF-Datei verändert wurde. Alle Update-Aktivitäten werden protokolliert.

Auswahl der betroffenen Geräte

Kommandos und Vormerkungen können Sie auf folgende Geräte und Gruppen anwenden:

- Einzelne Geräte
- Mehrere Geräte, die Sie im Fenster **Alle Geräte** markieren (Mehrfachauswahl mit STRG und UMSCHALT zulässig)
- OU
- Dynamische Gerätegruppe

Die Option **Auf neue Version prüfen** ist Teil der **Gerätekonfiguration > Firmware** und kann auf einzelne Geräte, OUs und alle Geräte angewendet werden.

Recovery-Installation

Wenn Sie Geräte komplett in den Auslieferungszustand zurücksetzen möchten, können Sie eine Recovery-Installation durchführen. Wenn kritische Feature-Pakete des BaseOS aktualisert worden sind oder die installierte Betriebssystemversion zu alt ist, kann ebenfalls ein Recovery notwendig werden. Eine Recovery-Installation zerstört alle Daten auf dem Speichermedium unwiederbringlich (bis auf die Lizenzen) und installiert die eLux-Software. Für weitere Informationen siehe Recovery-Verfahren in der Recovery-Kurzanleitung.

11.1. Voraussetzungen

Sie benötigen folgende Komponenten, um ein Firmware-Update durchzuführen:

- Scout Enterprise-Server mit Scout Enterprise-Konsole zur Konfiguration des Firmware-Updates für die Clients
- Das Tool ELIAS zur Erstellung und Änderung von Image Definition Files (IDF) im Software-Container
- Webserver (HTTP, HTTPS, FTP, FTPS) mit Container-Verzeichnis für eLux Software-Pakete und Image Definition Files
- zu installierende eLux-Software-Pakete

Scout Enterprise-Server und -Konsole mit ELIAS können Sie von www.myelux.com herunterladen. In der Standard-Installation sind diese Komponenten enthalten.

Das aktuelle Software-Bundle `eLux`*`version`*`_AllPackages.zip` und weitere Software-Pakete können Sie von www.myelux.com herunterladen.

Als Webserver empfehlen wir den Microsoft IIS oder einen anderen Webserver, beispielsweise Apache.
Die entsprechende Webserver-Rolle muss aktiviert sein.

11.2. Update-Partition

Neuere eLux-Versionen erzeugen eine Update-Partition auf Geräten mit der notwendigen Flash-Speichergröße. Eine Update-Partition ermöglicht folgende Funktionen:

- Software-Verteilung vor Update
- Client kann als dynamischer Proxy eingesetzt werden
- Signaturprüfung für eLux Software-Pakete

In folgenden Fällen erzeugt eLux eine Update-Partition auf dem Client:

eLux-Version (Minimum)	Flash-Speicher (Minimum)	Erzeugung der Update-Partition bei
eLux RP 4.6.1	2 GB	• PXE-Recovery oder • USB-Recovery oder • Firmware-Update mit Flash-Formatierung vor dem Update
eLux RP 5.1	4 GB	
eLux RP 5.3	4 GB	Systemstart – sofern neben der System-Partition (2 GB) noch keine Update-Partition vorhanden ist

Die Größe der Update-Partition richtet sich nach dem verfügbaren Speicherplatz. Bei eLux RP 5.3-Clients beträgt sie mindestens 2 GB und maximal 14 GB.

11.3. Update planen

Hinweis
Die folgende Schrittanleitung schließt die Firmware-Konfiguration der Clients ein. Für wiederholte Updates können bei entsprechender Konfiguration Schritt 1 und 2 ausreichen: Eine aktualisierte IDF-Datei führt zum Firmware-Update der mit dieser IDF konfigurierten Clients.

1. Wenn die relevante Software nicht im Container enthalten ist, laden Sie die entsprechenden Pakete herunter und importieren sie. Für weitere Informationen siehe Pakete in einen Container importieren im ELIAS-Handbuch.
2. In ELIAS erweitern Sie die relevante IDF-Datei um die relevanten Software-Features. Für weitere Informationen siehe IDF erstellen im ELIAS-Handbuch.
3. Öffnen Sie für die relevante OU oder für das relevante Gerät den Dialog **Konfiguration**. Wenn Sie das Update für alle Clients durchführen möchten, öffnen Sie den Dialog **Optionen > Basiskonfiguration**.
4. Überprüfen Sie im Register **Firmware** die korrekte Konfiguration für das Firmware-Update, insbesondere die Angaben in den Feldern **Protokoll**, **Server**, **Pfad** und **Image-Datei**.

*Aus diesen Werten wird die unter dem Feld **Pfad** angezeigte URL-Adresse generiert, die für die Übertragung von Image-Datei und eLux-Software-Paketen relevant ist.*

Die angegebene IDF-Datei muss mit der in ELIAS aktualisierten IDF-Datei identisch sein.

5. Wenn Sie das Update beim Ein- oder Ausschalten der Clients durchführen möchten, wählen Sie im unteren Bereich des Registers **Firmware** die entsprechende Option **Auf neue Version prüfen**.

   Da das Update vom Client initiiert wird, werden die lokal am Client gespeicherten Firmware-Parameter verwendet.

   Für weitere Informationen zur Konfiguration des Firmware-Updates siehe Geräte-Konfiguration/Firmware.
   Wenn Sie Updates über einen Proxy einspielen möchten, siehe Update über Proxy-Client.
6. Bestätigen Sie mit **OK**.

Das Firmware-Update ist für die relevanten Clients konfiguriert.

Hinweis
Soabld eine aktualisierte IDF-Datei vorliegt, und wenn eine der Optionen **Auf neue Version prüfen** aktiv ist, wird das Update beim nächsten Starten bzw. Ausschalten der Clients eingespielt.

Alternativ können Sie das Update mit folgenden Methoden auslösen:

- Update-Kommando ausführen
- Update-Kommando für bestimmten Zeitpunkt einplanen (einmalig oder periodisch)
- Update-Vormerkung setzen

Für weitere Informationen siehe Update über Kommando ausführen und Update über Vormerkung ausführen.

11.4. Update über Kommando ausführen

Hinweis
Wenn Sie die Software-Verteilung vom Einspielen der Updates entkoppeln möchten, verwenden Sie das Kommando **Auslieferung**.

Hinweis
Wenn Sie dem Anwender die Möglichkeit zum Verschieben geben möchten, muss dies für die relevanten Geräte in **Firmware > Erinnerung...** konfiguriert sein. Mit der Option zur Verschiebung des Updates kann der Anwender den Zeitpunkt des Firmware-Updates durch ein Update-Kommando selbst steuern. Für weitere Informationen siehe Verschiebung des Updates durch den Anwender.

1. Wählen Sie im Kontextmenü für ein Gerät, OU oder Dynamische Gerätegruppe **Kommandos > Update...**

   *Der Dialog **Kommando ausführen** öffnet.*

2. Wenn Sie den Benutzer informieren möchten, aktivieren Sie die Option **Benutzer informieren für**.

   Die Option aktiviert die Systemmeldung zum Firmware-Update am Client und gibt dem Anwender damit die Möglichkeit, den Update-Vorgang zu beeinflussen.

   *Wenn die **Anzahl der erlaubten Verschiebungen** von Firmware-Updates in den **Erinnerungseinstellungen** auf 1 oder höher konfiguriert ist, kann der Anwender im Dialog der Systemmeldung das angeforderte Firmware-Update verschieben.*

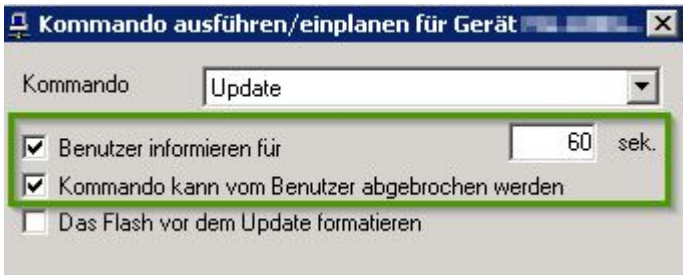
   - *Geben Sie die Anzeigedauer der Systemmeldung in Sekunden ein.*

     *Während dieser Zeit hat der Anwender die Möglichkeit, vor dem Firmware-Update offene Anwendungen zu schließen und sich ggf. aus bestehenden Sitzungen abzumelden. Innerhalb dieser Zeit kann der Anwender auch das Firmware-Update um einen auswählbaren Zeitraum (wie bei **Verzögerungen bis zur nächsten Erinnerung** definiert) verschieben.*

     Wenn Sie die Anzeigedauer auf 0 Sekunden belassen, wird die Systemmeldung solange angezeigt, bis der Anwender auf eine Schaltfläche klickt.

   - Wenn gewünscht, schalten Sie die Option **Kommando kann vom Benutzer abgebrochen werden** ein.

     *Die Systemmeldung am Client zeigt die Schaltfläche **Abbrechen**, damit kann der Anwender das Firmware-Update endgültig abbrechen. Es erfolgt kein automatischer Wiederanlauf des Vorgangs.*



3. Um den Flash-Speicher der Clients vor dem Beschreiben zu formatieren, aktivieren Sie die Option **Flash vor dem Update formatieren**.
4. Legen Sie den Zeitpunkt der Ausführung fest.
   Für weitere Informationen siehe Kommando ausführen.
5. Klicken Sie auf **Ausführen**.

*Der Update-Vorgang wird zum definierten Zeitpunkt angestoßen. Der Update-Status wird für jedes einzelne Gerät im **Eigenschaften**-Fenster angezeigt. Für weitere Informationen siehe* Update-Protokoll.

Beachten Sie, dass ein Update nur dann ausgeführt wird, wenn die relevante IDF-Datei verändert wurde. Wenn ein Update nicht ausgeführt werden konnte, wird kein Versuch unternommen, den Vorgang zu wiederholen.

Hinweis
Wenn Sie ein **Update**-Kommando durchführen, werden die relevanten Informationen als URL an die Clients übermittelt. Hierbei werden die Werte aus **Geräte-Konfiguration > Firmware** verwendet, die zum Zeitpunkt der Kommando-Ausführung eingetragen sind. Beachten Sie, dass dies bei Initiierung durch den Client (Ein- oder Ausschalten) die lokale **Firmware**-Konfiguration ist.

11.5. Update über Vormerkung ausführen

Clients können so konfiguriert werden, dass immer beim Ein- und Ausschalten auf eine neue IDF-Version geprüft wird und, sobald ein neueres IDF vorliegt, ein Updates ausgeführt wird.[1] Über eine Update-Vormerkung können Sie jedoch einmalig eine Update-Anforderung an bestimmte Clients senden, die bei der nächsten Verbindung zum Client ausgewertet wird und ein Update auf das in der Scout Enterprise-Konsole in der Firmware-Konfiguration konfigurierte IDF ausführt.

1. Markieren Sie ein Gerät, eine OU, eine Dynamische Gerätegruppe oder Geräte im Fenster **Alle Geräte**.
2. Wählen Sie im Kontextmenü die Option **Vormerkungen > Firmware-Aktualisierung veranlassen...**

   *Der Dialog **Firmware-Aktualisierung veranlassen** wird angezeigt.*
3. Legen Sie fest, ob und wie lang der Benutzer informiert werden soll, und ob der Benutzer das Kommando abbrechen darf.
4. Um die Systempartition vor dem Update zu formatieren, aktivieren Sie die entsprechende Option.
5. Bestätigen Sie die Vormerkung und die Bestätigung.

   Die Vormerkungen für das Firmware-Update werden gesetzt.

   *Für alle vorgemerkten Geräte wird im **Eigenschaften**-Fenster im Feld **Firmwareaktualisierungsvormerkung** der Status `Aktiviert` angezeigt.*

   Hinweis
   Wenn das Feld **Firmwareaktualisierungsvormerkung** im **Eigenschaften**-Fenster nicht angezeigt wird, klicken Sie auf die Schaltfläche  , um die anzuzeigenden Felder zu konfigurieren.
6. Wenn Sie die Update-Vormerkung für ein oder mehrere Geräte löschen möchten, verwenden Sie die Kontextmenü-Option **Vormerkungen >Aktualisierungsvormerkung löschen**.

Das Firmware-Update ist für die relevanten Clients vorgemerkt. Sobald ein Gerät neu startet und Verbindung zum Scout Enterprise-Server aufnimmt, erhält es eine Update-Anforderung und die Firmwareaktualisierungsvormerkung wird automatisch gelöscht.

