

Scout Enterprise Management Suite

Administrationshandbuch zur Verwaltung einer Client-Infrastruktur mit der Scout Enterprise-Konsole 15

Stand: 2020-08-13

0. Rechtliche Hinweise	5
1. Darstellung	6
2. Überblick	7
2.1. Funktionsumfang der Scout Enterprise Management Suite	7
2.2. Kommunikation zwischen Thin Client und Scout Enterprise-Server	9
2.3. Installation	10
2.4. Tastenkombinationen	11
3. Oberfläche der Scout Enterprise-Konsole	12
3.1. Organisationsstruktur	12
3.2. Symbole in der Strukturansicht	13
3.3. Fenster	14
3.4. Statusleiste	19
3.5. Einstellungen zur Ansicht	19
3.6. Sprache ändern	20
3.7. Nach Geräten, OUs oder Anwendungen suchen	21
3.8. Elemente verschieben und kopieren	23
3.9. OU auf höchste Ebene verschieben	25
4. Geräteverwaltung	26
4.1. Automatische Geräteerfassung	27
4.2. DHCP-Konfiguration	29

4.3. Geräte suchen (Discovery)	32
4.4. Reverse Discovery ausführen	34
4.5. Geräteprofil reservieren	35
4.6. Sichere Geräteverwaltung mit Scout Enterprise	36
4.7. OU-Filter	37
4.8. Dynamische Gerätegruppen	46
4.9. Geräteumzug zwischen Scout Enterprise-Servern	51
5. Geräte-Konfiguration	58
5.1. Konzept	58
5.2. Konfigurationsmethode	67
5.3. Auswertung von Konfigurationsinformationen	69
5.4. FollowMe-Desktop	70
5.5. Register Allgemein	74
5.6. Register Netzwerk	75
5.7. Register Desktop	90
5.8. Register Anzeige	100
5.9. Register Maus/Tastatur	108
5.10. Register Firmware	111
5.11. Register Sicherheit	125
5.12. Register Multimedia	140
5.13. Register Laufwerke	142
5.14. Register Drucker	145
5.15. Register Hardware	152
5.16. Register Diagnose	158
5.17. Register Energieverwaltung	158
5.18. Problembehandlung Geräte-Konfiguration	164
6. Erweiterte Geräte-Konfiguration und Erweiterte Optionen	168
6.1. Geräte	169
6.2. Update/Auslieferung	170
6.3. Management	170
6.4. Vordefinierte IDFs und Container	171
6.5. Vordefinierte Kommandos	173
6.6. Wake On LAN	173
6.7. VPN	175
6.8. Konfigurierte Dateiübertragung	178
6.9. Erweiterte Dateieinträge	180
6.10. Regeln	184
6.11. Umgebungsvariablen	185
6.12. TPM 2.0-Unterstützung	186
7. Anwendungsdefinition	188
7.1. Allgemeines	188
7.2. Verbindung zu einer Citrix-Farm	199

7.3. Zusätzliche Software für Citrix-Umgebungen	226
7.4. RDP	229
7.5. Virtual Desktop	235
7.6. Browser	238
7.7. Lokale und benutzerdefinierte Anwendungen	246
7.8. Emulation	250
7.9. SAP GUI	254
7.10. Anwendungen im Kiosk-Modus	254
7.11. Problembehandlung Anwendungsdefinition	263
8. Client-Fernverwaltung durch Kommandos	265
8.1. Verfügbare Kommandos	265
8.2. Kommando ausführen	268
8.3. Kommando einplanen	269
8.4. Kommando-Ergebnisse und Update-Informationen	270
8.5. Kommandoverlauf	272
8.6. Kommando Grundzustand	274
8.7. Vordefinierte Kommandos erstellen	275
8.8. Vorlagen für Standard-Kommandos definieren	277
8.9. eLux Command Scheduler	278
9. Fernwartung	282
9.1. Spiegelung	282
9.2. Gerätediagnose	285
10. Firmware-Update	290
10.1. Voraussetzungen	291
10.2. Update planen	292
10.3. Update über Kommando ausführen	293
10.4. Update über Vormerkung ausführen	295
10.5. Update automatisch bei Systemstart oder Ausschalten	296
10.6. Auswirkungen beim Update mit Verschieben-Option	297
10.7. Software getrennt ausliefern	298
10.8. Statischer Proxy-Client	300
10.9. Dynamischer Proxy-Client	302
10.10. Problembehandlung Firmware-Update	306
11. Kennwörter	307
11.1. Lokales Geräte-Kennwort	307
11.2. Scout Enterprise Konsolen-Kennwort	309
12. Administratorenverwaltung	310
12.1. Administratorenverwaltung aktivieren	310
12.2. Administrator hinzufügen	310
12.3. Administrator löschen	311
12.4. Administratorenrechte	312
12.5. Administrator-Aktivitäten anzeigen	317

12.6. Passthrough-Authentifizierung	318
12.7. Wartungsfenster	318
13. Scout Enterprise-Statistikservice	320
13.1. Definieren der Statusmeldungen (keep alive messages)	321
13.2. Beispiele für Statusmeldungen	322
13.3. Dynamische Geräteinformationen zur statistischen Auswertung	322
14. Konsolenkommunikation	323
14.1. Konsole schließen	323
14.2. Nachricht senden	323
14.3. Konsolen verwalten	324
14.4. Kommandos verwalten	324
14.5. Reports für Dashboard verwalten	325
15. Import/Export	327
15.1. Exportieren	327
15.2. Importieren	327
16. Protokollierung und Optimierung	328
16.1. Protokollierung	328
16.2. Optimierung	332
17. Anhang	336
18.1. Programm- und Datei-Verzeichnisse	337
18.2. eLux-Partitionen	338
18.3. IP-Ports	339
18.4. SNMP	344

0. Rechtliche Hinweise

© 2020 Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH

Die vorliegende Dokumentation ist urheberrechtlich geschützt. Alle Rechte sind vorbehalten. Kein Teil dieser Dokumentation darf ohne unsere Genehmigung in irgendeiner Form vervielfältigt werden. Technische Änderungen vorbehalten. Texte und Abbildungen wurden mit größter Sorgfalt erarbeitet. Gleichwohl übernehmen wir weder juristische Verantwortung noch Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Informationen.

eLux® und Scout Enterprise Management Suite® sind eingetragene Marken der Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH in der Europäischen Union und in den USA.

ScoutaaS® ist eine eingetragene Marke der Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH in der Europäischen Union.

ScoutaaS™ ist eine eingetragene Marke der Unicon Software Entwicklungs- und Vertriebsgesellschaft mbH in Japan und in den USA.

Alle anderen Produktnamen sind eingetragene Warenzeichen der jeweiligen Eigentümer.

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

1. Darstellung

Die folgenden Textdarstellungen und Konventionen werden in diesem Handbuch verwendet:

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

Abkürzungen

Abkürzung	Bedeutung
AD	Active Directory, Verzeichnisdienst von Microsoft Windows Server
EBKGUI	Oberfläche des eLux Builder Kit (Komponente der Scout Enterprise-Software)
EPM	eLux package module (<code>.epm</code> , Software-Paket)
FPM	Feature package module (<code>.fpm</code> , Teil eines Software-Paketes)
FQDN	Fully qualified domain name
GB	Gigabyte
GHz	GigaHertz (Prozessorgeschwindigkeit)
HDD	Hard disk drive (Flash-Speicher)
IDF	Image Definition File (<code>.idf</code>)
IIS	Microsoft Internet Information Services
MB	Megabyte
OU	Organizational unit Organisationseinheit oder Gruppe innerhalb der Organisationsstruktur
VPN	Virtual Private Network

2. Überblick

2.1. Funktionsumfang der 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 meisten Komponenten sind Bestandteil der Standard-Installation, 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 "klassischen" Dialogprogramm eLux Image Administration Service (ELIAS) können individuelle Imagedefinitionsdateien (.idf) zum modularen Update der Firmware von eLux-Clients erstellt werden. Der klassische ELIAS wird von ELIAS 18 abgelöst.	Scout Enterprise.exe ¹
Scout Enterprise ELIAS 18	Neue Web-basierte und Plattform-unabhängige ELIAS-Anwendung zur Erstellung individueller Imagedefinitionsdateien (.idf)	gesondert (EliasInstaller.exe)

¹ab Scout Enterprise Management Suite Version 15.7 ist der klassische ELIAS nicht in der Standard-Installation enthalten. Um die Komponente zu installieren, wählen Sie **Benutzerdefiniert**.

Komponente	Beschreibung	Installation
Scout Enterprise-Report-generator	Tool zum Erstellen von frei definierbaren Reports über die aktuell in der Scout Enterprise-Datenbank enthaltenen Geräte, Anwendungen und OUs	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 ³	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

Die Funktionalität wird in folgenden Handbüchern beschrieben:

¹bis Scout Enterprise Management Suite Version 14.9 separate Installation erforderlich

²ab Scout Enterprise Management Suite Version 15.0

³nur bis Scout Enterprise Management Suite Version 15.3

- Scout Enterprise Management Suite:
Konfiguration, Steuerung und Verwaltung der Clients durch die Scout Enterprise-Konsole
Scout Enterprise-Statistikservice
Spiegeln mit der Scout Enterprise Mirror App
- Scout Enterprise ELIAS (der "klassische" ELIAS)
- Scout Enterprise ELIAS 18
- Scout Enterprise-Reportgenerator
- Scout Enterprise Command Interface
- 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 die Software-Pakete enthält.

Für weitere Informationen siehe [eLux-Container installieren](#).

2.2. Kommunikation zwischen Thin Client und Scout Enterprise-Server



Hinweis

Das zertifikatsbasierte Management-Protokoll gewährleistet eine sichere Kommunikation zwischen Scout Enterprise-Server und Clients.¹ Für weitere Informationen siehe [Zertifikatsbasiertes Management-Protokoll](#) in der Kurzanleitung **Installation**.

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: Geräte-Konfiguration, 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

¹ab Scout Enterprise Management Suite Version 15.1 und eLux RP 6.1

Konfiguration zu synchronisieren. Für weitere Informationen siehe [Optimierung durch Hands-hake](#).

Die Aktualisierung kann sich auf die Geräte-Konfiguration, 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 (ausgenommen sind VPN-Verbindungen).

2.3. Installation

Alle Themen, die mit der Installation zusammenhängen, werden in der Kurzanleitung **Installation** behandelt. Für weitere Informationen siehe [Installation der Scout Enterprise Management Suite](#).

2.4. 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

3. Oberfläche der Scout Enterprise-Konsole

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.