[1] **Firmware > Auf neue Version prüfen**

*Je nach Konfiguration in der Vormerkung und in **Gerätekonfiguration > Firmware > Erinnerung** wird das Update sofort gestartet oder der Benutzer erhält eine Systemmeldung mit Optionen zum Verschieben. Für weitere Informationen siehe* Auswirkungen beim Update mit Verschieben-Option.

*Der Update-Status wird für jedes einzelne Gerät im **Eigenschaften**-Fenster angezeigt. Für weitere Informationen siehe* Update-Protokoll.

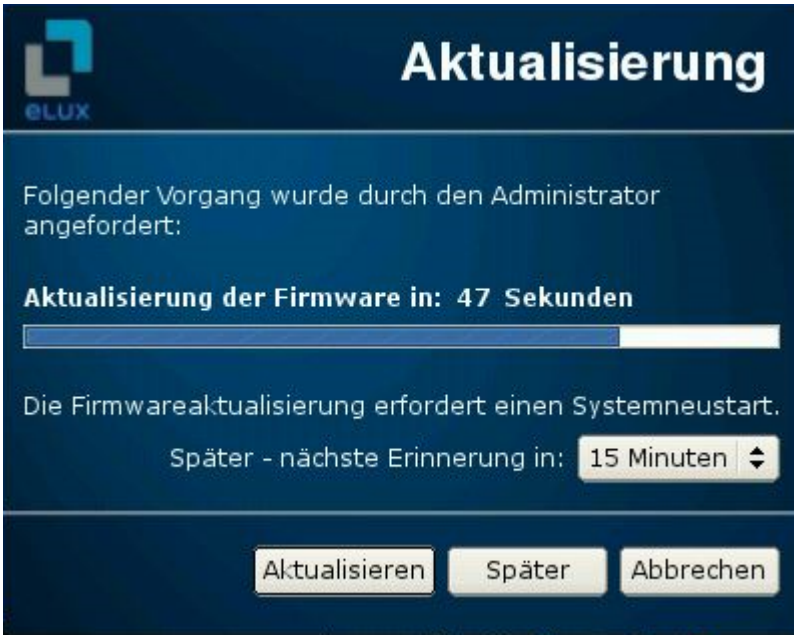
Beachten Sie, dass ein Update nur dann ausgeführt wird, wenn die relevante IDF-Datei verändert wurde. Wenn ein Update nicht ausgeführt werden konnte, wird kein Versuch unternommen, den Vorgang zu wiederholen.

Bei Geräten ohne Update-Partition kann es vorkommen, dass eine Update-Anforderung angezeigt wird, obwohl kein Update erforderlich ist. Sobald der Benutzer auf die Schaltfläche **Aktualisieren** klickt, wird das Fenster ausgeblendet und es findet kein Update statt.

Hinweis
Im Scout Enterprise-Reportgenerator können Sie Geräte nach dem Feld **Firmwareaktualisierungsvormerkung** auswerten.

11.6. Auswirkungen beim Update mit Verschieben-Option

Ein **Update**-Kommando mit aktivierter Option **Benutzer informieren** führt zu einer Systemmeldung mit den konfigurierten Optionen für den Anwender. Wenn in **Firmware > Erinnerung...** konfiguriert, werden dem Anwender entsprechende Schaltflächen zum Verschieben und Abbrechen des Updates zur Verfügung gestellt.



Option	Beschreibung
Später - nächste Erinnerung in	Auswahlliste für den Zeitintervall bis zur nächsten Erinnerung an das Firmware-Update, enthält die Werte gemäß **Verzögerungen bis zur nächsten Erinnerung** Wird nur dann angezeigt, wenn die **Anzahl der erlaubten Verschiebungen** von Firmware-Updates `1` oder höher ist, und wenn noch mindestens eine Verschiebung für den Anwender möglich ist
Schaltfläche **Aktualisieren**	Update der Firmware sofort durchführen
Schaltfläche **Später**	Update der Firmware um den gewählten Zeitintervall verschieben Wenn der Client vor Ablauf des Zeitintervalls heruntergefahren wird, erfolgt das Update während des Ausschaltens. Wird dann angezeigt, wenn die **Anzahl der erlaubten Verschiebungen** von Firmware-Updates `1` oder höher ist, und wenn noch mindestens eine Verschiebung für den Anwender möglich ist
Schaltfläche **Abbrechen**	Update der Firmware endgültig abbrechen Wird dann angezeigt, wenn die Option **Kommando kann vom Benutzer abgebrochen werden** aktiv ist

11.7. Software getrennt ausliefern

Bevor Sie ein Firmware-Update durchführen, können Sie die erforderlichen Software-Pakete in einem getrennten Schritt verteilen. Erst wenn die Auslieferung der Software auf allen Geräten erfolgreich war, starten Sie die Installation über ein Update-Kommando.

Voraussetzung

Die folgende Schrittanleitung setzt eine korrekte Firmware-Konfiguration der relevanten Clients voraus. Für weitere Informationen siehe Update planen.
Weiterhin gelten folgende Voraussetzungen:

- Scout Enterprise Version 14.6 oder höher
- eLux RP 5.2 oder höher
- Clients verfügen über eine Update-Partition.

1. Öffnen Sie für das relevante Gerät oder OU das Kontextmenü und wählen Sie **Kommandos > Auslieferung...**.
2. Legen Sie fest, ob und wie lang der Benutzer informiert werden soll, und ob der Benutzer das Kommando abbrechen darf.
3. Wenn Sie die Update-Partition der Clients vor dem Beschreiben bereinigen möchten, aktivieren Sie im Dialog **Kommando ausführen** die Option **Update-Partition vor der Auslieferung bereinigen**.
4. Legen Sie den Zeitpunkt der Ausführung fest.
   Für weitere Informationen siehe Kommando ausführen.

5. Klicken Sie auf **Ausführen**.

Der Auslieferungs-Vorgang wird zum definierten Zeitpunkt angestoßen. Wenn eine aktualisierte IDF-Datei vorliegt, und wenn die erforderlichen Software-Pakete noch nicht auf der Update-Partition des Clients vorhanden sind, wird die Auslieferung gestartet. Das System lädt nur diejenigen Pakete herunter, die noch nicht vorhanden sind. Vor jeder Übertragung wird der freie Speicherplatz geprüft. Wenn weniger als 30 MB zur Verfügung stehen, werden alte Pakete gelöscht.

Während der Auslieferung wird am Client ein grüner Pfeil als Systray-Symbol angezeigt. Wenn der Administrator im ***Kommando****-Dialog die Option* ***Kommando kann vom Benutzer abgebrochen werden*** *aktiviert hat, kann der Benutzer im Popup-Dialog* ***Ausliefungskontrolle*** *die Schaltfläche* ***Auslieferung abbrechen*** *anklicken.*

Der Auslieferungs-Status wird für jedes Gerät in der Scout Enterprise-Konsole im ***Eigenschaften****-Fenster angezeigt. Für weitere Informationen siehe* Kommando-Ergebnisse pro Gerät*.*

Hinweis

Die anschließende Installation der Software-Pakete und die Aktualisierung auf das neue IDF initiieren Sie mit einem Update-Kommando.

11.8. Statischer Proxy-Client

Wenn Sie beispielsweise schmalbandig angebundene Thin Clients mit einem Firmware-Update aktualisieren möchten, können Sie einen Proxy-Client einsetzen, der die Updates weitergibt. Proxy-Clients downloaden die benötigten Software-Pakete und verteilen sie an die anderen Clients.

Als Proxyserver kommt die freie Software Squid zum Einsatz.

Hinweis

- Voraussetzung für den Einsatz eines Proxy-Clients ist eine Arbeitsspeichergröße von mindestens 1 GB RAM, da die Pakete lokal im RAM des Proxy-ThinClients vorgehalten werden. Abhängig von der Gesamtgröße der Pakete, die in der IDF-Datei definiert sind, kann auch mehr RAM erforderlich sein.
- Squid unterstützt kein `HTTPS`, da der Cache-Mechanismus bei Datenübertragung mit HTTPS-Protokoll nicht genutzt werden kann. Verwenden Sie Signaturen, um den Update-Prozess sicherer zu machen. Für weitere Informationen siehe Firmware-Sicherheit durch Signatur.

Die Konfiguration in Scout Enterprise beinhaltet drei Schritte:

- Anwendungsdefinition für Squid erstellen
- Proxy-Client einrichten
- Relevante Geräte für das Proxy-Update konfigurieren

Anwendungsdefinition für Squid erstellen

1. Erstellen Sie eine eigene OU für den Proxy-Client.
2. Definieren Sie in der OU eine neue lokale Anwendung, siehe Anwendung hinzufügen.
3. Wählen Sie im Register **Lokal** folgende Einstellungen:

Option	Wert
Name dieser Anwendung	`Squid`
Lokale Anwendung	`Benutzerdefiniert`
Parameter	`squid`
Versteckt	Ein
Automatisch starten nach 0 Sekunden	Ein

4. Verschieben Sie den Proxy-Client in diese OU und starten Sie den Client neu.

Der Client übernimmt die Squid-Anwendungsdefinition.

Proxy-Client einrichten

1. Installieren Sie auf dem Proxy-Client ein Firmware-Image, das das Squid-Paket enthält. Passen Sie dafür das IDF in ELIAS an. Für weitere Informationen siehe Update planen.

   Nach dem Neustart ist Squid auf dem Proxy-Client installiert.

2. Öffnen Sie für die OU des Proxy-Clients **Konfiguration > Allgemein** und deaktivieren Sie die Option **Übergeordnete Instanz verwenden**.

   Die Vererbung wird unterbrochen und die Proxy-OU kann unabhängig konfiguriert werden.

3. Lassen Sie in **Konfiguration > Firmware**, wenn Sie HTTP verwenden, die Felder **Benutzer** und **Kennwort** leer.

4. Wählen Sie für den Proxy-Client **Konfiguration > Netzwerk > LAN**, markieren Sie den ersten Eintrag und klicken Sie auf **Bearbeiten**.
   Wählen Sie im Dialog **Netzwerkprofil bearbeiten** die Option **Folgende IP-Adresse verwenden**.
   Lassen Sie das Feld **Domäne** leer und bestätigen Sie mit **OK**.

   Die zuletzt bezogene IP-Adresse wird als feste IP-Adresse vom Proxy-Client weiterverwendet.

Geräte für das Update über den Proxy konfigurieren

1. Öffnen Sie für die OU oder das Gerät, das über den Proxy aktualisiert werden soll, den Dialog **Konfiguration**.
   Wenn Sie den Proxy für alle Clients definieren möchten, öffnen Sie den Dialog **Optionen > Basiskonfiguration**.

2. Bearbeiten Sie auf dem Register **Firmware** folgende Felder:

Protokoll	`HTTP`
Proxy	`<IP-Adresse Proxy-Client>:3128`
Benutzer und Kennwort	*<kein Eintrag>*

3. Bearbeiten Sie die weiteren Felder wie gewohnt, siehe Geräte-Konfiguration/Firmware.

Die relevanten Clients bekommen ihre Firmware-Updates vom Proxy-Client, sobald die Konfiguration aktiv ist.

11.9. Dynamischer Proxy-Client

Auch dynamische Proxy-Clients können für die Softwarepaket-Verteilung an alle Clients eines Subnetzes eingesetzt werden. Ein dynamischer Proxy-Client ist ein automatisch ausgewähltes Gerät eines Subnetzes, das die benötigten Software-Pakete vom konfigurierten Webserver downloadet und anschließend den anderen Clients seines Subnetzes zur Verfügung stellt.

Die Lösung basiert auf den Geräterollen **Provider** und **Consumer**.

Das voll automatisierte Provisioning (Provider) und Discovering (Consumer) des Proxy-Services innerhalb von Subnetzen ist in eLux RP mit der zero-configuration networking-Implementierung Avahi realisiert.

11.9.1. Voraussetzungen

Um Updates über einen dynamischen Proxy-Client durchführen zu können, müssen neben dem Betriebssystem eLux folgende Pakete auf den Geräten eines Subnetzes installiert sein:

- dynamicproxy-*xxx*.UC_RP-*x*
- avahi-*xxx*.UC_RP-*x*
- squid-*xxx*.UC_RP-*x*

11.9.2. Rahmenbedingungen und Rollen

Das Konzept des dynamischen Proxy-Clients basiert auf folgenden Rollen:

Provider

Der Provider ist das Gerät, das als Dynamischer Proxy-Client agiert. Alle Geräte mit einer Update-Partition kommen für die Provider-Rolle in Frage. Sobald ein Gerät als Provider gewählt wurde, verbleibt es in der Provider-Rolle für nachfolgende Updates. Wenn ein Provider zum Update-Zeitpunkt nicht verfügbar ist, übernimmt ein anderes Gerät mit Update-Partition die Provider-Rolle. Der Provider wird automatisch und dynamisch gewählt.

Um bestimmte Geräte von der Provider-Rolle auszuschließen, bearbeiten Sie die lokale Datei `/setup/terminal.ini`.

1. Verwenden Sie die **Erweiterte Dateieinträge**-Funktion der Scout Enterprise-Konsole, um die `ini`-Datei zu bearbeiten. Für weitere Informationen siehe Individuelle Dateieinträge festlegen.

Option	Wert
Datei	`/setup/terminal.ini`
Abschnitt	`DynamicProxy`
Eintrag	`UseProvider`
Wert	`false`

Consumer

Alle Clients eines Subnetzes, die nicht die Provider-Rolle haben, sind Consumer. Die Consumer führen ihre Updates über den Subnetz-Provider durch und müssen daher keine Software-Pakete vom Webserver downloaden.

Um bestimmte Geräte von der Consumer-Rolle auszuschließen, bearbeiten Sie die lokale Datei `/setup/terminal.ini`.

- Verwenden Sie die **Erweiterte Dateieinträge**-Funktion der Scout Enterprise-Konsole, um die `ini`-Datei zu bearbeiten. Für weitere Informationen siehe Individuelle Dateieinträge festlegen.

Option	Wert
Datei	`/setup/terminal.ini`
Abschnitt	`DynamicProxy`
Eintrag	`UseConsumer`
Wert	`false`

Hinweis
In der Firmware-Konfiguration dürfen die Felder **Benutzer** und **Kennwort** bei Verwendung von HTTP keinen Eintrag erhalten.

11.9.3. Update-Verfahren

Auf Updates prüfen

Im Fall einer Update-Anforderung, die entweder durch den Scout Enterprise-Server oder durch die lokale **Firmware**-Konfiguration (**Auf neue Version beim Start/Ausschalten prüfen)** ausgelöst werden kann, downloaden die Consumer die neueste IDF-Datei vom Webserver und prüfen, ob ein Update notwendig ist.

Proxy-Service ermitteln

Wenn weitere Software-Pakete benötigt werden, versuchen die Consumer, den Provider im Subnetz zu ermitteln. Wenn kein Provider im Subnetz existiert, übernimmt eines der Geräte mit Update-Partition im Subnetz automatisch die Provider-Rolle und stellt den Proxy-Service zur Verfügung.

Software-Pakete downloaden

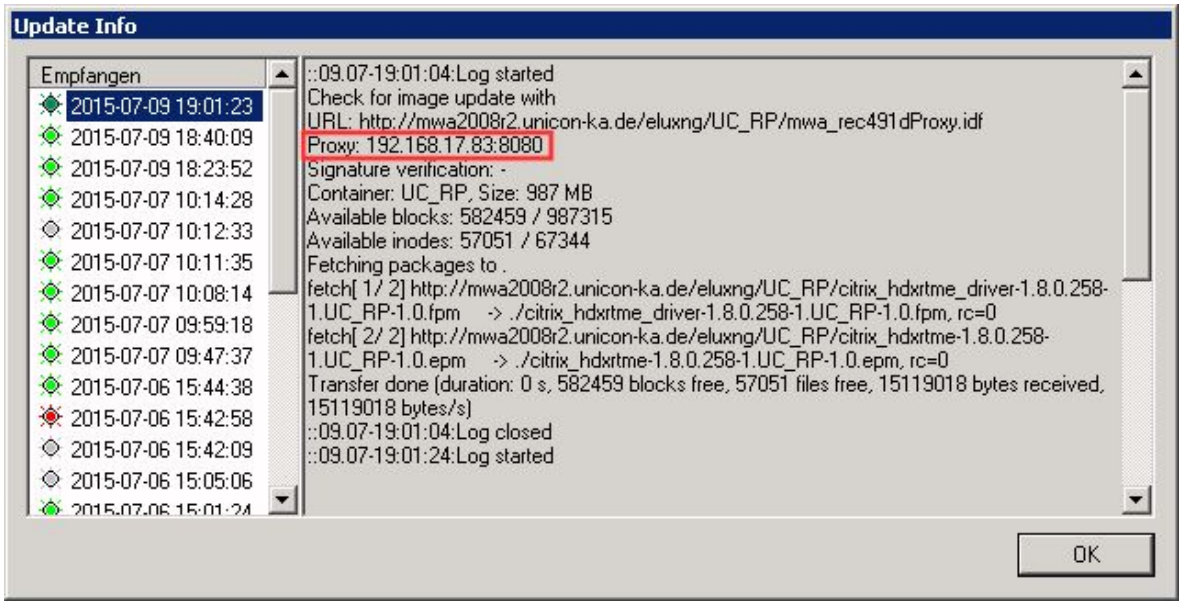
Der Provider überprüft, ob die angeforderten Software-Pakete auf seiner Update-Partition vorhanden sind und lädt fehlende Pakete von dem oder den Webservern herunter, die von den Consumern angegeben wurden.

Software-Pakete verteilen und installieren

Die Software-Pakete werden vom Provider zu den Consumern übertragen und die Consumer installieren die Pakete. Dabei gehen Geräte ohne Update-Partition im Rythmus 'ein Paket holen - ein Paket installieren usw.' vor, während Geräte mit Update-Partition alle benötigten Pakete in einem Schritt holen und sie anschließend installieren. Erst nachdem der letzte Consumer mit allen Paketen versorgt worden ist, aktualisiert der Provider, falls notwendig, sein eigenes System.

Die Update-Vorgänge werden sowohl für die Consumer als auch für den Provider aufgezeichnet:

- Für jedes aktualisierte Gerät können Sie die **Update Info** durch Doppelklick auf **Update Status** im **Eigenschaften**-Fenster anzeigen. Hier wird auch der Provider angegeben, der den Proxy-Service durchgeführt hat.
  Für weitere Informationen siehe Update-Protokoll.



- Der Provider hat eine lokale Datei `/tmp/dynamic-proxy.log`, die die Consumer auflistet, die mit Software-Paketen versorgt wurden.

11.10. Problembehandlung

Fehlermeldungen

Fehlermeldung	Ursache	Lösung
Falscher Container	Container sind hardwarespezifisch	Prüfen Sie, ob Ihr Container zu Ihren Client-Spezifikationen passt.
Falsche Flashspeicher-Größe	Größe des IDF übersteigt vorhandenen Speicherplatz	Überprüfen Sie, ob die in Ihrem IDF definierte Gesamtgröße der Software-Pakete der tatsächlichen Größe des Client-Flashspeichers entspricht.
Falsches Kennwort	Falsches Gerätekennwort	Korrigieren Sie die Eingabe in **Setup > Sicherheit**.
Client benötigt eine Recovery-Installation	Wenn kritische Feature-Packages (`.fpm`) im Base OS aktualisiert werden, benötigt der Thin Client eine Recovery-Installation vor dem Update.	Für weitere Informationen siehe Recovery-Verfahren in der Recovery-Kurzanleitung.

Update-Optionen

Sollte das Update weiterhin fehlerhaft sein, hilft es möglicherweise, die Update-Einstellungen zu ändern. Für weitere Informationen siehe Update-Optionen in der **Erweiterten Konfiguration**.

12. Kennwörter

12.1. Lokales Gerätekennwort

Das Geräte-Kennwort betrifft die lokalen Geräte. Alle Thin Clients, die von einem Scout Enterprise Server verwaltet werden, erhalten dasselbe Gerätekennwort.

Das Geräte-Kennwort ist erforderlich zur Verifizierung der Zugriffsrechte auf die Thin Clients. Scout Enterprise benötigt dieses Kennwort, wenn der Administrator beispielsweise ein Discovery ausführen möchte.

Das Geräte-Kennwort kann nur zentral in Scout Enterprise geändert werden. Im Auslieferungszustand lautet das Kennwort `elux`.

Normalerweise hat der Benutzer keine Zugriffsrechte auf die lokale Konfiguration im Register **Sicherheit**. Wenn jedoch der Administrator das Gerätekennwort lokal in der Systemsteuerung eines Clients ändert, kann der Client nicht mehr durch Scout Enterprise verwaltet werden.

Hinweis
Ändern Sie das Kennwort sofort, um unberechtigte Gerätekonfigurationen durch die lokalen Benutzer zu verhindern.

Für weitere Informationen siehe Gerätekennwort im eLux-Handbuch.

12.1.1. Lokales Geräte-Kennwort zentral über Scout Enterprise ändern

Achtung
Mit dieser Funktion ändern Sie das Geräte-Kennwort für **alle** mit diesem Scout Enterprise-Server verwalteten Clients.

1. Wählen Sie in der Scout Enterprise-Konsole **Optionen > Basiskonfiguration... > Sicherheit** und klicken Sie unter **Lokale Sicherheitseinstellungen** auf die Schaltfläche **Bearbeiten**.

   *Der Dialog **Benutzereigenschaften** öffnet.*

2. Geben Sie im Feld **Geräte-Kennwort** das neue Kennwort ein und wiederholen Sie das Kennwort im Feld **Geräte-Kennwortbestätigung**.
3. Bestätigen und schließen Sie den Dialog mit **OK**.

Mit dem nächsten Geräte-Neustart wird den Clients das neue Geräte-Kennwort vom Scout Enterprise Server übermittelt.

Hinweis
Um das neue Geräte-Kennwort sofort zu aktivieren, führen Sie einen Neustart der betroffenen Geräte (sofort oder zeitgesteuert) durch. Verwenden Sie dazu das Scout Enterprise-Kommando **Neustart des Geräts**. Für weitere Informationen siehe Kommando ausführen/einplanen.

12.1.2. Lokales Gerätekennwort am Thin Client ändern

1. Wählen Sie in der eLux-Systemsteuerung **Setup > Sicherheit**.
2. Klicken Sie unter **Lokale Sicherheit** auf **Bearbeiten**.
3. Geben Sie das neue Kennwort in beide Felder ein und bestätigen Sie mit **OK**.

Achtung

Der Client kann ab sofort nicht mehr durch Scout Enterprise verwaltet werden.

12.2. Scout Enterprise Konsolen-Kennwort

Das Standard-Konto `Administrator` mit Konsolen-Kennwort ist nur dann aktiv, wenn die Option **Administratorenverwaltung aktivieren** nicht aktiv ist.

Im Auslieferungszustand ist die Administratorenverwaltung ausgeschaltet und das Konsolen-Kennwort lautet `elux`.

Hinweis

Ändern Sie das Kennwort sofort, um unberechtigten Zugriff zu verhindern.

- Um das Konsolen-Kennwort zu ändern, melden Sie sich als Administrator an und wählen **Optionen > Konsolen-Kennwort ändern...**. Geben Sie die entsprechenden Daten im Dialog ein.

  oder

- Aktivieren Sie die Administratorenverwaltung.

  Sobald die Administratorenverwaltung eingeschaltet ist, ist das Standard-Konto mit Konsolen-Kennwort nicht mehr aktiv.

Wir empfehlen, die Administratorenverwaltung zu aktiveren und Ihre AD-Konten als Scout Enterprise-Konten anzupassen.

13. Administratorenverwaltung

13.1. Administratorenverwaltung aktivieren

Um mehrere Scout Enterprise-Administratoren zu verwalten, muss die Administratorenverwaltung eingeschaltet werden. Scout Enterprise Administratoren-Konten basieren auf AD-Konten, die bereits existieren müssen. Scout Enterprise Administratoren-Konten können in vielerlei Hinsicht konfiguriert werden.

Standardmäßig ist die Administratorenverwaltung nicht aktiv.

Hinweis
Um die Administratorenverwaltung einzuschalten, müssen Sie als Administrator mit Vollzugriff eingeloggt sein. Standardmäßig steht das Konto `Administrator` mit Kennwort `elux` zur Verfügung.

1. Wählen Sie in der Scout Enterprise-Konsole den Menübefehl **Sicherheit > Administratorenverwaltung aktivieren**.
2. Bestätigen Sie mit **OK**.

Sie werden abgemeldet und können sich nur noch mit Ihrem Windows AD-Konto anmelden.
Alle Menüoptionen unter **Sicherheit** *werden aktiviert. Beispielsweise können Sie jetzt die* Pass-through-Anmeldung *einschalten.*

Das Standard-Konto `Administrator` *steht nicht mehr zur Verfügung und die Option* ***Konsolen-Kennwort ändern...*** *wird deaktiviert.*

13.2. Administrator hinzufügen

Die vorhandenen AD-Benutzer und AD-Gruppen können Sie als Scout Enterprise-Administratoren definieren.