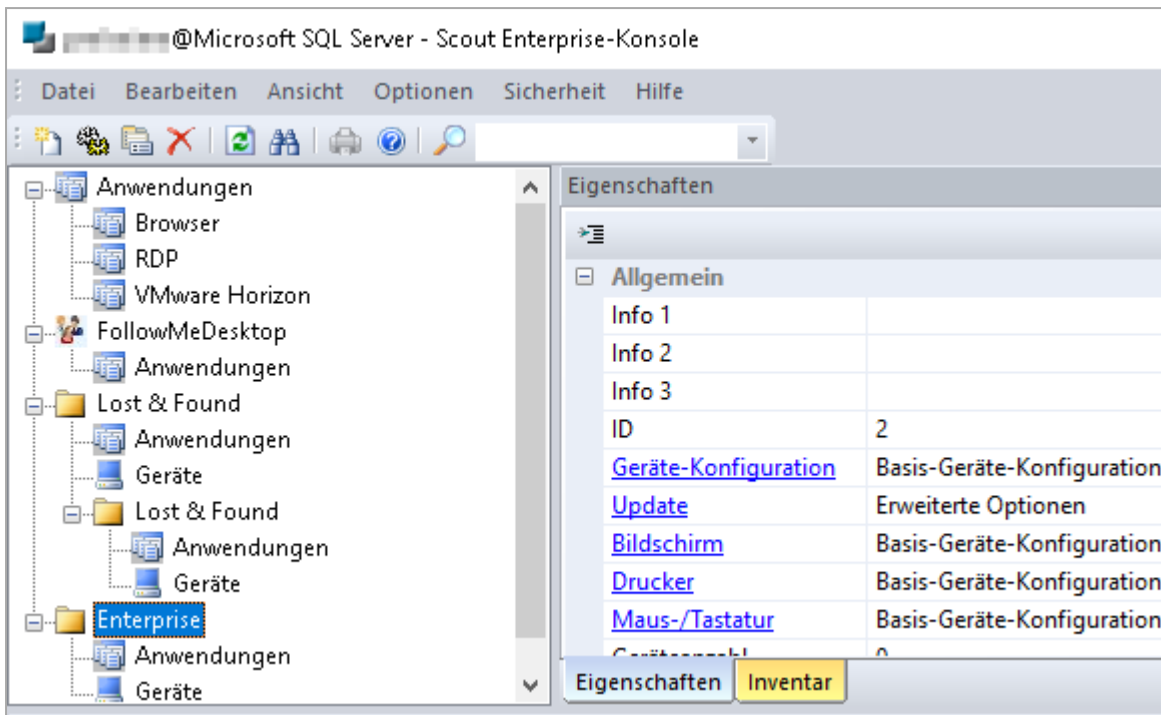
Wenn einer OU ein neues Gerät hinzugefügt wird, erhält es automatisch die Anwendungsdefinitionen und Konfiguration dieser OU.

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](#).

¹ab Scout Enterprise Management Suite Version 15.0



²ab 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 Geräte-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 in der Strukturansicht


Symbol	Beschreibung
	Organisationseinheit (OU)
	Anwendungen

Symbol	Beschreibung
	Gerät, 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. der Anmelde-Dialog ist geöffnet
	Gerät, Firmware-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 anzeigen oder ausblenden. Folgende Fenster stehen zur Verfügung:


Fenster	Beschreibung
Eigenschaften	Eigenschaften für markierte Anwendung, OU oder Gerät Für weitere Informationen siehe Eigenschaften .
Assets/Inventar (nur für Geräte)	Informationen zur Hardware des markierten Gerätes Wird als Register im Eigenschaften-Fenster angezeigt Für weitere Informationen siehe Hardware-Informationen .
Dynamische Gerätegruppen	Zeigt alle definierten Dynamischen Gerätegruppen (Listenansicht) Für weitere Informationen siehe Dynamische Gerätegruppen
Unabhängige Konfigurationen	OUs und Geräte, die nicht die übergeordnete Instanz für die Geräte-Konfiguration verwenden (Listenansicht) Für weitere Informationen siehe Vererbung unterbrechen – unabhängige Konfiguration
Konfigurationsvergleich	Zeigt Unterschiede in den Geräte-Konfigurationen von Geräten oder OUs an (Listenansicht)
OU-Geräte/Anwendungen	Zeigt Geräte oder Anwendungen einer OU ohne Symbole an (Listenansicht) Wenn Sie auf ein Gerät doppelklicken, wird das zugehörige Gerät in der Baumstruktur markiert. Diese Funktion kann deaktiviert werden, siehe unten.

Fenster	Beschreibung
Alle Geräte	<p>Zeigt alle Geräte ohne Symbole an (Listenansicht)</p> <p>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.</p> <p>Das Kontextmenü bietet die gleichen Funktionen wie in der Baumstruktur. Viele Funktionen wie Kommandos können Sie auf mehrere Geräte in der Liste anwenden. Dazu markieren Sie die Geräte mit STRG oder UMSCHALT.</p> <p>Wenn Sie auf ein Gerät doppelklicken, wird das zugehörige Gerät in der Baumstruktur angezeigt. Diese Funktion kann deaktiviert werden, siehe unten.</p> <p>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.</p>

Spalten sortieren

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

Eigenschaften ein-/ausblenden

- Klicken Sie auf die Schaltfläche , um Eigenschaften/Felder anzuzeigen oder auszublenden. Alternativ verwenden Sie das Kontextmenü.

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:

- Setzen 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

3.3.1. Eigenschaften


Für die markierte Anwendung, OU oder das markierte Gerät werden die Eigenschaften angezeigt.

Viele Eigenschaften werden in der Geräte-Konfiguration (Geräte und OUs) oder in der Anwendungsdefinition (Anwendungen) gepflegt und werden mit jeder Konfigurationsaktualisierung auf den aktuellen Stand gebracht. Für weitere Informationen siehe [Konfigurationsmethode](#).

Einige Eigenschaften kommen vom Scout Enterprise-Server und werden dynamisch aktualisiert.
Datum/Uhrzeit-Felder werden im internationalen Format nach ISO 8601 angezeigt.¹



Hinweis

Standardmäßig werden nicht alle Felder angezeigt. Um Felder anzuzeigen oder auszublenzen, klicken Sie auf die Schaltfläche .

Geräteeigenschaften

Beispiele:

Option	Beschreibung
Name	Hostname des Clients
Geräte-Konfiguration	Herkunft der Geräte-Konfiguration, meistens durch Vererbung aus höherer Instanz
Manager	IP-Adresse des Scout Enterprise-Servers, dem der Client zugeordnet ist
Info1-3	Die Info -Felder werden am Client im Configuration panel unter Information (eLux RP 6) ² angezeigt und können für die Benutzer zum Bearbeiten freigeschaltet werden (Benutzerrechte). Sie können bereits im First Configuration Wizard ausgefüllt werden.
OS-Version	Betriebssystem-Version des Clients
Container	eLux-Container, der dem Client in der Firmware-Konfiguration (Geräte-Konfiguration) zugeordnet wurde
Update-Zeitpunkt	Zeitpunkt des letzten Firmware-Updates Für weitere Informationen siehe Kommando-Ergebnisse und Update-Informationen
Letzter Kontakt	Zeitpunkt des letzten Kontakts zwischen Server und Client Die Aktualisierung findet nicht nur beim Client-Neustart statt, ³ sondern bei jedem erfolgreichen Verbindungsaufbau vom Server zum Client
Status	Beispiel: <code>Eingeschaltet</code> Der Status eines Gerätes wird durch den 'keep alive'-Mechanismus aktualisiert und durch aktive Statusmeldungen des Clients beim Hochfahren, Abmelden, Ausschalten, Einspielen von Updates und mehr.
Status-Zeitpunkt	Zeitpunkt der letzten Status-Aktualisierung

¹ab Scout Enterprise Management Suite Version 15.0

²am eLux RP 5-Client im Systray unter Geräteinformation

³ab Scout Enterprise Management Suite Version 15.0

Option	Beschreibung
Primäre MAC-Adresse	Geräteadresse der Hardware (MAC=Media Access Control)
Partitionen	System-, Setup- und Update-Partition werden mit ihrer jeweiligen Größe angezeigt.

Eigenschaften einer OU

Beispiele:

Option	Beschreibung
OU	<p>Zeigt die ID dieser OU</p> <p>Zusätzlich zum Dezimalwert der ID können Sie den Hexadezimalwert einblenden. Dazu setzen Sie in der Registry folgenden Eintrag:</p> <p>Schlüssel: HKEY_CURRENT_USER\Software\UniCon\Scout\Settings Wertname: DisplayHexOUID Werttyp: DWORD : 32 Wert: 1</p>
Geräteanzahl	Anzahl aller Geräte in und unterhalb der OU

Schnelle Links im Eigenschaften-Fenster für Geräte und OUs

- Doppelklicken Sie auf die blau dargestellten Links, um schnell und zuverlässig zu den jeweils relevanten Dialogen für Konfiguration und Information zu gelangen. Beispiele:

Markiertes Element	Option	Beschreibung
Gerät	Geräte-Konfiguration	Öffnet die relevante Geräte-Konfiguration
Gerät	Image	Öffnet ELIAS mit der für das Gerät konfigurierten IDF-Datei im relevanten Container
Gerät	Update-Status	Doppelklick oder ... öffnet die Update-Info für das Gerät mit Informationen über die durchgeführten Updates. Für weitere Informationen siehe Update-Protokoll .
OU	Geräte-Konfiguration	Öffnet die relevante Geräte-Konfiguration
OU	Update	Öffnet die relevanten Update-Einstellungen in der Erweiterten Geräte-Konfiguration oder den Erweiterten Optionen .
OU	Bildschirm, Drucker, Maus/Tastatur	Öffnet die relevante Konfiguration (Geräte-Konfiguration oder Erweiterte Geräte-Konfiguration) für Bildschirm, Drucker bzw. Maus/Tastatur.


3.3.2. Hardware-Informationen

Für das markierte Gerät werden im **Eigenschaften**-Fenster im Register **Inventar** gerätespezifische Hardware-Informationen angezeigt:

- Hardware-Informationen zum Gerät
- Hardware-Informationen zu angeschlossenen Geräten wie USB-Geräten und Bildschirmen



Hinweis

Standardmäßig werden nicht alle Felder angezeigt. Um Felder anzuzeigen oder auszublenzen, klicken Sie auf die Schaltfläche .

Hardware-Informationen zum Gerät

Beispiele:

Option	Beschreibung
Geräte-Typ	Produktbeschreibung seitens des Hardwarelieferanten (Zeichenkette).
Hauptspeicher	Größe des Arbeitsspeichers (RAM)
Flash-Speicher	Flash-Speichergröße und -typ
Flash-Größe	Größe des Flash-Speichers

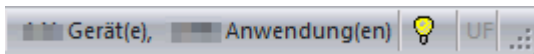
Hardware-Informationen zu angeschlossenen Geräten

Beispiele für ein USB-Gerät:

Option	Beschreibung
Produkt	Art des USB-Grätes
Hersteller	Name des Herstellers
Seriennummer	Seriennummer des USB-Gerätes
Revisionsnummer ¹	Firmware-Stand des USB-Gerätes

¹ab Scout Enterprise 15.8

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. Einstellungen zur Ansicht

Einige Voreinstellungen in Bezug auf die Ansicht können Sie über das Menü **Ansicht > Einstellungen** festlegen:

Option	Beschreibung
Aktualisierung der Geräte-Anzeige	
In der Baumansicht	Zeitspanne in Sekunden für die periodische Aktualisierung der Anzeige von Geräten, OUs und Anwendungen in der Baumansicht (Baumstruktur)
In der Listenansicht	Zeitspanne in Sekunden für die periodische Aktualisierung der Anzeige von Geräten, OUs und Anwendungen in der Listenansicht
Neue Geräte automatisch in Baumansicht anzeigen ¹	Neue Geräte werden nach dem Onboarden automatisch in die Baumstruktur eingefügt. (standardmäßig nicht aktiv)
Statusleiste / Aktualisierung der Gesamtzahlen	Zeitspanne in Sekunden für die periodische Aktualisierung der Anzahl aller in der gesamten Infrastruktur vorhandenen Geräte und Anwendungen
Bei Start der Konsole / Zuletzt markiertes Element anzeigen	Setzt nach dem Neustart der Konsole die Markierung auf das zuletzt markierte Element in der Baumansicht
Bestätigungsmeldungen anzeigen / Vor Aktualisierung der Ansicht	Nachdem Sie F5 gedrückt oder Ansicht > Aktualisieren gewählt haben, fragt das System nach, bevor die Anzeige aktualisiert wird.

¹ab Scout Enterprise 15.8

Option	Beschreibung
Prüfung von unabhängigen Konfigurationen	<p>Nach dem Ändern einer Geräte-Konfiguration werden alle untergeordneten unabhängigen Konfigurationen geprüft. Sie erhalten dann eine Übersicht über die jeweiligen Parameter und können komfortabel festlegen, ob und auf welche Instanzen die Änderungen übertragen werden sollen.</p> <p>Für weitere Informationen siehe Vererbung unterbrechen – unabhängige Konfiguration.</p>
Hinweis-Stufe	Bei Hinweis-Stufe 1 wird vor dem Ausführen von Kommandos eine Bestätigungs-Meldung angezeigt, die die Anzahl der betroffenen Geräte angibt.

3.6. Sprache ändern

Die Konsole wird mit der Spracheinstellung gestartet, die Sie für die Installation der Scout Enterprise Management Suite gewählt haben. Die Spracheinstellung bezieht sich auf die Anzeige der Oberflächen-Elemente und kann jeder Zeit geändert werden:

1. Wählen Sie **Anzeige > Sprache wählen** und wählen Sie die gewünschte Sprache aus.
2. Starten Sie die Scout Enterprise-Konsole neu.

Die Konsole wird mit der gewählten Sprache gestartet.



Achtung

Individuelle Fenster-Layouts werden nach Ändern der Spracheinstellung nicht wiederhergestellt.

3.7. Nach Geräten, OUs oder Anwendungen suchen

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.



Hinweis

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

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.



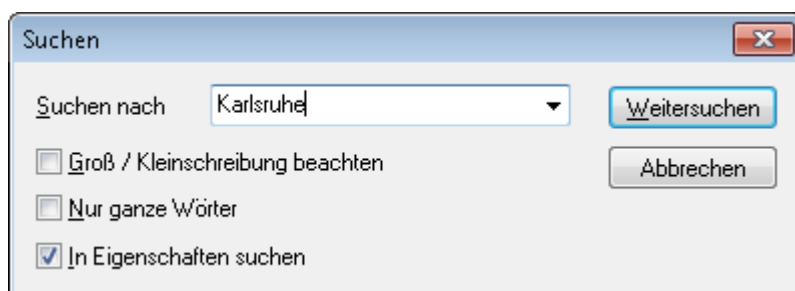
Hinweis

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.

Erweiterte Suche

Das Fenster **Erweiterte Suche**¹ bietet die Gerätesuche mit beliebig vielen Filterkriterien und mit Wildcards. Auf die Suchergebnisse können Kommandos und Vormerkungen angewendet werden.

1. Zeigen Sie das Fenster für die Erweiterte Suche an. Verwenden Sie dazu die Menüfunktion **Ansicht > Fenster > Erweiterte Suche**.

Einige Felder werden als Spalten und mit einem Suchfeld angezeigt.

2. Um Felder als Spalten anzuzeigen oder auszublenden, klicken Sie auf die Schaltfläche

*Das Fenster **Anpassen** mit allen verfügbaren Feldern öffnet und Sie können konfigurieren, welche Felder als Spalten angezeigt werden.*

Felder, nach denen nicht gesucht werden kann, werden im Suchfeld mit N/A angezeigt.

¹ab Scout Enterprise Management Suite 15.2

3. Um die Reihenfolge der Spalten zu verändern, verwenden Sie ebenfalls das Fenster **Anpassen**.
Die Reihenfolge ist relevant, wenn Sie mehrere Filterkriterien setzen möchten.
4. Geben Sie in der gewünschten Spalte im Suchfeld eine Zeichenfolge als Suchbegriff ein. Der Suchbegriff kann mit dem Wildcard-Zeichen % am Anfang oder Ende des Suchbegriffs abgekürzt werden.
5. Um die Suche zu starten, klicken Sie auf das Filter-Symbol.
6. Um die Suche einzuschränken, verwenden Sie weitere Filterkriterien in erlaubten Spalten.


Auf die gefilterten Geräte können Sie per Kontextmenü Kommandos, Vorkmerkungen und weitere Funktionen anwenden.

3.8. 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**.

Nach einer Bestätigungsabfrage wird das Element in die Ziel-OU verschoben.

Gerät per Kontextmenü in eine andere OU verschieben

1. Öffnen Sie in der Baumstruktur, im Fenster **OU-Geräte** oder im Fenster **Alle Geräte** für das relevante Gerät das Kontextmenü.
2. Wählen Sie die Option **Bearbeiten > Verschieben...**
3. Erweitern Sie im Dialog die Organisationsstruktur und markieren Sie die Ziel-OU.
4. Bestätigen Sie mit **OK**.

Nach einer Bestätigungsabfrage wird das Element 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 die 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](#).

3.9. 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-Geräte-Konfiguration gültig.

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 Geräte-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

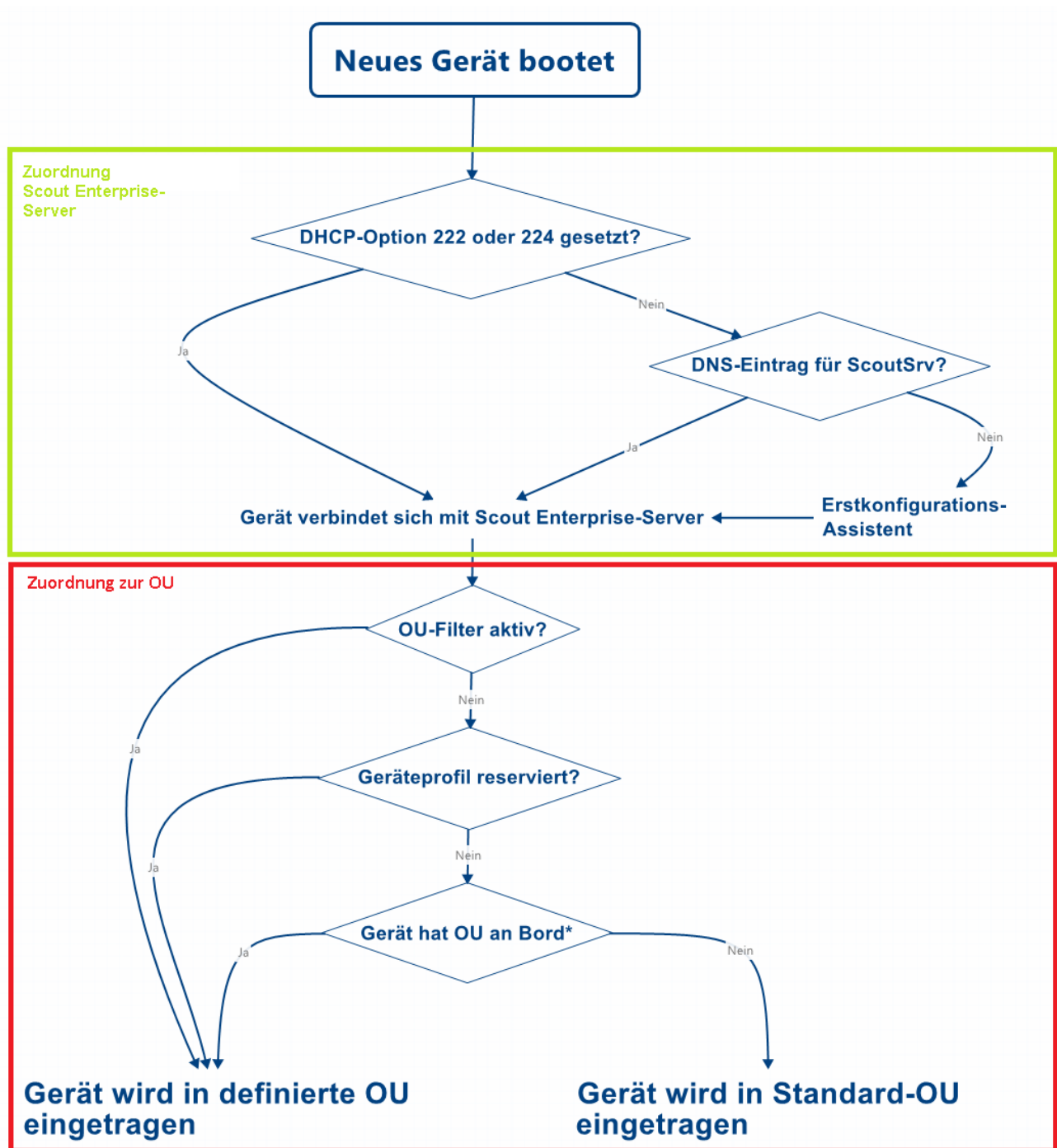
- DNS: Der DNS-Server löst den Hostnamen des Scout Enterprise-Servers `ScoutSrv` (Groß-/ Kleinschreibung irrelevant) auf.

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:

- ▶ 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.