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Administratoren verwalten**.
2. Klicken Sie im Dialog **Administratorenrechte** auf die Schaltfläche **Administrator hinzufügen...**

   Der Dialog **Administrator-Profil** *öffnet.*
3. Bestimmen Sie den Zugriffsbereich für den neuen Administrator und bestätigen Sie mit **OK**.

   Der Windows-Dialog **Berechtigungen für Administratoren** *öffnet.*
4. Klicken Sie unterhalb des Feldes **Gruppen- oder Benutzernamen** auf die Schaltfläche **Hinzufügen...**

   Der Windows-Dialog **Benutzer oder Gruppen auswählen** *öffnet.*
5. Geben Sie den relevanten Namen des AD-Benutzers oder der AD-Gruppe ein und klicken Sie auf **Namen überprüfen**.
   Oder:
   Suchen Sie den AD-Benutzer oder die AD-Gruppe über die **Erweitert...**-Schaltfläche.

6. Bestätigen Sie mit **OK**.

Der neue Benutzer oder die neue Gruppe wird zur Administratoren-Liste hinzugefügt. Sie können ihm oder ihr nun die relevanten Rechte zuweisen. Für weitere Informationen siehe Administratorenrechte.

Der oder die neuen Administratoren können sich mit ihren Windows-Account-Daten anmelden.

Hinweis
Wenn sich ein Benutzer bei ausschließlicher Verwendung von AD-Gruppen in mehreren Gruppen befindet, findet keine Konsolidierung der Rechte statt, sondern es gelten die Rechte der ersten AD-Gruppe, in der der Benutzer ermittelt wird.
Wenn ein Benutzer mit seinem AD-Benutzer und zusätzlich über eine oder mehrere AD-Gruppen berechtigt wurde, findet keine Konsolidierung der Rechte statt, sondern es gelten die Rechte, die dem AD Benutzer zugeordnet sind.

13.3. Administrator löschen

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Administratoren verwalten**.
2. Markieren Sie einen Administrator .
3. Klicken Sie auf die Schaltfläche **Administrator löschen**.

Wählen Sie **Sicherheit > Administratoren verwalten**.

Der markierte Administrator wird ohne Rückfrage gelöscht.

13.4. Administratorenrechte

Für alle Scout Enterprise-Administratoren können Sie folgende Arten der Berechtigung setzen:

Basisrechte	Hauptzugriffsrechte
Menürechte	Zugriffsrechte auf einzelne Menüpunkte
Objektrechte	Zugriffsrechte für die OUs oder Geräte

In dem jeweiligen **Administratorenrechte**-Dialog werden für den markierten Administrator die vorhandenen Rechte mit grünem oder roten Symbol angezeigt:

Berechtigung vorhanden	
Berechtigung nicht vorhanden	

Durch Doppelklick oder Drücken der Leertaste ändern Sie die Berechtigung.

Wenn Sie auf die Schaltflächen **Voller Zugriff** oder **Kein Zugriff** klicken, werden ALLE angezeigten Rechte auf grün bzw. auf rot gesetzt..

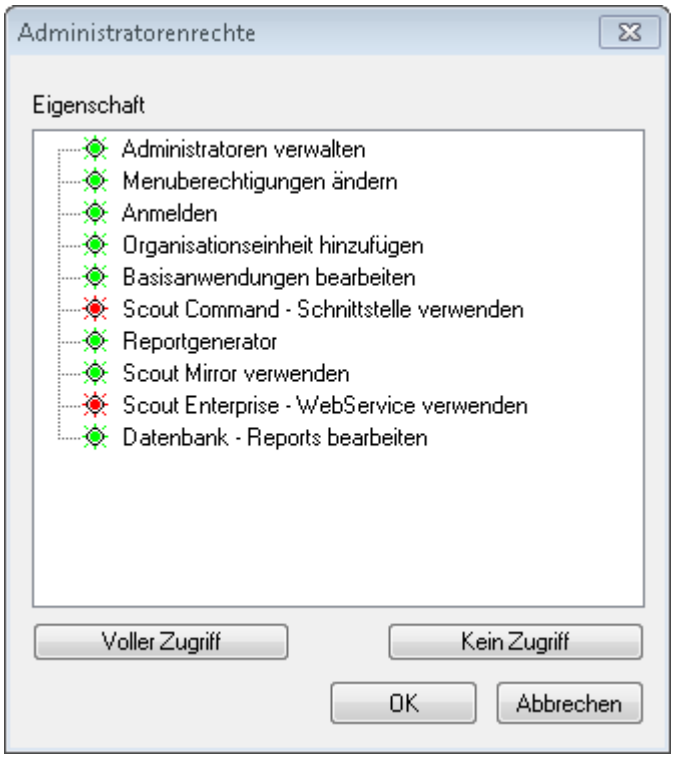
Achtung

Für alle Rechte gilt: Wird ein Recht deaktiviert, hat der Administrator keinen Zugriff mehr darauf. Für den letzten oder einzigen Administrator ist das Deaktivieren der Zugriffsberechtigung nicht möglich. Damit wird verhindert, dass Sie sich von der Konsole aussperren.

13.4.1. Basisrechte ändern

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Administratoren verwalten**.
2. Markieren Sie einen Administrator .
3. Klicken Sie auf die Schaltfläche **Basisrechte ändern**.

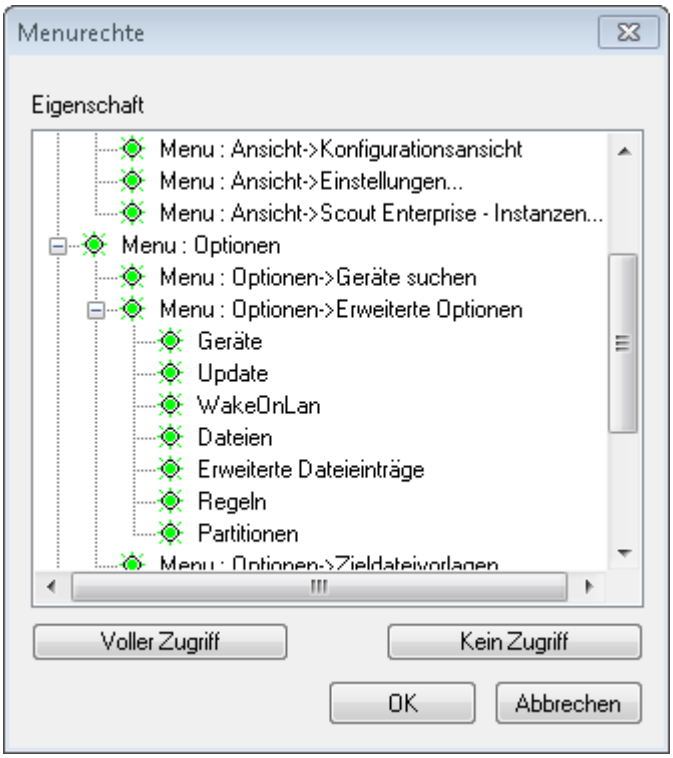
   *Der Dialog **Administratorenrechte > Basisrechte** öffnet.*
4. Ändern Sie die relevanten Berechtigungen durch Doppelklick.
5. Bestätigen Sie mit **OK**.



13.4.2. Menüberechtigungen ändern

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Menüberechtigungen...**.
2. Markieren Sie einen Administrator .
3. Klicken Sie auf die Schaltfläche **Menürechte...**.

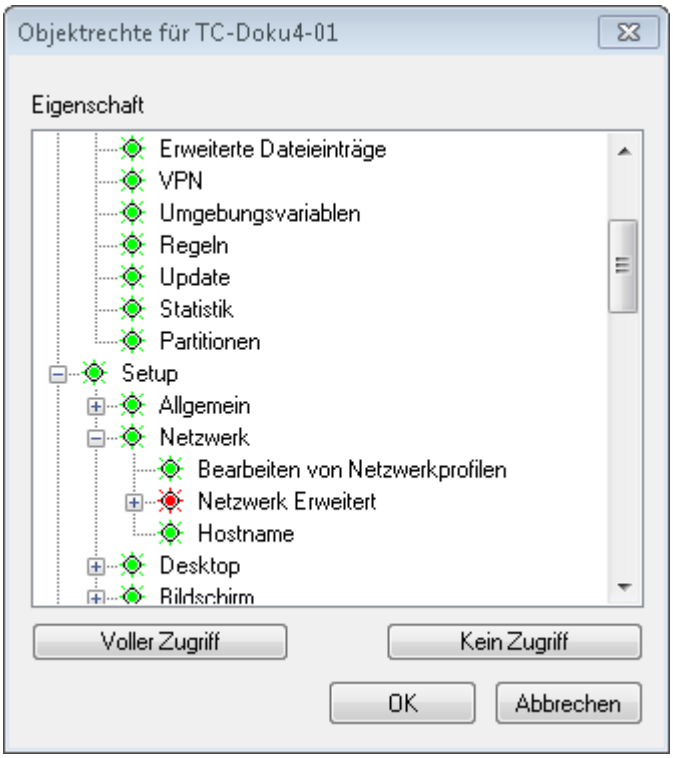
   *Der Dialog **Menürechte** öffnet.*
4. Ändern Sie die relevanten Berechtigungen durch Doppelklick.
5. Bestätigen Sie mit **OK**.



13.4.3. Objektberechtigungen ändern

1. Markieren Sie in der Scout Enterprise-Konsole eine OU oder ein Gerät.
2. Wählen Sie **Sicherheit > Objektberechtigungen...**.
   Oder:
   Wählen Sie den Kontextmenü-Eintrag **Objektberechtigungen...**
3. Markieren Sie einen Administrator.
4. Klicken Sie auf die Schaltfläche **Objektrechte...** .

   *Der Dialog **Menürechte für ...** öffnet.*
5. Ändern Sie die relevanten Berechtigungen durch Doppelklick.
6. Bestätigen Sie mit **OK**.



13.4.4. Standard-Objektrechtberechtigungen ändern

Standard-Objektrechte gelten für alle Objekte, für die keine speziellen Regeln definiert wurden.

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Administratoren verwalten**.
2. Markieren Sie einen Administrator .
3. Klicken Sie auf die Schaltfläche **Standard-Objektrechte...**.

   *Der Dialog **Standard-Objektrechte** öffnet.*
4. Ändern Sie die relevanten Berechtigungen durch Doppelklick.

5. Bestätigen Sie mit **OK**.

13.4.5. Start-OU festlegen

Mit dieser Funktion können Sie festlegen, dass ein Administrator nur die Start-OU und alle darin befindlichen OUs sehen darf.

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Administratoren verwalten**.
2. Markieren Sie einen Administrator .
3. Klicken Sie auf die Schaltfläche **Start-OU festlegen...**.

   *Der Dialog **Start Organisationseinheit** öffnet.*
4. Aktivieren Sie die Option **Folgende Start Organisationseinheit verwenden**.
5. Wählen Sie eine Start-OU aus.
6. Bestätigen Sie mit **OK**.

13.5. Passthrough-Authentifizierung

Die Passthrough-Authentifizierung aktiviert die Anmeldung über Single Sign-On. Ihre Windows Kontoinformationen werden genutzt, um Sie an der Scout Enterprise-Konsole automatisch anzumelden. Der Scout Enterprise Anmeldedialog erscheint nicht mehr.

14. Scout Enterprise-Statistikservice

Der Scout Enterprise-Statistikservice wird ab Scout Enterprise Management Suite Version 13.5.0 über die Scout Enterprise-Installation installiert und ermöglicht die Auswertung von konfigurierbaren Statusmeldungen (keep alive messages) der Clients. Im definierten Zeitintervall senden die konfigurierten Clients jeweils eine Statusmeldung an den Scout Enterprise-Statistikservice. Durch diese Statusmeldungen wird die Statusanzeige der Geräte in der Scout Enterprise-Konsole aktualisiert.

Hinweis

In Scout Enterprise Management Suite Version 14.4.0 ist der Scout Enterprise-Statistikservice nicht enthalten und die Setup-Routine deinstalliert einen eventuell vorhandenen Statistik-Dienst einer älteren Version.