*Eine OU kann dem Gerät beispielsweise durch die DHCP-Option 223 oder den Erstkonfigurations-Assistent mitgegeben werden

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

– optional –



Hinweis

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

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

- IP-Adresse oder Name des Scout 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 <i>Diese Eingabe wird automatisch mit dem hexadezimalen Wert ergänzt (45 4C 55 58 4E 47).</i>

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

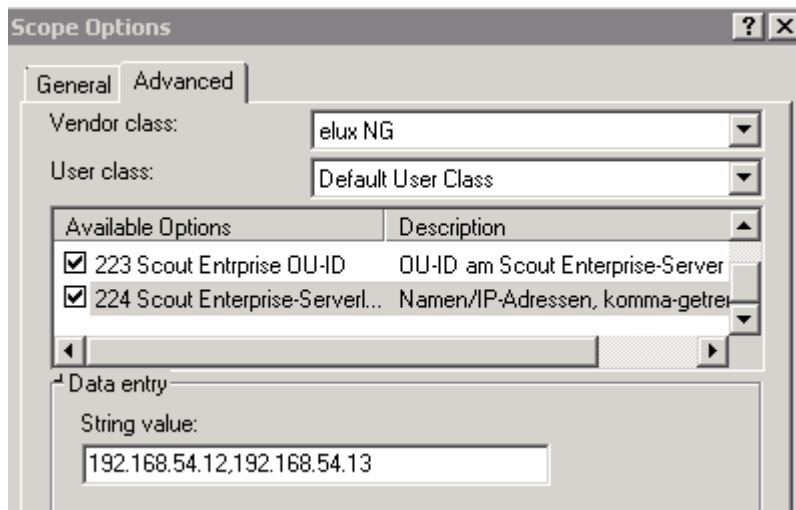
7. Wenn Sie neue Geräte über DHCP einer bestimmten OU zuordnen möchten, erstellen Sie mit **Hinzufügen** eine Option mit folgenden Angaben:

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.

- Öffnen Sie den DHCP-Manager.
- Markieren Sie den relevanten DHCP-Server und wählen Sie **Vorgang > Vordefinierte Optionen einstellen...** und dann im Listenfeld **Optionsklasse** den Eintrag **DHCP-Standardoptionen**.
- Erstellen Sie mit **Hinzufügen** folgende Standard-Optionen nach dem in Methode 1 beschriebenen Muster:
 - Scout Enterprise Server, Zeichenkette, 222
 - Scout Enterprise-Serverliste, Zeichenkette, 224
 - Scout Enterprise OU-ID, Lang, 223
- 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 (Geräte-Konfiguration, Anwendungsdefinition, erweiterte Dateieinträge, Dateiübertragung).



Hinweis

Wenn der OU-Filter aktiv ist, bestimmt dieser die Ziel-OU bzw. Ziel-OUs. Für weitere Informationen siehe [Erweiterte Geräte-Konfiguration/Geräte](#).

Voraussetzungen:

- Die Geräte sind eingeschaltet und mit dem Netzwerk verbunden.
- Die Geräte haben gültige IP-Adressen.
- Das Geräte-Kennwort 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:

IP-Adresse Start	Erste IP-Adresse im Bereich
Zähler	Anzahl der IP-Adressen im Bereich (maximal 255)
IP-Adresse Ende	Letzte IP-Adresse im Bereich
Kennwort	Geräte-Kennwort (Standard: <code>elux</code>) Das Geräte-Kennwort muss mit dem aktuell gültigen Geräte-Kennwort der jeweiligen Clients übereinstimmen.
Ziel-OU	Die OU, der die Geräte zugeordnet werden sollen Default ist die vordefinierte OU <code>Lost&Found</code> mit der Basis-Geräte-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 abgebrochen werden	Erlaubt dem Benutzer, den Neustart zu unterdrücken. Die Konfiguration 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 für den Client bereits ein Geräteprofil reserviert wurde, 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



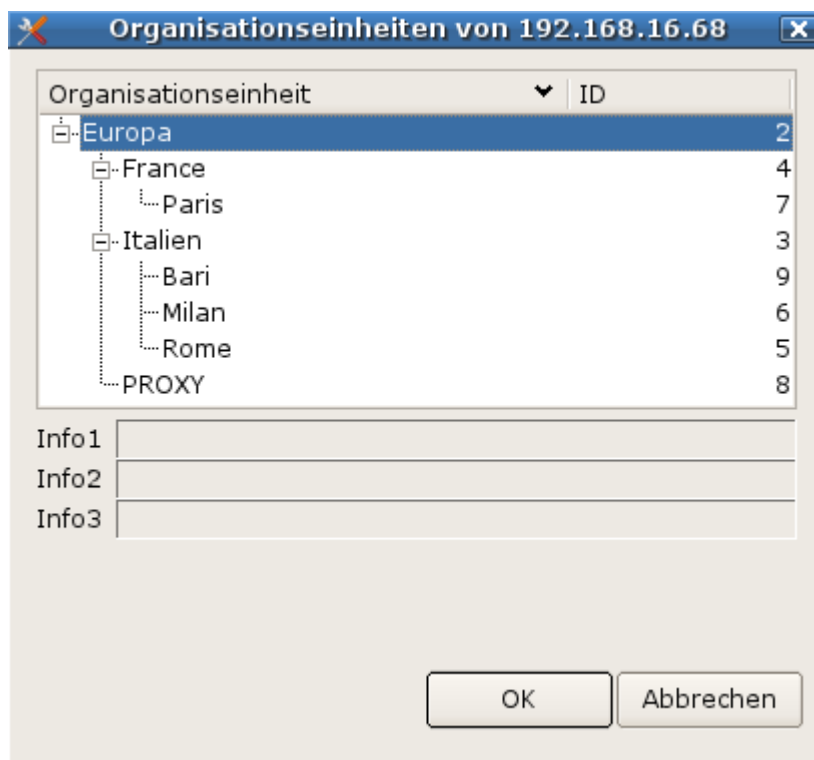
Hinweis

Diese Funktion ist bis eLux RP 5.x verfügbar. In eLux RP 6 verwenden Sie das Configuration panel unter **Scout Enterprise > OU-Zuordnung**.

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.
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 Gerätenamen verwendet.

Wenn für den Client bereits ein Geräteprofil reserviert wurde, 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 Geräte-Konfigurationsdaten 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 **Geräte-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.

Zwei Optionen zur Konfiguration des OU-Filters stehen zur Verfügung:

- 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 Geräte-Konfiguration¹ > Management**).



Hinweis

OU-Filter werden beim Export der Datenkategorie **Erweiterte Optionen** berücksichtigt. Für weitere Informationen siehe [Import/Export](#).

¹früher: Erweiterte Einstellungen

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-Netzwerkadresse)**.
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.

OU-Zuweisung durch benutzerdefinierten OU Filter

Filtertyp: Subnetz-Filter (Client-Netzwerkadresse) Filter für alle Geräte aktivieren: Aktivieren...

Netzadresse: 192.168.16.0 Netzmaske (CIDR Notation): 24 OU: Enterprise

Hinzufügen Lösch

Subnetz - Adresse	Subnetz - Maske	Organisationseinheit	Aktiviert
192.168.16.0	24	Enterprise / IT / Rome	<input checked="" type="checkbox"/>
192.168.17.0	24	Enterprise / IT / Milan	<input checked="" type="checkbox"/>

Nicht zutreffende Geräte werden: ignoriert OK Abbrechen

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, IDF-Name,¹ MAC-Adresse.²

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:

Geräte-Information aus dem OU-Filtertext	Vergleichsoperator =	Wert, auf den Sie filtern möchten
---	-------------------------	-----------------------------------

Beispiele:

```
ELUX_HOSTNAME=Melissa;
ELUX_OSNAME=eLux RP;
ELUX_OSVERSION=6.1.0-3;
```

¹ab eLux RP 5.7 und eLux RP 6.2

²ab eLux RP 5.7 und eLux RP 6.2

```

ELUX_SERIAL=72500422542;
ELUX_SUPPLIER=WYSE;
ELUX_DEVICETYPE=ZQ Class;
ELUX_BIOS=1.0J;
ELUX_CPU=1500;
ELUX_PRODUCT=ZQ Class;
ELUX_KERNEL=4.9.30;
ELUX_FLASH=16GB SATA Flash;
ELUX_FLASHSIZE=15272;
ELUX_MEMORY=4096;
ELUX_GRAPHICS=ATI AMD Radeon HD8330E;
ELUX_IDF=rec5608.idf;1
ELUX_MAC=7CD30A22D0AE2

```


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.

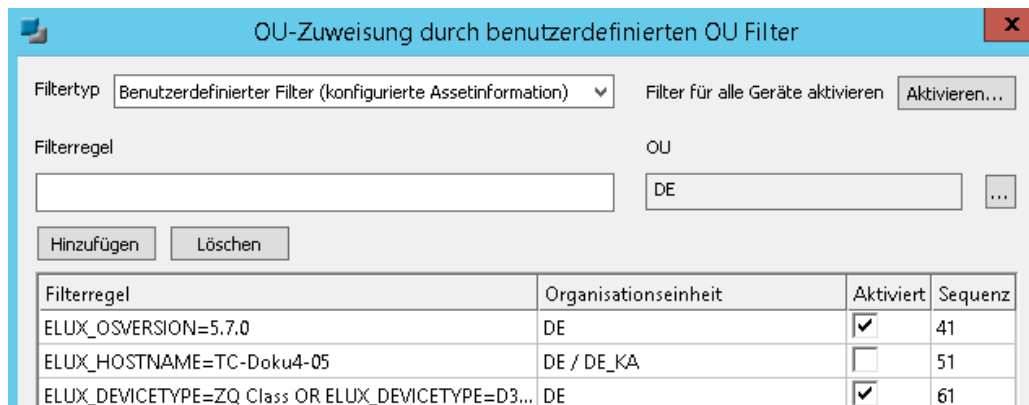
Beispiele für Filterregeln:

Beispiel 1: ELUX_OSNAME=eLux RP AND ELUX_OSVERSION=5.7

Beispiel 2: ELUX_DEVICETYPE=D3314-A1 OR ELUX_DEVICETYPE=ZQ Class

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

Die Filterregel wird im unteren Feld angezeigt.



Filterregel	Organisationseinheit	Aktiviert	Sequenz
ELUX_OSVERSION=5.7.0	DE	<input checked="" type="checkbox"/>	41
ELUX_HOSTNAME=TC-Doku4-05	DE / DE_KA	<input type="checkbox"/>	51
ELUX_DEVICETYPE=ZQ Class OR ELUX_DEVICETYPE=D3...	DE	<input checked="" type="checkbox"/>	61

- Optional fügen Sie weitere Filterregeln hinzu und nehmen weitere Einstellungen vor. Für weitere Informationen siehe [OU-Filterregeln bearbeiten](#).
- Definieren Sie bei **Nicht zutreffende Geräte werden**, was mit Geräten passieren soll, die nicht

¹ab eLux RP 5.7 und eLux RP 6.2

²ab eLux RP 5.7 und eLux RP 6.2

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 mit Hilfe des benutzerdefinierten Filters der angegebenen OU zugeordnet. Wenn zusätzlich 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.

- 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.

- Überprüfen Sie alle aktiven Filterregeln sorgfältig, um unbeabsichtigte Zuordnungen zu vermeiden.
- 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 Geräte-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**.

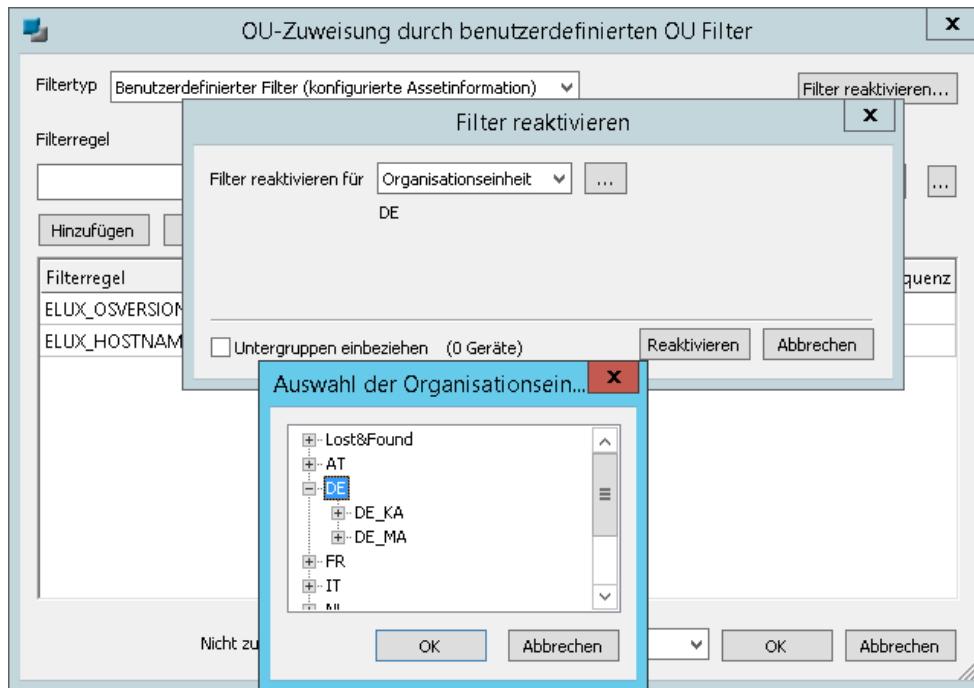
Das Gerät ist der neuen OU zugeordnet und der OU-Filter ist für dieses Gerät deaktiviert.


4.7.5. OU-Filter re-aktivieren

Nachdem der OU-Filter für einzelne Geräte deaktiviert wurde, beispielsweise durch das Verschieben von Geräten über Drag&Drop, können Sie die betroffenen Geräte wieder zurückholen, indem Sie den OU-Filter re-aktivieren.

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-Zuweisung durch benutzerdefinierten Filter** zu öffnen.
4. Klicken Sie oben rechts auf die Schaltfläche **Filter reaktivieren...**¹

¹Bis Scout Enterprise Management Suite Version 15.1 kann die Schaltfläche **Aktivieren...** dazu verwendet werden, den OU-Filter wieder für **alle** Geräte zu aktivieren. Die Auswahl-Option wird erst ab Version 15.2 unterstützt.



5. Wählen Sie, ob Sie den OU-Filter für alle Geräte, für eine Organisationseinheit (OU) oder für eine Dynamische Gerätegruppe re-aktivieren möchten.
6. Um den OU-Filter für eine OU oder Dynamische Gerätegruppe zu re-aktivieren, klicken Sie neben der Auswahl auf die Schaltfläche  und wählen die gewünschte OU oder Dynamische Gerätegruppe.

Um untergeordnete OUs einzubeziehen, aktivieren Sie die Option **Untergruppen einbeziehen**.

7. Bestätigen Sie mit **Reaktivieren** und **OK**.

Der OU-Filter wird für die gewählten Geräte aktiviert.

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. Im einzelnen können folgende Funktionen angewendet werden:

- Kommandos
- Konfigurationslauf
- Vormerkungen für Update
- Vormerkungen für Geräteumzug

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. 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.

Berechtigungen

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

Das Ausführen von Kommandos und anderen Funktionen auf eine Dynamische Gerätegruppe unterliegt standardmäßig den Objektrechten, die für die jeweiligen Geräte und OUs konfiguriert wurden.¹ Dies kann dazu führen, dass eine Funktion nicht ausgeführt werden kann, weil auf mindestens ein Gerät die erforderlichen Objektrechte fehlen. Die Prüfung auf die zugrundeliegenden Objektrechte kann unter **Sicherheit > Administratorenverwaltung > DGG-Berechtigungen** ausgeschaltet werden.

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.

¹ab Scout Scout Enterprise-Konsole 15.1

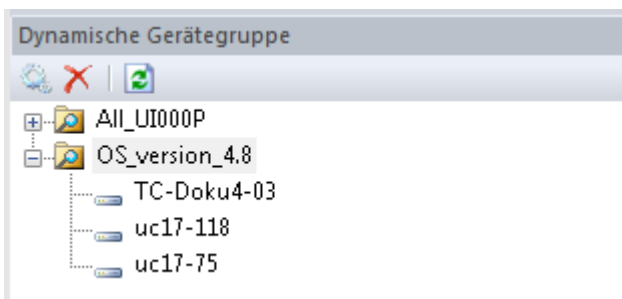
Für weitere Informationen zur Definition von dynamischen Gerätegruppen siehe [Dynamische Gerätegruppen erstellen](#) im Scout Enterprise-Reportgenerator-Handbuch.

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.

Wenn die erforderlichen Objektrechte vorhanden sind, werden Kommandos und Vormerkungen 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.

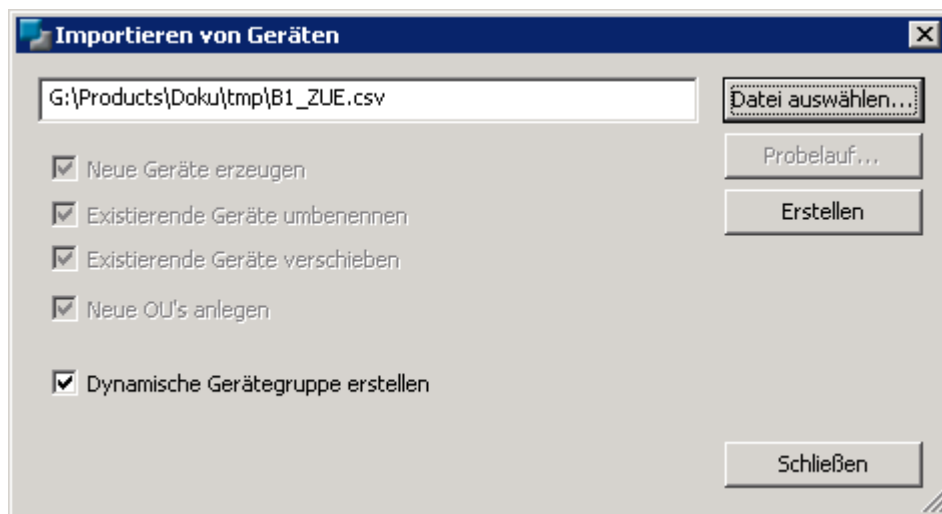
Dynamische Gerätegruppe über Geräte-Import erstellen



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**.

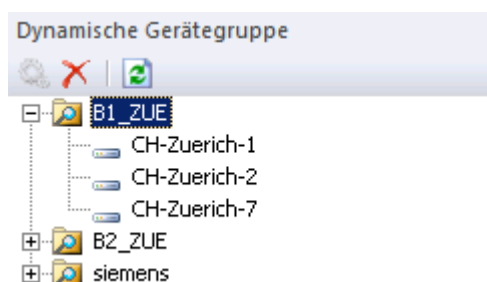
Die Optionen für den Geräte-Import werden abgeblendet.

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. Geräteumzug zwischen Scout Enterprise-Servern

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 oder höher
- eLux RP Version 4.10 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 werden 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 (Version 14.5.0 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 Konfigurationseinstellungen 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 –

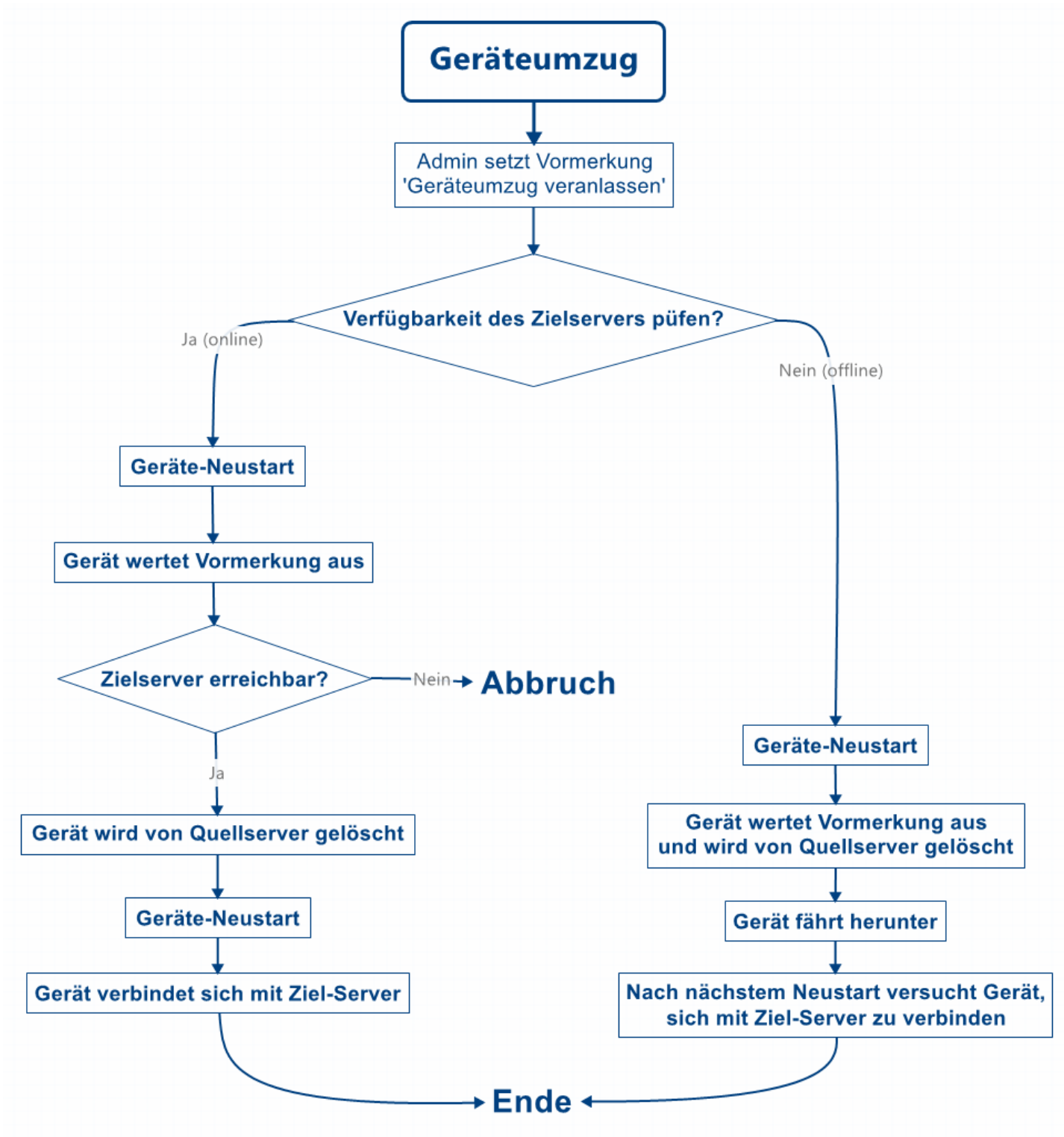
Das Umzugsverfahren wird vom Quell-Server (Geräte-abgebender Server) initiiert und von den betroffenen Geräten durchgeführt. Beim Offline-Verfahren entfällt die Prüfung des Geräte-aufnehmenden Ziel-Servers auf Verfügbarkeit und Durchführbarkeit.