Ab Scout Enterprise Management Suite Version 14.5.0 ist ein modifizierter Statistikservice (Wechsel von UDP-Protokoll auf HTTPS-Protokoll) mit erweiterter Funktionalität Bestandteil der Scout Enterprise Management Suite-Installation. Um den neuen Statistikservice zu nutzen, aktualisieren Sie die bisherige Installation auf Scout Enterprise Management Suite Version 14.5.0, rufen nach dem Update die Setup-Routine (setup.exe) von Scout Enterprise 14.5.0 noch einmal auf und führen über **Programm ändern** die Nachinstallation des Features **Scout Statistic service** durch.

Zur Nutzung der Statusmeldungen (keep alive messages) der Clients mit dem neuen Statistikservice benötigen die Clients mindestens eLux RP Version 4.9.0. Das UDP-Protokoll für keep alive messages darf an den Geräten über die Funktion **Erweiterte Dateieinträge** nicht aktiviert sein. Für weitere Informationen siehe Definieren von Statusmeldungen (keep alive messages).

Erweiterte Funktionalität des Statistikservice ab Scout Enterprise Management Suite Version 14.5.0

Neben konfigurierbaren Statusmeldungen der Clients (keep alive messages) verarbeitet der Statistik-Dienst zusätzlich dynamische Geräteinformationen zur statistischen Auswertung. Die Speicherung der Statistik-Daten erfolgt in einer separaten SQL-Datenbank. Ob und welche Statistik-Daten von den Geräten übermittelt werden, können Sie über die Scout Enterprise-Konsole konfigurieren. Die Auswertung und Anzeige der Statistik-Daten erfolgt über das Scout Enterprise-Dashboard.

14.1. Voraussetzungen

Kompatibilität

Folgende Server- und Client-Versionen sind kompatibel:

- Scout Enterprise Version 13.5.0 bis 14.3.0 / Clients mit eLux RP 4.4.0 bis 4.8.0 ⇒ keine Anpassung zur Nutzung der 'keep alive' messages erforderlich
- Scout Enterprise Version 13.5.0 bis 14.3.0 / Clients mit eLux RP 4.9.0 oder höher ⇒ **Legacy Mode** für 'keep alive' aktivieren*
- Scout Enterprise Version 14.4.0 ⇒ 'keep alive' messages wegen fehlendem Scout Enterprise-Statistikservice nicht nutzbar
- Scout Enterprise Version 14.5.0 oder höher / Clients mit eLux RP 4.4.0 bis 4.8.0 ⇒ Update auf eLux RP 4.9.0 oder höher für 'keep alive' erforderlich
- Scout Enterprise Version 14.5.0 oder höher / Clients mit eLux RP 4.9.0 oder höher ⇒ keine Anpassung erforderlich
  Die Übermittlung der 'keep alive' messages und der statistischen Geräteinformationen erfolgt von den Geräten an den Scout Enterprise-Statistikservice über das HTTPS-Protokoll.

*Die Aktivierung des **Legacy Mode** für 'keep alive' messages erfolgt über die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole:

Datei	`/setup/terminal.ini`
Abschnitt	`Statistics`
Eintrag	`KeepAliveLegacy`
Wert	`true`

Für weitere Informationen siehe Erweiterte Dateieinträge.

Hardware-Voraussetzungen

Bei einer Geräteanzahl unter 200.000 empfehlen wir mindestens

- 8 GB RAM
- 4 CPUs

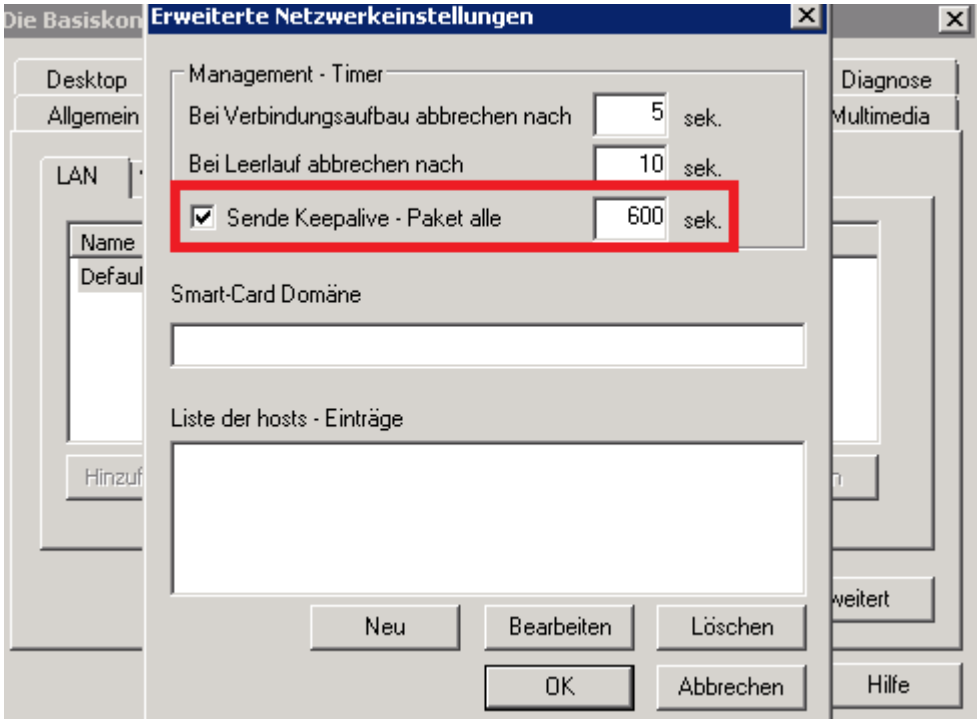
Für 200.000 bis 400.000 Geräte empfehlen wir mindestens

- 16 GB RAM
- 8 CPUs

14.2. Definieren der Statusmeldungen (keep alive messages)

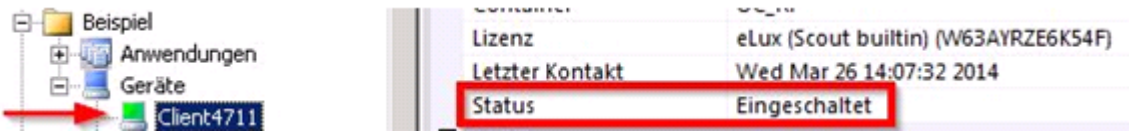
Mit Hilfe des Scout Enterprise-Statistikservice können Sie die automatische Aktualisierung der Statusmeldungen (keep alive messages) konfigurieren.

1. Wählen Sie im Scout Enterprise-Menü **Optionen > Basiskonfiguration > Netzwerk > Erweitert** oder öffnen Sie für das relevante Gerät oder OU den Dialog **Konfiguration > Netzwerk > Erweitert**.



2. Aktivieren Sie die Option **Sende Keepalive-Paket**.
3. Definieren Sie den Zeitintervall in Sekunden.
4. Bestätigen Sie mit **OK**.

Die konfigurierten Clients senden im definierten Zeitintervall eine Statusmeldung an den Scout Enterprise-Statistikservice. Dadurch wird die Statusanzeige dieser Clients in der Scout Enterprise-Konsole (Symbol und Eigenschaft) aktualisiert:



Wenn die Statusmeldung eines Clients im definierten Zeitintervall ausbleibt, wird die Statusanzeige in der Scout Enterprise-Konsole ebenfalls aktualisiert:

Hinweis
Bitte beachten Sie zur Nutzung der 'keep alive messages' die Abhängigkeiten der unterschiedlichen Scout Enterprise- und eLux RP-Versionen. Für weitere Informationen siehe Voraussetzungen Scout Enterprise Statistikservice.

14.3. Beispiele für Statusmeldungen

Die Farbe der Client-Symbole in der Baumansicht zeigt den aktuellen Status der Geräte an:

- 

Dieser Client ist ordnungsgemäß in Betrieb. Statusmeldungen werden erfolgreich an den Scout Enterprise Statistik Dienst übermittelt.
- 

Bei diesem Client liegt eine Unterbrechung der Netzwerkanbindung vor. Statusmeldungen können nicht mehr an den Scout Enterprise Statistik Dienst gesendet werden.
- 

Die Netzwerkverbindung für dieses Gerät ist wieder hergestellt. Statusmeldungen werden wieder erfolgreich an den Scout Enterprise Statistik Dienst übermittelt.

Für weitere Informationen über Client-Symbole siehe Oberfläche/Symbole.

14.4. Dynamische Geräteinformationen zur statistischen Auswertung

Wie die Geräteinformationen zur statistischen Auswertung übermittelt werden, können Sie mit Hilfe der Funktion **Erweiterte Dateieinträge** in der Scout Enterprise-Konsole konfigurieren:

Datei	`/setup/terminal.ini`
Abschnitt	`Statistics`
Eintrag	`Supervise`
Wert	`usb,pci`

Für weitere Informationen siehe Erweiterte Dateieinträge.

Wenn Sie als Wert `usb` und/oder `pci` angeben, werden die Geräteinformationen der entsprechenden Gerätegruppe von den Geräten an den Scout Enterprise-Statistikservice über HTTPS übermittelt und in der Statistik-Datenbank gespeichert. Voraussetzung für diese Funktion ist die Installation des Scout Enterprise-Statistikservice mit der Scout Enterprise Management Suite unter Angabe eines gültigen Zertifikates mit dem Zweck Serverauthentifizierung. Für weitere Informationen siehe Scout Enterprise Management Suite installieren.

Die Auswertung und Anzeige der Statistik-Daten erfolgt über das Scout Enterprise-Dashboard. Das Scout Enterprise-Dashboard wird mit der Scout Enterprise Management Suite unter Angabe der relevanten Datenbanken (Scout Enterprise, Statistik- und Dashboard-Datenbank) installiert.[1]

14.5. Zertifikat für Statistik-Service

Die Kommunikation zwischen eLux und dem Statistik-Service erfolgt über HTTPS. Daher wird bei der Installation des Statistik-Service ein SSL-Zertifikat zur Serverauthentifizierung standardmäßig an den Port 22124 gebunden.

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

Hinweis
Wenn der Rechner 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 folgenden Befehl ein:
   ```
   netsh.exe http show sslcert
   ```

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

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=192.168.10.1:22124
   ```

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

Neues SSL-Zertifikat an Port binden

1. Rufen Sie die Kommandozeile auf.
2. Verwenden Sie das `netsh.exe`-Tool, wie in folgendem Beispiel gezeigt:
   ```
   netsh.exe http add sslcert ipport=192.168.10.1:22124 certhash=0000000000003ed9cd0c315bbb6dc1c08da5e6 appid={957ba029-e2a1-4a13-b426-645a5e3802e2}
   ```

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

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

[1] Bis Scout Enterprise Management Suite Version 14.9 wird das Dashboard separat installiert.

Der `appid`-Parameter ist die ID des Statistik-Service und hat den im Beispiel angegebenen Wert.

Anzeigen der Thumbprints (Fingerabdrücke) von Zertifikaten

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.

15. Konsolenkommunikation

Sobald mehrere Scout Enterprise-Konsolen und/oder Scout Enterprise-Dashboards verwendet werden, sind die Funktionen zur Konsolenverwaltung und -kommunikation von Bedeutung. Das webbasierte Scout Enterprise-Dashboard wird wie eine Konsole behandelt und kann beispielsweise wie eine Konsole Nachrichten empfangen.

15.1. Konsole schließen

1. Wählen Sie **Datei > Konsolenverwaltung > Konsole schließen**.
2. Wählen Sie Aktualisieren, um die aktuelle Liste mit Konsolen anzuzeigen
3. Wählen Sie Suchen, um die Liste zu filtern.
4. Wenn der Benutzer eine Meldung bekommen soll, aktivieren Sie "Benutzer informieren für x Sekunden" und geben Sie die Zeitspanne ein.
5. Wenn der Benutzer die Möglichkeit bekommen soll, den Befehl abzubrechen, aktivieren Sie "Kommando kann vom Benutzer abgebrochen werden".
6. Wählen Sie **Konsole(n) schließen**.
   Das Kommando wird an die Konsolen übermittelt und wartet anschließend bis alle Konsolen geschlossen sind. Dies kann einige Minuten dauern. Der Dialog wartet bis zu 5 Minuten auf die Bestätigung aller Konsolen. Die Liste der aktiven Konsolen wird in dieser Zeit ständig aktualisiert.

15.2. Nachricht senden

Mit dieser Funktion können Sie Nachrichten an andere Konsoleninstanzen senden. Jede Konsoleninstanz zeigt eine Nachricht nur einmal. Wurde die Konsoleninstanzwährend des gesamten Gültigkeitszeitraums nicht gestartet, so wird die Nachricht nicht angezeigt. Startet ein Benutzer während des Gültigkeitszeitraums eine Konsoleninstanz, die noch nicht in der Datenbank enthalten war, wird die Nachricht nur angezeigt, wenn die Option **An alle Konsolen** aktiv war.

1. Wählen Sie unter **Empfänger** aus, welche Konsolen Ihre Nachricht erhalten sollen
2. Wählen Sie unter **Zeitraum** aus, wie lange die Nachricht angezeigt werden soll.
3. Geben Sie unter **Nachricht** den Text ein.
4. Die Option **Benutzer informieren...** schließt die Nachricht in der Empfängerkonsole automatisch nach Ablauf der angegebenen Zeit.
5. Die Option **Kommando kann vom Benutzer abgebrochen werden** ermöglicht es dem Benutzer der Empfängerkonsole, die Nachricht zu schließen, ohne ihren Empfang zu bestätigen. In diesem Fall wird sie bei einem Neustart der Konsole innerhalb des Gültigkeitszeitraumes erneut angezeigt. Wird die Anzeigezeit der Nachricht überschritten, ohne das der Benutzer einen Button auswählt, gilt die Nachricht als angenommen.
6. Wählen Sie **Senden**.
   Die Nachricht wird an die ausgewählten Konsolen gesendet.

15.3. Konsolen verwalten

Jede Konsole, die von einem Benutzer geöffnet wird, registriert sich in der Scout Enterprise-Datenbank. Die registrierten Konsolen können über den Menüpunkt **Konsolen verwalten** angezeigt werden.

- Wählen Sie **Datei > Konsolenverwaltung > Konsolen verwalten**.

Für jede Konsole wird der angemeldete Benutzer, der Computername, und die Anmeldedomäne angezeigt. Die aufrufende Konsole wird dabei ausgeblendet. Hat ein Benutzer mehrere Konsoleninstanzen auf demselben Computer geöffnet, werden die Konsolen durchnumeriert. Zum Beispiel ist "mfr #2" die zweite Konsoleninstanz des Benutzers ‚mfr'.

Es ist möglich, Konsoleninstanzen zu deaktivieren, indem das Häkchen in diesem Dialog entfernt wird. Die Konsoleninstanz wird dann in den anderen Dialogen zur Konsolenkommunikation nicht mehr angezeigt.

Alternativ können Sie eine Konsoleninstanz auch löschen. Allerdings werden dann auch alle Kommandos, die sich auf diese Konsoleninstanz beziehen, gelöscht. Damit verlieren Sie einen Teil der Kommando-Historie, und ggf. auch Kommandos, die noch nicht bearbeitet wurden. Diese Funktion dient dazu, alte, nicht mehr benutzte Konsolen aus dem Speicher zu entfernen. Auf aktuell geöffnete Konsolen hat diese Funktion keine Auswirkungen.

Sie können prüfen, ob alle Benutzer im Active Directory bekannt sind. Nicht bekannte Benutzer können selektiert (und ggf. anschließend gelöscht) oder deaktiviert werden.

Der Button **Suchen** blendet für jede Spalte der Liste ein Suchfeld ein. Die Platzhalter ‚*' und ‚?' im Suchtext sind zulässig, Groß-/Kleinschrift wird ignoriert. Der Button **X** schließt die Suchfeldanzeige wieder.

Alle Änderungen werden erst gültig, wenn mit Klick auf **OK** bestätigt wurde.

15.4. Kommandos verwalten

Der Dialog zum Verwalten von Kommandos ermöglicht das Löschen von Kommandos und das Verändern des Gültigkeitszeitraums.

Die Optionen **Alle**, **Aktive**, **Inaktive**, **Älter als XX Tage** und **Jünger als XX Tage** filtern die angezeigten Kommandos. Wird ein Kommando in der Liste selektiert, kann es über den Button **Löschen** gelöscht oder sein Gültigkeitszeitraum verändert werden. Der Button **Alle Löschen** löscht alle angezeigten Kommandos.

Der Button **Suchen** blendet für jede Spalte der Liste ein Suchfeld ein.

Die Liste Empfänger zeigt an, an welche Konsolen das Kommando gesendet wurde, und wann die Konsolen das Kommando bearbeitet haben. Ist als Benutzer, als Computer und als Domäne ***** (alle) angegeben, wurde das Kommando an alle Konsolen gesendet, und gilt daher auch für Konsoleninstanzen, die sich neu bei der Datenbank anmelden. Ein Eintrag dieser Form weist daher niemals einen Zeitpunkt in der Spalte Bearbeitet auf.

Alle Änderungen werden erst gültig, wenn der Button **OK** gedrückt wurde.

15.5. Reports für Dashboard verwalten

In der Datenbank gespeicherte Reports sind zentral verfügbar und können von allen berechtigten Scout Enterprise-Administratoren (Basisrecht **Reportgenerator**) im Scout Enterprise-Reportgenerator genutzt werden. Zusätzlich können in der Datenbank gespeicherte Reports im Scout Enterprise-Dashboard genutzt werden.

Die Verwendung von Reports in Dashboard kann mit Hilfe der Reportverwaltung der Scout Enterprise-Konsole eingeschränkt werden: Reports können AD-Benutzern oder oder AD-Gruppen zugeordnet werden und umgekehrt.

Voraussetzung

- Die Administratorenverwaltung ist eingeschaltet (**Sicherheit > Administratorenverwaltung aktivieren**).
- Sie besitzen die Menüberechtigung für **Datei > Konsolenverwaltung > Dashboard > Reports verwalten...**

Einem Report Administratoren zuordnen

1. Wählen Sie **Datei > Konsolenverwaltung > Dashboard > Reports verwalten...**
2. Stellen Sie sicher, dass die Reports in der linken Liste angezeigt werden. Wenn erforderlich, klicken Sie auf **Ansicht wechseln...**
3. Markieren Sie in der **Reports**-Liste einen Report und klicken Sie unterhalb der **Administratoren**-Liste auf **Hinzufügen...**

   Alle Scout Enterprise-Administratoren werden angezeigt.
4. Markieren Sie einen oder mehrere Administratoren oder Gruppen, und bestätigen Sie mit **OK**.

   Für den ausgewählten Report werden die berechtigten Administratoren angezeigt.
5. Aktivieren Sie die Option **Report-Zuordnung für Dashboard verwenden**.

Die berechtigten Administratoren können den ausgewählten Report im Scout Enterprise-Dashboard verwenden.

Einem Administrator/einer Administratorengruppe Reports zuordnen

1. Wählen Sie **Datei > Konsolenverwaltung > Dashboard > Reports verwalten...**
2. Stellen Sie sicher, dass die Administratoren in der linken Liste angezeigt werden. Wenn erforderlich, klicken Sie auf **Ansicht wechseln...**
3. Markieren Sie in der **Administratoren**-Liste einen Benutzer oder eine Gruppe und klicken Sie unterhalb der **Reports**-Liste auf **Hinzufügen...**

   Alle in der Scout Enterprise-Datenbank gespeicherten Reports werden angezeigt.
4. Markieren Sie einen oder mehrere Reports, und bestätigen Sie mit **OK**.

Für den ausgewählten Administrator/Gruppe werden die erlaubten Reports angezeigt.

5. Aktivieren Sie die Option **Report-Zuordnung für Dashboard verwenden**.

Der ausgewählte Administrator/Gruppe kann die zugewiesenen Reports im Scout Enterprise-Dashboard verwenden.

Achtung

Wenn die Option **Report-Zuordnung für Dashboard verwenden** nicht aktiv ist, sind alle in der Datenbank gespeicherten Reports für alle Administratoren verfügbar.

16. Import/Export

Alle Import- und Export-Funktionen können Sie entweder über die Scout Enterprise-Konsole oder über das SCMD-Interface durchführen. Informationen zum SCMD-Interface finden Sie in der SCMD-Dokumentation.

Beim Export werden Dateien im XML-Dateiformat angelegt. Je nach exportiertem / importierten Bereich ändert sich die Dateierweiterung.

Datenkategorie für den Export/Import	Dateierweiterung
Konfigurationen von OUs	.oustp
Basis-Konfiguration	.oustp
Konfigurationen von Geräten	.devstp
Eigenschaften / Erweiterte Einstellungen von OUs	.oupro
Basis/ Erweiterte Optionen	.oupro
Eigenschaften von Geräten	.devpro
Eigenschaften von Anwendungen	.appro
Geräteliste	.csv
OU-Baum	.outree

Diese Dateien können mit dem Konfigurationseditor bearbeitet werden. Für weitere Informationen siehe Scout Enterprise Konfigurationseditor.