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 werden 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 Zielsystem 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



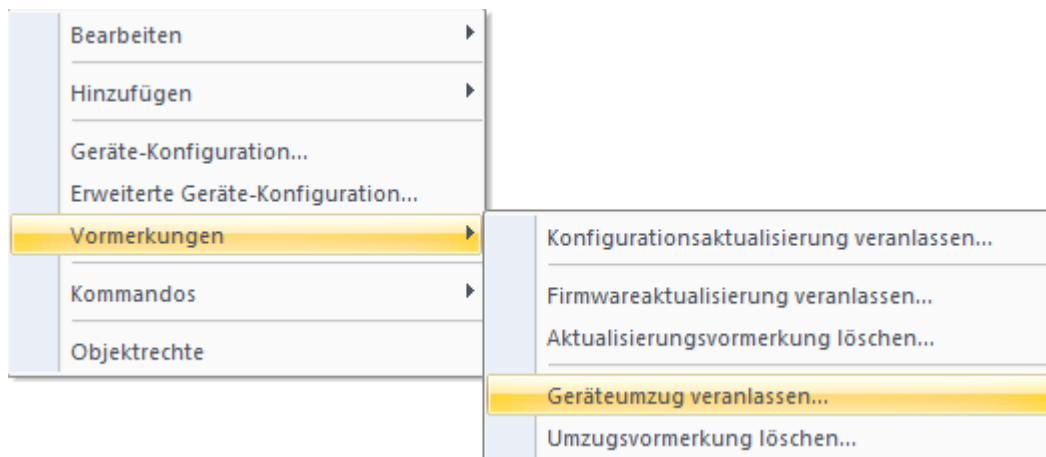
4.9.4. Geräteumzug veranlassen



Voraussetzung

- Deaktivieren Sie auf dem Zielserver die Option **Erweiterte Geräte-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 jedoch DHCP-Optionen für den Quell-Server konfiguriert wurden, müssen Sie am Ziel-Server in der Geräte-Konfiguration **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.

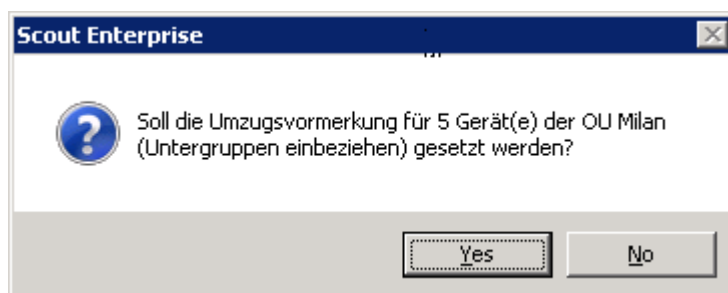
6. Um vor dem Umzug die Verfügbarkeit des Zielserverns prüfen zu lassen ("Online"-Umzug), stellen Sie sicher, dass die Option `Verfügbarkeit des neuen Scout-Servers vor dem Umzug prüfen` aktiv ist.
7. Wenn Sie Geräte in eventuell vorhandenen untergeordneten OUs berücksichtigen möchten, aktivieren Sie die Option **Untergruppen einbeziehen**.

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

Hinweis

Vormerkungen werden immer für alle ausgewählten Geräte gesetzt oder gelöscht, unabhängig davon ob für einzelne Geräte bereits eine Vormerkung vorhanden war.

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.

Umzugsvormerkung	Aktiviert (doku4.unicon-ka.de / 192.168.1...
------------------	--

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.

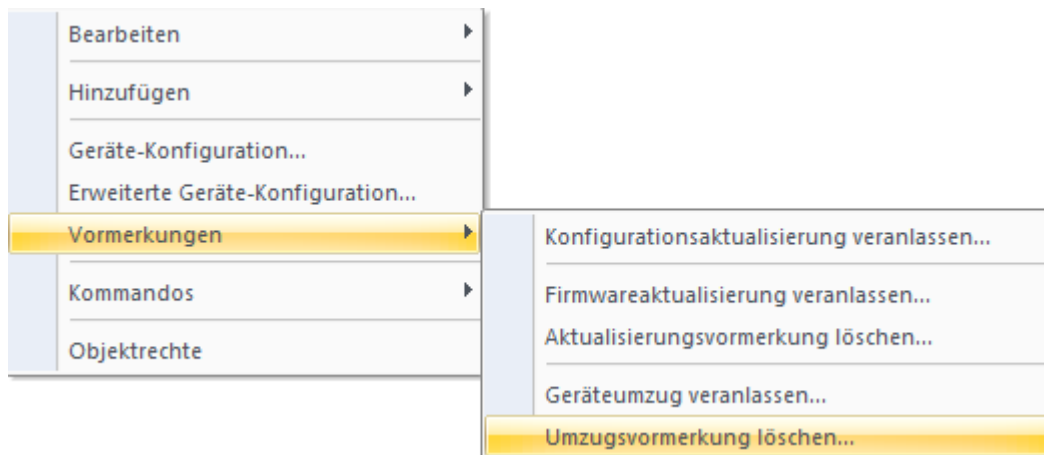
Die relevanten Geräte werden zu dem von Ihnen festgelegten Zeitpunkt umgezogen und bekommen ihre Konfiguration vom Ziel-Server.

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.*



Hinweis

Vormerkungen werden immer für alle ausgewählten Geräte gesetzt oder gelöscht, unabhängig davon ob für einzelne Geräte bereits eine Vormerkung vorhanden war.

5. Geräte-Konfiguration

5.1. Konzept

Für die effiziente Verwaltung zahlreicher Thin Clients ist die Geräte-Konfiguration 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-Geräte-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 Geräte-Konfiguration der Clients in Abhängigkeit der auf den Clients installierten Software-Paketen erfolgt.

5.1.1. Vererbung der Konfiguration

Die Basis-Geräte-Konfiguration und die Geräte-Konfiguration von OUs können auf niedrigere Instanzen vererbt werden.

Die Basis-Geräte-Konfiguration 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 Geräte-Konfiguration verwenden**¹ aktiv ist, so wird die Geräte-Konfiguration des nächsthöheren Elementes in der Hierarchie auf die aktuell bearbeitete Instanz angewendet. Standardmäßig ist die Verwendung der übergeordneten Instanz durch die Option **Übergeordnete Geräte-Konfiguration verwenden** aktiv, sodass ein Gerät seine Geräte-Konfiguration von der Basis-Geräte-Konfiguration erbt.

Die Einstellungen für die Geräte-Konfiguration können auf drei Ebenen in der Scout Enterprise-Konsole verändert werden:

- Basis-Geräte-Konfiguration (**Optionen > Basis-Geräte-Konfiguration**)
- OU (**Kontextmenü > Geräte-Konfiguration**)

¹früher: Übergeordnete Instanz verwenden

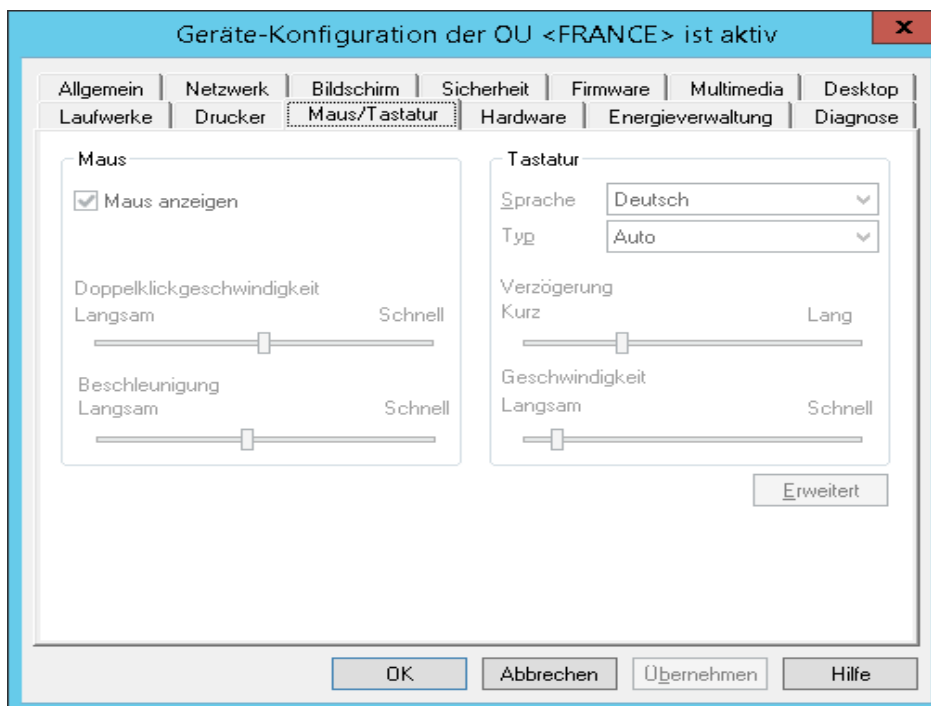
● Gerät (Kontextmenü > Geräte-Konfiguration)

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

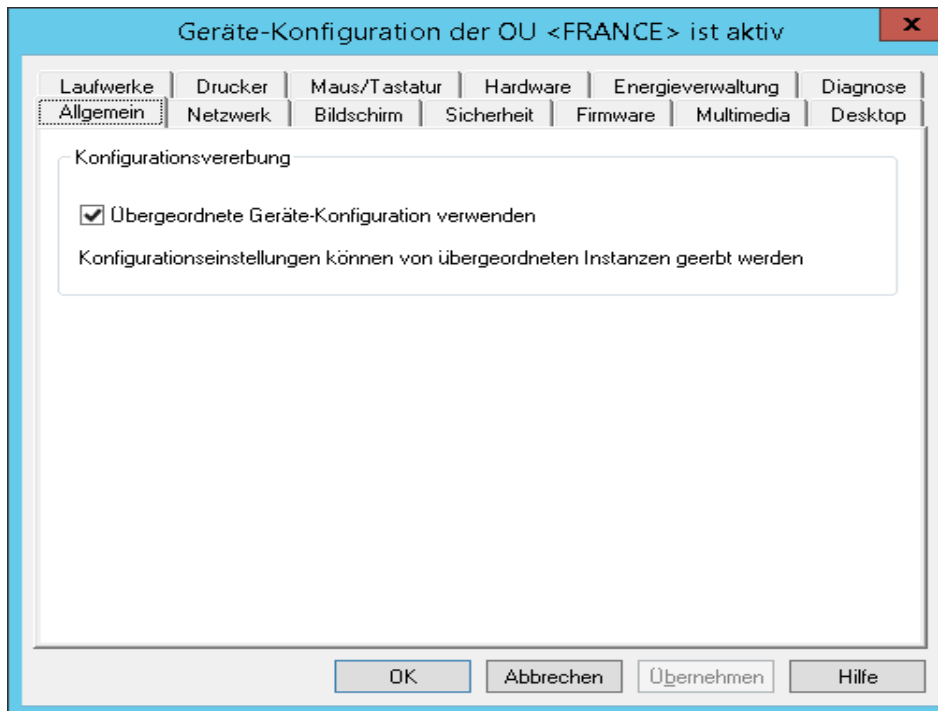
Beachten Sie den jeweils in der Titelleiste des Geräte-Konfigurations-Dialogs angezeigten Gültigkeitsbereich. Das kann die Basis-Geräte-Konfiguration oder eine übergeordnete OU sein.



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

5.1.2. Vererbung unterbrechen - unabhängige Geräte-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 **Geräte-Konfiguration...**

Der Geräte-Konfigurations-Dialog öffnet und zeigt in der Titelleiste die aktuell gültige Instanz für die Geräte-Konfiguration an. Das kann die Basis-Geräte-Konfiguration oder eine übergeordnete OU sein. Für weitere Informationen siehe [Geräte-Konfiguration öffnen](#).

2. Deaktivieren Sie im Register **Allgemein** die Option **Übergeordnete Geräte-Konfiguration verwenden**¹.

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.

¹früher: Übergeordnete Instanz verwenden

5.1.3. Lokale Geräte-Konfiguration schützen

Die Benutzerrechte zur Bearbeitung der lokalen Geräte-Konfiguration 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 Monitor-Einstellungen 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 **Lokale Konfiguration (nicht-gesperrte Felder) beibehalten**.¹

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

Lokale Konfiguration trotz Grundzustand schützen

– ab Scout Enterprise 15.7 und eLux RP 6.7 –

1. Aktivieren Sie die Option **Erweiterte Optionen > Lokale Konfiguration (nicht-gesperrte Felder) beibehalten**, siehe oben.
2. Aktivieren Sie im Kommando-Dialog für den Grundzustand die Option **Lokale Konfiguration beibehalten (nicht-gesperrte Felder)**.

Der Client wird auf den Grundzustand gesetzt und die Geräte-Konfiguration der gesperrten Felder wird zurückgesetzt. Die lokalen Benutzerkonfigurationen in erlaubten Feldern bleiben jedoch erhalten.

Für weitere Informationen siehe [Kommando Grundzustand](#).

Einmalige Aktualisierung der gesamten Geräte-Konfiguration veranlassen

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

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

¹früher: Nur gesperrte Felder werden am Client aktualisiert

Für das Gerät wird vorgemerkt, dass beim nächsten Neustart die gesamte Geräte-Konfiguration inklusive nicht-gesperren Feldern mit der in Scout Enterprise definierten Geräte-Konfiguration überschrieben wird.

5.1.4. Geräte-Konfiguration öffnen

Basis-Geräte-Konfiguration öffnen

- ▶ Wählen Sie im Scout Enterprise-Menü **Optionen > Basis-Geräte-Konfiguration...**

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

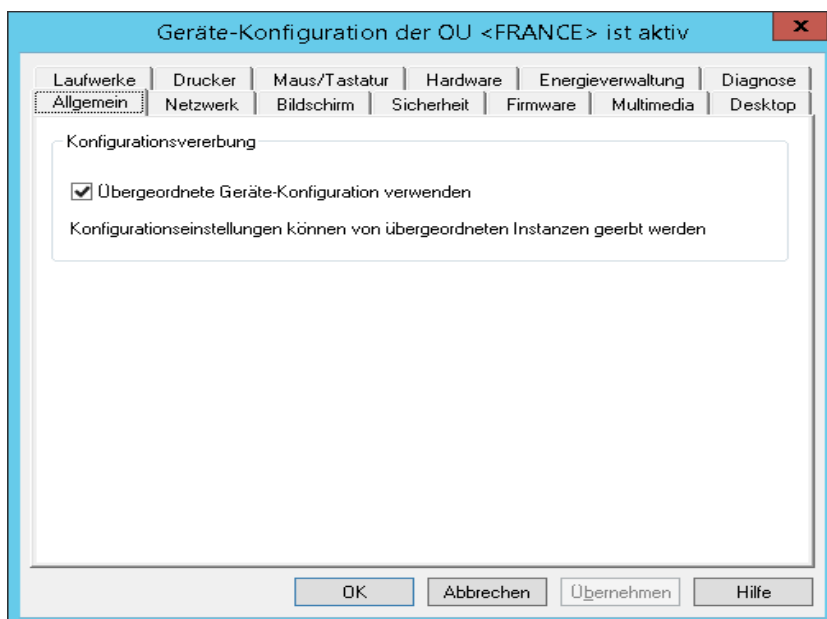
Geräte-Konfiguration für ein Gerät oder OU öffnen

- ▶ Markieren Sie das Element in der Baumstruktur und wählen Sie die Menüoption **Bearbeiten > Geräte-Konfiguration...**

oder

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

Der Dialog **Geräte-Konfiguration** für das markierte Element öffnet. Möglicherweise sind die Optionen abgeblendet, weil die Option **Übergeordnete Geräte-Konfiguration verwenden**¹ eingeschaltet ist. Die jeweilige OU oder die Basis-Geräte-Konfiguration wird dann in der Titelleiste angegeben.



Die Abbildung zeigt den Geräte-Konfigurations-Dialog eines Gerätes unterhalb der OU *FRANCE*. Wenn der Dialog wie oben beschrieben geöffnet wurde, sind die Optionen auf den anderen Registern abgeblendet, weil die übergeordnete Instanz verwendet wird.

¹früher: Übergeordnete Instanz verwenden

Jeweils gültige Geräte-Konfiguration öffnen (bevorzugte Methode)

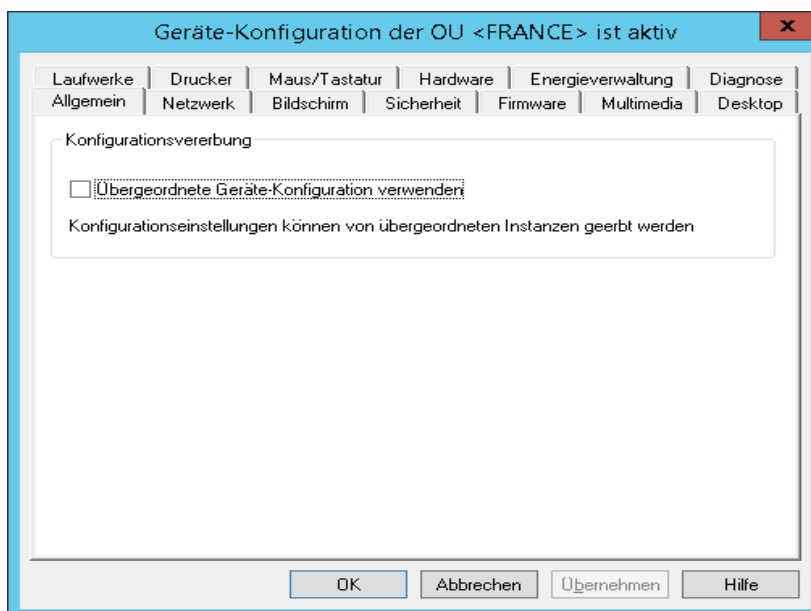
Mit dieser Methode kommen Sie schnell und einfach an die Stelle, an der die Geräte-Konfiguration für die relevanten Geräte definiert sind.

1. Markieren Sie ein Gerät (oder eine OU) in der Baumstruktur.
2. Um das **Eigenschaften**-Fenster anzuzeigen, wählen Sie **Ansicht > Fenster > Eigenschaften-Fenster**.

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

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

Die aktuell gültige Geräte-Konfiguration wird geöffnet. Dies kann die Geräte-Konfiguration einer übergeordneten Instanz sein. Die Optionen der anderen Register sind wählbar soweit durch die Benutzerrechte zugelassen.



*Die Abbildung zeigt die gültige Geräte-Konfiguration für das gleiche Gerät. Dies ist die Konfiguration für die OU *France*.*



Hinweis

Um Änderungen zu speichern, genügt ab Scout Enterprise Management Suite 15.4 ein Klick auf **Übernehmen**. In früheren Versionen muss der Dialog außerdem mit **OK** geschlossen werden, damit die Änderungen gespeichert werden.

5.1.5. Geräte-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 Geräte-Konfiguration 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 **All** in der Symbolleiste des Fensters **Konfigurationsvergleich**.

Alle Eigenschaften werden angezeigt.



Hinweis

Um die aktuelle Geräte-Konfiguration eines Gerätes mit der in der Konsole definierten Geräte-Konfiguration auf Übereinstimmung zu überprüfen (Soll – Ist), verwenden Sie einen Geräte-Report. Für weitere Informationen siehe [Auswertung von Konfigurationsinformationen](#).

5.1.6. Konfigurationstransfer sperren

– ab Scout Enterprise Management Suite Version 15.0¹ –

Einzelne Geräte können von der Aktualisierung der Geräte-Konfigurationsdaten ausgeschlossen werden.



Voraussetzung

Objektrecht **Konfigurationstransfer aktivieren/ sperren**

1. Öffnen Sie für das relevante Gerät das Kontextmenü.
2. Wählen Sie die Option **Konfigurationstransfer sperren**.

¹ersetzt die Funktion **Verwaltung deaktivieren** aus früheren Scout Enterprise Management Suite-Versionen

Das Gerät wird nicht mit neuen Geräte-Konfigurationsdaten versorgt, bleibt jedoch weiterhin in der Scout Enterprise-Verwaltung.