16.1. Exportieren

1. Markieren Sie die OU, aus der Sie Daten exportieren möchten.
2. Wählen Sie **Datei > Export** und im Untermenü die Datenkategorie, die Sie exportieren möchten.
3. Wählen Sie den Speicherort.
4. Bestätigen Sie mit **OK**.

16.2. Importieren

Sie können Gerätekonfigurationen, Geräteeigenschaften und Anwendungseigenschaften importieren, aber auch Gerätelisten und OU-Bäume. Die zu importierende Datei muss die entsprechende Dateinamenserweiterung besitzen.

1. Markieren Sie die OU, in die Sie Daten importieren möchten.
2. Wählen Sie **Datei > Import** und im Untermenü die Datenkategorie, die Sie importieren möchten.
3. Bestätigen Sie mit **OK**.

17. Protokollierung und Optimierung

17.1. Protokollierung

Scout Enterprise bietet drei verschiedene Protokollierungs-Möglichkeiten, die als Log Dateien auf der Scout Enterprise Server-Maschine gespeichert werden.

Option	Protokolldatei	Beschreibung
Scout Enterprise-Konsole	`scout.log`	Dient der Fehlersuche Pfad: *%USERPROFILE%*`\Documents\UniCon\Scout\Console` In der Scout Enterprise-Konsole öffnen Sie die Datei über **Ansicht > Systemdiagnose > Konsolenprotokoll**.
Scout Enterprise-Server	`eluxd.log`	Protokolldatei für den Scout Enterprise Serverdienst, hilfreich bei Support-Anrufen Standard-Pfad: *%PUBLIC%*`\Documents\UniCon\Scout\Server` Ältere Versionen werden umbenannt in `elux.log.1...elux.log.3` etc. In der Scout Enterprise-Konsole öffnen Sie die Datei über **Ansicht > Systemdiagnose > Serverprotokoll** (nur wenn die Scout Enterprise-Konsole auf derselben Maschine installiert wurde wie der Scout Enterprise Server).
Server keep alive log	`keepAlive.log`	Protokolldatei für keep alive-Einträge des Scout Enterprise-Servers Einträge unter Einhaltung eines fest definierten Zeitstempels von 10 Minuten Standard-Pfad: *%PUBLIC%*`\Documents\UniCon\Scout\Server`

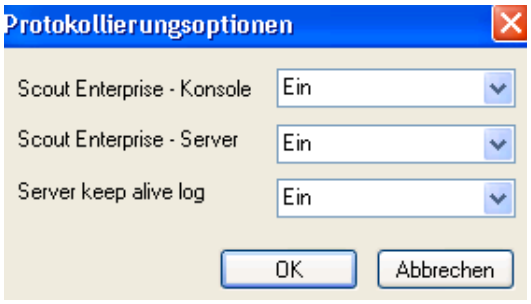
Für weitere Informationen zu den Dateipfaden siehe Pfade.

Hinweis

Verwenden Sie **Ansicht > Systemdiagnose > Server-Dateien**, um das `Unicon` Serverdateien-Verzeichnis im Windows-Explorer zu öffnen (wenn Konsole und Server auf der gleichen Maschine installiert sind). Das `Unicon`-Verzeichnis enthält alle Konfigurations- und Protokolldateien in entsprechenden Anwendungs-Unterverzeichnissen.

17.1.1. Protokollierung einschalten

1. Wählen Sie in der Scout Enterprise-Konsole **Optionen > Protokollierungsoptionen**.
2. Wählen Sie für die relevanten Optionen im Listenfeld `Ein`.



Die eingeschalteten Protokolldateien werden vom System erstellt, wie beschrieben.

17.1.2. Scout Enterprise-Server-Protokoll konfigurieren

Für die Protokolldatei des Serverdienstes `eluxd.log` werden mehrere Sicherungen angelegt. Sobald eine neue `eluxd.log` erstellt wird, wird die vorige Version in die Datei `eluxd.log.1` gesichert, die alte Version aus `eluxd.log.1` wird nach `eluxd.log.2` gesichert usw.

Ab Scout Enterprise Management Suite Version 14.5 werden die Protokolldateien nach einem Server-Neustart weitergeführt. Anstelle des Server-Neustarts führen folgende Indikatoren zum Anlegen einer neuen Protokolldatei:

- die Größe der Protokolldatei
- die maximale Anzahl der Protokolldateien

Größe und Anzahl der Sicherungen für Server-Protokoll anpassen

1. Öffnen Sie im Dateisystem unter *`%PUBLIC%`*`\Documents\UniCon\Scout\Server` die Datei `eluxd.ini` zur Bearbeitung.
2. Setzten Sie folgende Einträge:

Abschnitt	Eintrag	Default	Beschreibung
[ELUXD]	`MaxLogFileSizeMB`	`100`	Maximale Größe der Protokolldatei in MB
[ELUXD]	`MaxLogFiles`	`10`	Maximale Anzahl der Protokolldateien (`eluxd.log` plus Sicherungen)

Hinweis
Bis Scout Enterprise Version 14.4 wurden bis zu drei Sicherungen angelegt, Indikator war der Neustart des Serverdienstes.

Standardmäßig werden die Protokolldateien für den Serverdienst und für die keep alive-Einträge im Verzeichnis `%PUBLIC%\Documents\UniCon\Scout\Server` geschrieben. Ab Scout Enterprise Management Suite Version 14.8 können Sie für diese Protokolldateien ein beliebiges lokales Verzeichnis festlegen. Ein Netzwerk-Verzeichnis darf nicht angegeben werden.

Verzeichnis für Protokolldateien konfigurieren

Achtung

Geben Sie ein lokales Verzeichnis an, auf das der Scout Enterprise-Server zugreifen kann. Verwenden Sie nicht das UNC (Uniform Naming Convention)-Format.

1. Öffnen Sie im Dateisystem unter `%PUBLIC%\Documents\UniCon\Scout\Server` die Datei `eluxd.ini` zur Bearbeitung.
2. Setzten Sie folgenden Eintrag:

Abschnitt	Eintrag	Beispiel	Beschreibung
[ELUXD]	`LogFileLocation`	`c:\log`	Lokales Verzeichnis, in das die Protokolldateien `eluxd.log` und `keepAlive.log` geschrieben werden

Beim nächsten Starten des Scout Enterprise-Dienstes werden die Protokolldateien im angegebenen Verzeichnis geschrieben. Wenn der Scout Enterprise-Dienst nicht in das Verzeiichnis schreiben kann, erzeugt er einen Eintrag in der Windows Ereignisanzeige.

17.2. Optimierung

Folgende Möglichkeiten zur Optimierung der Performance stehen Ihnen bei hohem Netzaufkommen von Scout Enterprise-Seite her zur Verfügung:

- Konfiguration der Handshake-Optionen pro Gerät, OU oder organisationsweit
- ManagerLoadBalancing (konfigurierbare Lastverteilung) bei Verwendung einer SQL-Datenbank
- Konfiguration der Anzahl der ODBC-Verbindungen bei Verwendung einer SQL-Datenbank

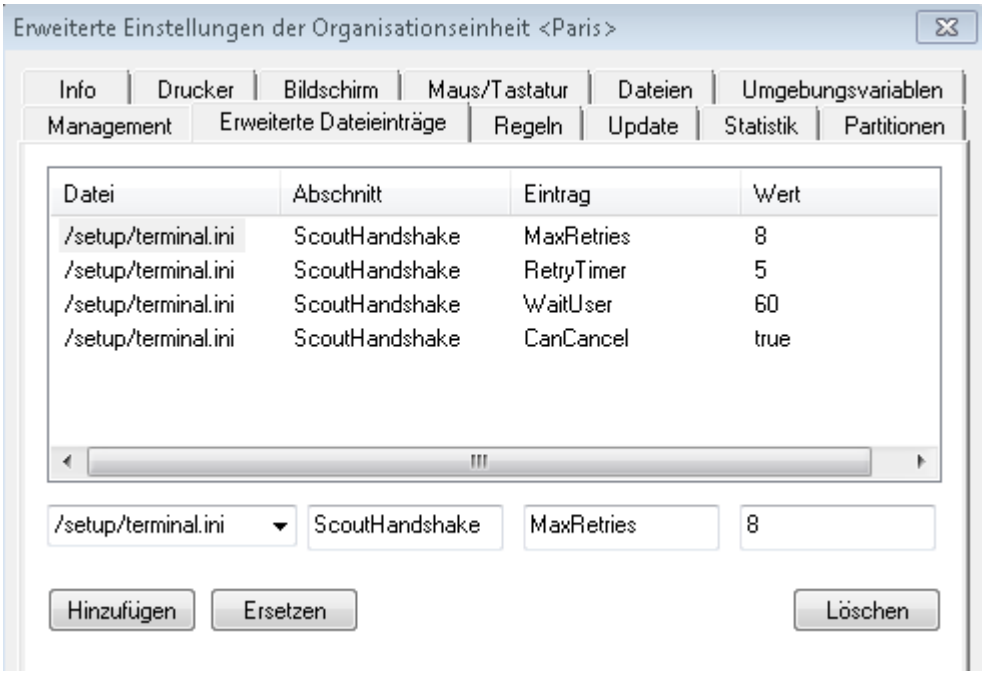
17.2.1. Optimierung durch Handshake

Bei jedem Neustart kontaktieren die Thin Clients den Scout Enterprise-Server und prüfen dabei, ob neue Konfigurationseinstellungen zur Verfügung stehen. Wenn der Scout Enterprise-Server nicht erreicht wird, wiederholt der Scout Agent für Windows der Thin Clients den Verbindungsversuch entsprechend seiner Handshake-Konfiguration, um die Gerätekonfiguration sowie die Anwendungsdefinitionen zu synchronisieren.

Der Anwender wird informiert, falls die Aktivierung der neuen Konfigurationseinstellungen einen Client-Neustart erfordert. Hierbei besteht für den Anwender die Möglichkeit, den Client-Neustart zu unterdrücken.

Die Handshake-Parameter werden mit Hilfe der Funktion **Erweiterte Dateieinträge** in die Datei `terminal.ini` am Client geschrieben. Für weitere Informationen siehe Erweiterte Dateieinträge.

Die Clients können organisations-, OU- oder geräteweise konfiguriert werden.



Die Werte in der Abbildung sind Beispielwerte und können entsprechend angepasst werden. Standardmäßig sind keine Handshake-Parameter konfiguriert.

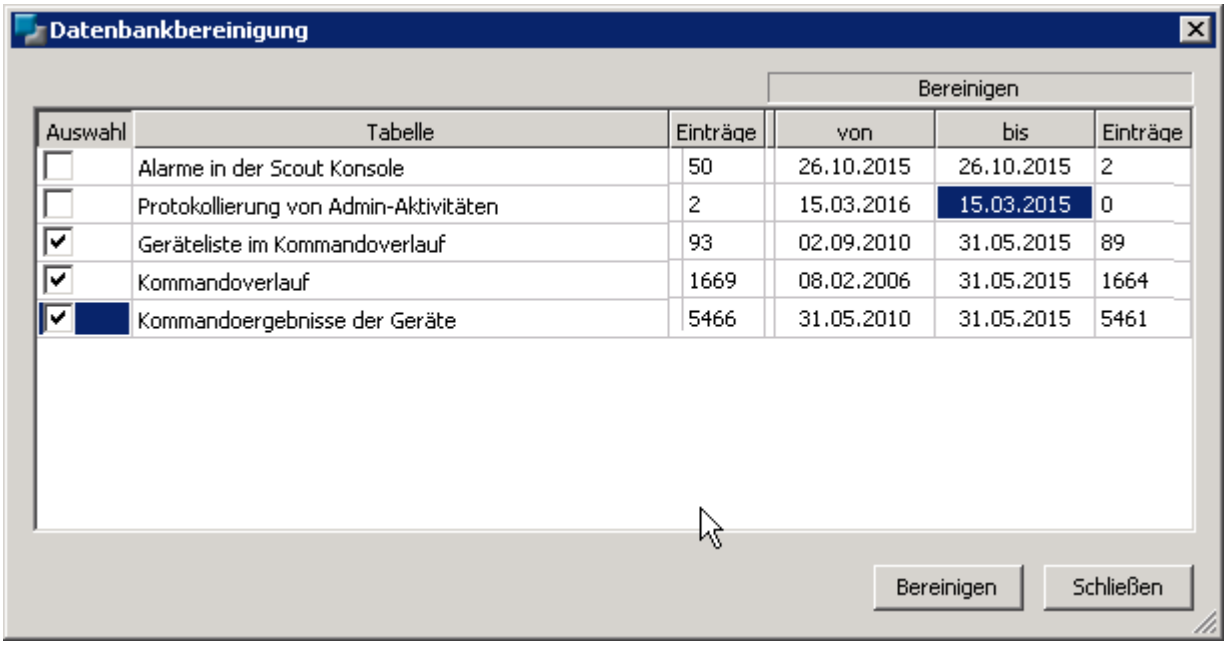
Der Abschnitt `ScoutHandshake` verfügt überfolgende konfigurierbare Parameter:

Parameter	Beschreibung
MaxRetries	Anzahl der Verbindungsversuche Der Wert `0` deaktiviert den Handshake.
RetryTimer	Zeit in Sekunden bis zum nächsten Verbindungsversuch Nach jedem Versuch wird die Zeit verdoppelt (+/- Zufallswert). Beispiel: Bei `8` Verbindungsversuchen mit **RetryTimer**-Startwert `5` Sekunden erfolgt der 8.Versuch nach ca. 22 Minuten.
WaitUser	Wartezeit vor dem Client-Neustart, damit der Benutzer Anwendungen schließen oder eine Abmeldung durchführen kann
CanCancel	Definiert, ob der Anwender den Client-Neustart unterdrücken kann (`true` | `false`).

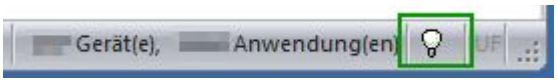
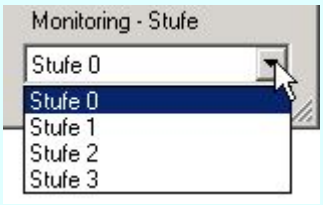
17.2.2. Datenbankbereinigung

Scout Enterprise speichert Daten über alle durchgeführten Update-, Auslieferungs und benutzerdefinierten Kommandos, sowie von weiteren Vorgängen. Um die entsprechenden Scout Enterprise-Datenbanktabellen von alten Daten zu bereinigen, kann ein berechtigter Administrator bestimmte Datenbankeinträge bis zu einem frei definierbaren Datum löschen[1].

Der Dialog **Datenbankbereinigung** listet fünf verschiedene Tabellen jeweils mit der Gesamt-Anzahl der Einträge und dem Erstelldatum des ersten Eintrages. Der Administrator kann nur die Felder **Auswahl** und **bis** bearbeiten.



[1] für LocalDB steht diese Funktion ab Scout Enterprise Management Suite Version 14.9 zur Verfügung

Alarme in der Scout Enterprise-Konsole	Alarmmeldungen (Fehler, Warnung, Info), die nach Doppelklick auf das Lampensymbol der Scout Enterprise-Konsole angezeigt werden 
Protokollierung von Admin-Aktivitäten	Protokolleinträge der durchgeführten Administratoren-Aktivitäten gemäß der über **Sicherheit > Administratorenverwaltung...** konfigurierten Monitoring-Stufe (Tabelle `Monitor` der Scout Enterprise-Datenbank) 
Geräteliste im Kommandoverlauf	Verlaufsdaten von Kommandos, die im Dialog **Ansicht > Kommandoverlauf** der Scout Enterprise-Konsole angezeigt werden (Einträge für einzelne Geräte)
Kommandoverlauf	Verlaufsdaten von Kommandos, die im Dialog **Ansicht > Kommandoverlauf** der Scout Enterprise-Konsole angezeigt werden (Einträge für OUs)
Kommandoergebnisse der Geräte	Ergebnisprotokollierung von Kommandos, die auf den Geräten ausgeführt wurden (Update, Auslieferung, Benutzerdefiniertes Kommando). Die Anzeige der Protokolle erfolgt in der Scout Enterprise-Konsole durch Doppelklick auf das entsprechende Statusfeld Eigenschaften-Fenster oder über das Kontextmenü eines Gerätes **Kommandos > Update/Auslieferung/Kommando Info**. Für weitere Informationen siehe Kommando-Ergebnisse pro Gerät.

Datenbankbereinigung durchführen

1. Wählen Sie **Ansicht > Systemdiagnose > Datenbankbereinigung...**
2. Setzen Sie für die relevante Tabelle im Feld **bis** das Datum, das die Zeitspanne der zu löschenden Einträge begrenzt (alle Einträge bis zu einschließlich diesem Datum werden gelöscht).

   *In der letzten Spalte **Einträge** wird die Anzahl der zu löschenden Einträge angezeigt.*
3. Klicken Sie in die erste Spalte `Auswahl`, um die für diese Tabelle festgelegten Einträge für die Bereinigung zu aktivieren.

   Ein Haken zeigt an, dass aus dieser Tabelle Einträge zum Löschen vorgesehen sind.
4. Klicken Sie auf **Bereinigen**.

   Eine Meldung zeigt die komplette Anzahl zu löschender Einträge über alle ausgewählten Tabellen an.
5. Bestätigen Sie mit **Ja**.

Aus den ausgewählten Tabellen werden alle Einträge bis zu dem jeweils angegebenen Enddatum gelöscht.

Hinweis

Beachten Sie, dass Sie vor dem Löschen von Kommandoverlauf-Einträgen die entsprechenden Einträge der Geräteliste löschen müssen.

18. Anhang

18.1. Zeitserver

Um eine genaue Uhrzeit im Netzwerk zur Verfügung zu haben, empfehlen wir den Einsatz eines Zeitservers. Der Abgleich mit dem Zeitserver kann online in eLux über die Schaltfläche **Zeitabgleich** erfolgen.

Der Zeitserver muss dem Network Time Protocol (RFC 1305) bzw. dem Simple Network Time Protocol, einer vereinfachten Form, entsprechen. Microsoft Windows Betriebssysteme ab Windows 2000 enthalten den Dienst **W32Time**, der in älteren Betriebssystemen über SNTP kommuniziert und ab Windows Server 2003 NTP verwendet. Der Zeit-Dienst wird automatisch gestartet.

Der Dienst wird auf Port 123 mit dem UDP-Protokoll ausgeführt.

Weitere Informationen zum Windows Zeit-Service finden Sie in der Microsoft-Dokumentation.

Weitere Informationen zu NTP finden Sie unter http://www.ntp.org.

18.2. IP-Ports

eLux

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
	ESP	VPN (Datenphase)	Deinstallieren des Pakets `VPN System`	eingehend
	ESP	VPN (Datenphase)	Deinstallieren des Pakets `VPN System`	ausgehend
123	UDP	Windows-Zeitserver (NTP)	Keinen Zeitserver konfigurieren (**Setup > Desktop**)	eingehend
123	UDP	Windows-Zeitserver (NTP)	Keinen Zeitserver konfigurieren (**Setup > Desktop**)	ausgehend
21	TCP	Update via FTP control port (dynamic data port)		ausgehend
22	TCP	SSH-Anwendungen		ausgehend
23	TCP	3270, 5250, 97801 Emulationen und Telnet-Sitzungen		ausgehend
53	TCP	DNS-Server (Windows)		ausgehend

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
53	UDP	DNS-Server		ausgehend
67	UDP	DHCP-Server	Konfigurieren einer lokalen IP-Adresse (**Setup > Netzwerk**)	ausgehend
68	UDP	DHCP Client (oder BootP Client)	Konfigurieren einer lokalen IP-Adresse (**Setup > Netzwerk**)	eingehend
69	UDP	TFTP-Server (wird nur während eines PXE-Recovery verwendet)		ausgehend
80	TCP	Firmware-Update via HTTP (und Proxy Port, falls genutzt)		ausgehend
111	UDP	Portmapper – Treiberzugang auf NFS-Servern Funktioniert mit NFSD-Laufwerkszugriff (Port 2049) und mountd (random)	Deinstallieren des FPM `Automount` im Paket `Network Drive Share`	ausgehend
111	TCP	Portmapper – RPC nur zur internen Verwendung Funktioniert mit lockd (random)	Deinstallieren des FPM `Automount` im Paket `Network Drive Share`	eingehend
139	TCP	SMB Laufwerkszuordnung (NetBIOS) und SMB Benutzerauthentifizierung (CIFS)	Deinstallieren des FPM `Automount` im Paket `Network Drive Share` sowie des Pakets `User authorisation modules`	ausgehend
139	UDP	SMB Laufwerkszuordnung (NetBIOS) und SMB Benutzerauthentifizierung (CIFS)	Deinstallieren des FPM `Automount` im Paket `Network Drive Share` sowie des Pakets `User authorisation modules`	ausgehend
161	UDP	SNMP	Deinstallieren des Pakets `SNMP Environment`	eingehend
161	UDP	SNMP	Deinstallieren des Pakets `SNMP Environment`	ausgehend
162	UDP	SNMPTRAP	Deinstallieren des Pakets `SNMP Environment`	ausgehend
177	UDP	XCMCP-Protokoll		ausgehend

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
389	TCP	LDAP Benutzerauthentifizierung und AD-Benutzerauthentifizierung mit Benutzervariablen		ausgehend
443	HTTPS	VPN (Verbindungsaufbau)	Deinstallieren des Pakets `VPN System`	eingehend
443	HTTPS	VPN (Verbindungsaufbau)	Deinstallieren des Pakets `VPN System`	ausgehend
443	HTTPS	Firmware-Update via HTTPS		ausgehend
514	TCP	Shell, X11-Anwendungen		ausgehend
515	TCP	Drucken über LPD	Deinstallieren des Pakets `Print Environment (CUPS)`	ausgehend
515	TCP	Drucken über LPD	Deinstallieren des Pakets `Print Environment (CUPS)`	eingehend
631	TCP	CUPS (IPP) Druck-Client	Deinstallieren des Pakets `Print Environment (CUPS)`	ausgehend
631	UDP	CUPS (IPP) Druck-Client	Deinstallieren des Pakets `Print Environment (CUPS)`	ausgehend
2049	UDP	NFSD Laufwerkszugriff NFS	Deinstallieren des FPM `NFS Support` im Paket `Network Drive Share`	ausgehend
5900	TCP	Spiegelung des eLux Desktop	Spiegelung deaktivieren (**Konfig > Sicherheit**) oder `Mirror eLux Desktop`-Paket deinstallieren	eingehend
5901	TCP	Spiegelung der ersten XDMCP Sitzung	Spiegelung deaktivieren (**Konfig > Sicherheit**) oder `Mirror eLux Desktop`-Paket deinstallieren	eingehend
5902	TCP	Spiegung einer zweiten XDMCP Sitzung	Spiegelung deaktivieren (**Konfig > Sicherheit**) oder `Mirror eLux Desktop`-Paket deinstallieren	eingehend

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
6000	TCP	Remote X11 Anwendungen	Option **Konfig > Sicherheit > Remote X11 Clients zulassen** deaktiveren	eingehend
6001	TCP	erste XDMCP Sitzung		eingehend
6002	TCP	zweite XDMCP Sitzung		eingehend
7100	TCP	Fontserver Zuordnung in eLux Systemsteuerung möglich (**Setup > Bildschirm > Erweitert**)		ausgehend
20000	UDP	Wake On LAN		eingehend
20000	UDP	Wake On LAN		ausgehend
22123	TCP	Scout Enterprise Manager (secure)		eingehend
22123	TCP	Scout Enterprise Manager (secure)		ausgehend
22124	UDP	Scout Enterprise Statistics		ausgehend
9100	TCP	Direktdruck auf parallelen Port Zuordnung in eLux Systemsteuerung (**Setup > Drucker**)	Option **Setup > Drucker > TCP Direktdruck** deaktivieren	eingehend
9101	TCP	Direktdruck auf USB Port Zuordnung in eLux Systemsteuerung (**Setup > Drucker**)	Option **Setup > Drucker > TCP Direktdruck** deaktivieren	eingehend

Scout Enterprise Server

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
1433	TCP	MS SQL Server		eingehend
1433	TCP	MS SQL Server		ausgehend
1434	UDP	MS SQL Server (Browserdienst)		eingehend
1434	UDP	MS SQL Server (Browserdienst)		ausgehend
22123	TCP	Scout Enterprise Manager (secure)		eingehend

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
22123	TCP	Scout Enterprise Manager (secure)		ausgehend
22124	UDP	Scout Enterprise Statistics		eingehend

Scout Enterprise Konsole

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 `Mirror eLux Desktop`-Paket deinstallieren	ausgehend
5901	TCP	Spiegelung der ersten XDMCP Sitzung	Spiegelung deaktivieren (**Konfig > Sicherheit**) oder `Mirror eLux Desktop`-Paket deinstallieren	ausgehend
5902	TCP	Spiegung einer zweiten XDMCP Sitzung	Spiegelung deaktivieren (**Konfig > Sicherheit**) oder `Mirror eLux Desktop`-Paket deinstallieren	ausgehend

Scout Enterprise-Dashboard

Das Scout Enterprise-Dashboard kann entweder mit HTTP oder HTTPS installiert werden. Für beide Protokolle kann auch ein anderer Port als der Standard-Port eingestellt werden.

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
80	HTTP	Dashboard-Service / Webserver		eingehend
443	HTTPS	Dashboard-Service / Webserver		eingehend
1433	TCP	MS SQL Server		ausgehend

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
1434	UDP	MS SQL Server (Browserdienst)		ausgehend
5901	TCP	Spiegelung des eLux Desktop	Spiegelung deaktivieren (**Konfig > Sicherheit**) oder `Mirror eLux Desktop`-Paket deinstallieren	ausgehend

18.3. SNMP

SNMP (Simple Network Management Protocol) ist ein Netzwerkprotokoll, das zur Abfrage von Statusinformationen und zur Definition von Konfigurationsparametern dient.

Als Grundlage zur Konfiguration von

- SNMPv2 auf eLux RP4 dient das Softwarepaket: `snmp-5.6.1.1-2`
- SNMPv3 auf eLux RP5 dient das Softwarepaket: `snmp-5.5.2.1-1`

1. Downloaden Sie über **www.myelux.com eLux Software Packages > eLux RP Container > Released Packages > Add-On > snmp-5.x.x.x-x**

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

2. Um die SNMP-Konfiguration durchzuführen, stehen Ihnen zwei Methoden zur Verfügung:

   A) Übertragung der Konfigurationsdatei `snmpd.conf` nach
   `/setup/snmpd.conf` für eLux RP4 bzw.
   `/setup/snmp/snmpd.conf` für eLux RP5
   mit der Scout Enterprise-Funktion Dateien

   Oder:

   B) Konfiguration per Erweiterte Dateieinträge in Scout Enterprise

   Beispiel:

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

Hinweis

Wenn die Datei: `/setup/snmpd.conf` bzw. `/setup/snmp/snmpd.conf` vorhanden ist, hat die Methode A Priorität.
Wenn die Datei nicht vorhanden ist , wertet der Client den Abschnitt `[snmpd]` in der Datei `terminal.ini` aus.
Nur für eLux RP4: Wenn auch der Abschnitt `[snmpd]` nicht vorhanden ist, so wird die read only community `public` eingerichtet. Diese kann über die lokale Shell (XTERM) wie folgt getestet werden:
`snmpget -v 2c -c public <ip-address> SNMPv2-MIB::sysName.`

3. Geben Sie im Abschnitt `[SNMPD]` weitere dieser sogenannten SNMPD Configuration Directives wie z.B. `syscontact` oder `syslocation` an, um die Konfiguration anzupassen. Diese Direktiven regeln:
   - wer Zugriff auf den SNMP Agent hat
   - welche Informationen der SNMP Agent ausgibt
   - die aktive Überwachung des lokalen Systems
   - die Erweiterungen der Funktionalität des SNMP Agents
4. Zu Debugging-Zwecken können Sie im Abschnitt `[SNMP]` weitere Befehle angeben, die sogenannten **SNMP configuration directives**. Beispielsweise können Sie über die Funktion **Erweiterte Dateieinträge** den Eintrag `doDebugging` auf den Wert `1` im Abschnitt `[SNMP]` der Datei `terminal.ini` setzen.

Für weitere Informationen zu SNMPD und SNMP Konfigurations-Befehlen siehe http://www.net-snmp.org.

18.4. SNMPD und SNMP Konfigurations-Befehle

Die nachstehende Liste bezieht sich auf das Softwarepaket **snmp-5.6.1.1-2** unter eLux.
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)

Verwendung	Befehl
escapeQuotes	(1|yes|true|0|no|false)
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