Hinweis

Für neu hinzugefügte Geräte ohne Management-Lizenz wird der Konfigurationstransfer automatisch gesperrt.

5.2. Konfigurationsmethode

Während die mit der Scout Enterprise Management Suite verwalteten Clients starten, verbinden sie sich zu ihrem Scout Enterprise-Server und prüfen unter Berücksichtigung der Vererbung, ob Aktualisierungen vorliegen. Aktualisierungen können sich auf folgende Daten beziehen:

- Geräte-Konfiguration
- Anwendungsdefinition
- Konfigurierte Dateiübertragung
- Erweiterte Dateieinträge

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.

5.2.1. Konfigurationslauf

– ab Scout Enterprise Management Suite Version 14.6 –

Wenn aktualisierte Konfigurationsinformationen 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 der Administrator die Ermittlung und komprimierte Speicherung der Konfigurationsinformationen durch einen Konfigurationslauf vorab (z.B. abends/nachts) initiieren. Die dadurch in einem Datenobjekt vorbereiteten Konfigurationsinformationen werden beim nächsten Neustart der Clients, beispielsweise am nächsten Arbeitstag, in einem Schritt übertragen.

Konfigurationslauf durchführen



Hinweis

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

-
1. Öffnen Sie für die relevante OU oder Dynamische Gerätegruppe das Kontextmenü und wählen Sie **Kommandos**.

Kommando: Konfigurationslauf

☐ Sofort

☒ Einmalig

Datum: Sonntag ,30.07.2017

Zeit: 12:00

☐ Wiederholend

Monatstag: 1, 2, 3, 4

Zeit: 14:51

Einplanen Abbrechen

2. Wählen Sie aus dem Untermenü das Kommando **Konfigurationslauf...**
3. Legen Sie den Zeitpunkt der Ausführung fest und bestätigen Sie mit **Einplanen**.


*Der Bearbeitungsfortschritt wird im Dialog **Kommandoverlauf** angezeigt.*

5.3. Auswertung von Konfigurationsinformationen

Der Report-Generator bietet verschiedene Felder zur Auswertung von Konfigurationsinformationen:

Konfigurations-ID	<p>ID für ein komprimiertes Datenobjekt mit Konfigurationsdaten</p> <p>Wird erstellt durch einen Konfigurationsabgleich beim ersten Kontakt zwischen Server und Client nach dem Ändern von Konfigurationseinstellungen oder durch einen Konfigurationslauf</p>
Konfiguration aktuell	<p>Ja – Client hat die Konfiguration, die per Konsole aktuell für ihn definiert ist</p> <p>Nein – Client hat eine ältere eLux-Version, die das Feld nicht auswerten kann</p>
Konfigurationstransfer	<p>Für den Client ist die Option Konfigurationstransfer sperren gesetzt</p> <p>Für weitere Informationen siehe Konfigurationstransfer sperren.</p>

Beispiel:

 Filter

Filter

	Operator	Not	(Spalte / Inhalt	Vergleich	Wert
→		NOT		Konfiguration aktuell	LIKE	%Ja%

5.4. FollowMe-Desktop

– ab Scout Enterprise 15.8 –



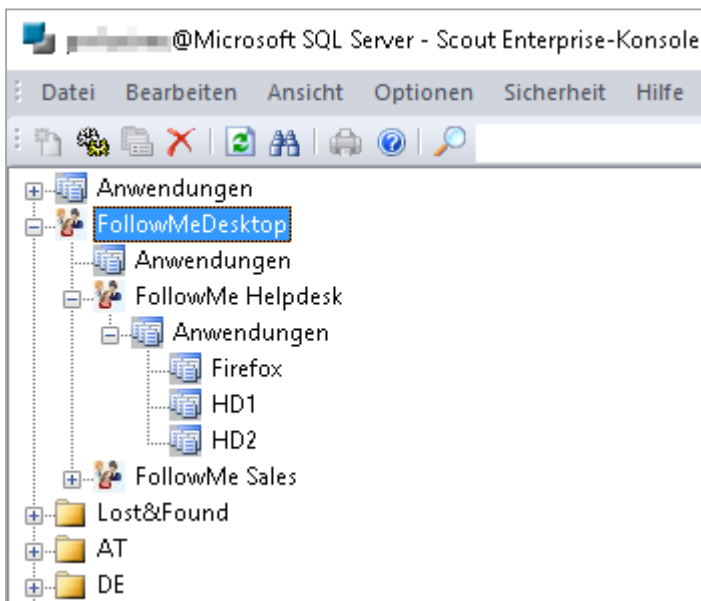
Hinweis

Die Benutzer-Authentifizierung über Active Directory muss konfiguriert sein.

FollowMe-Desktop ermöglicht Benutzer-spezifische Konfigurationseinstellungen, die geräteübergreifend genutzt werden können.

Neben der Geräte-Konfiguration, die an das Gerät gebunden ist, erlaubt die Funktion des FollowMe-Desktop eine Benutzer-orientierte Konfiguration, die der Benutzer zu beliebigen Geräten "mitnehmen" kann. Ein konfiguriertes Desktop-Layout und konfigurierte Anwendungen "folgen" dem Benutzer, unabhängig davon, auf welchem Gerät er sich anmeldet.

Die Konfiguration des FollowMe-Desktop erfolgt in dem gleichnamigen Knoten in der Baumstruktur, der als Basis-OU auf der obersten Ebene realisiert ist. Diese FollowMe-Desktop-Instanz kann direkt genutzt werden oder als Container für weitere FollowMe-Konfigurationen fungieren, die als untergeordnete OUs hinzugefügt werden. Damit lässt sich eine Geräte-unabhängige und Hierarchie-übergreifende Struktur von Konfigurationen abbilden, die beispielsweise durch fachliche Funktionen der Benutzer motiviert ist. Zum Beispiel könnte eine OU **FollowMe Helpdesk** alle Anwendungsdefinitionen und das Desktop-Layout für Helpdesk-Mitarbeiter enthalten.



Eine FollowMe-Desktop-Konfiguration kann aus Anwendungsdefinitionen und definierten Konfigurationswerten der Geräte-Konfiguration bestehen. Für weitere Informationen siehe "Umfang der konfigurierbaren Optionen" auf Seite 73.

Die FollowMe-Konfigurationen werden den Benutzern über AD-Eigenschaften zugeordnet. Auf die FollowMe-Desktop-Instanz und alle untergeordneten OUs werden Filterdefinitionen angewendet, die auf die relevante AD-Zugehörigkeit filtern.

Sobald sich ein AD-Benutzer auf einem Gerät anmeldet, für das FollowMe-Desktop aktiviert ist, werden die AD-Eigenschaften des Benutzers mit den Filterdefinitionen der FollowMe-OUs abgeglichen. Wenn eine FollowMe-Konfiguration mit passenden Filterwerten vorhanden ist, wird anschließend der Desktop mit dem in dieser FollowMe-OU definierten Layout und Anwendungen geladen. Während der Benutzer mit der FollowMe-Konfiguration arbeitet, kann er zwar Änderungen in der Konfiguration durchführen, beispielsweise Anwendungssymbole frei auf dem Desktop platzieren, aber die Änderungen werden nicht gespeichert.

Nachdem der Benutzer seine Sitzung beendet und sich abmeldet, wird wieder die ursprüngliche Geräte-Konfiguration aktiviert.

FollowMe-Desktop-Konfigurationen können exportiert und importiert werden.

5.4.1. FollowMe-Desktop konfigurieren

Um FollowMe-Desktop einsetzen zu können, benötigen Sie eine oder mehrere FollowMe-Konfigurationen, die Sie jeweils über Filterdefinitionen bestimmten AD-Benutzern zur Verfügung stellen. Außerdem definieren Sie, auf welchen Geräten das Abrufen einer FollowMe-Konfiguration möglich sein soll.

FollowMe-Konfigurationen erstellen



Voraussetzung

Administratoren-Basisrecht **OU für FollowMe-Desktop anzeigen**

1. Erstellen Sie in der Baumstruktur unterhalb der Basis-OU **FollowMe-Desktop** weitere FollowMe-OUs, beispielsweise eine OU **FollowMe Helpdesk**. Verwenden Sie dazu das Kontextmenü mit **Hinzufügen > Organisationseinheit**.
2. Bearbeiten Sie die Geräte-Konfiguration der neuen FollowMe-OUs (Desktop, Laufwerke, USB-Optionen, Energieverwaltung). Fügen Sie den FollowMe-OUs anschließend die gewünschten Anwendungsdefinitionen hinzu.



Hinweis

Neue FollowMe-Desktop-OUs übernehmen keine Konfigurationswerte aus der Basis-Geräte-Konfiguration und keine Basis-Anwendungen. Innerhalb der FollowMe-Desktop-Struktur ist die Vererbung jedoch standardmäßig aktiv. Untergeordnete FollowMe-OUs erben Geräte-Konfiguration und Anwendungen der übergeordneten FollowMe-Desktop-Instanz, solange Sie die Vererbung nicht ausschalten.

Die Konfigurationswerte einer FollowMe-OU überschreiben die Werte der am Gerät gültigen Geräte-Konfiguration.

3. Definieren Sie für jede FollowMe-OU einen Filter, der auf eine AD-Mitgliedschaft filtert. Verwenden Sie dazu die Kontextmenü-Option **Filter setzen**.



Hinweis

Die Filterdefinitionen sind unabhängig von einer möglichen Vererbung der Konfiguration. Setzen Sie für jede FollowMe-OU einen eigenen Filter.

Filterregel	Organisationseinheit	Aktiviert	Sequenz
GROUP=Helpdesk	FollowMeDesktop / FollowMe He...	<input checked="" type="checkbox"/>	60

In der Filterregel können Sie auf die AD-Eigenschaften **Benutzer**, **Gruppe** oder **Domäne** filtern.

Syntax: USER | GROUP | DOMAIN=<Wert>

Mehrere Filterregeln sind erlaubt.



Hinweis

Für Geräte, für die FollowMe-Desktop aktiviert ist, werden die übermittelten AD-Eigenschaften des Benutzers in die Protokolldatei `eluxd.log` geschrieben (suche `FollowMeDesktop`).

Alle aktiven Filterregeln werden in der angegebenen Reihenfolge abgearbeitet. AD-Benutzer, die auf diese Filterdefinition passen, erhalten nach der Anmeldung auf Geräten, für die FollowMe-Desktop aktiviert ist, die Anwendungen und Desktop-Eigenschaften, die in der FollowMe-OU konfiguriert wurden.

Benutzer-orientierte FollowMe-Konfigurationen sind definiert. Definieren Sie im nächsten Schritt, für welche OUs oder Geräte diese Konfigurationen abgerufen werden dürfen.

Geräte für FollowMe-Desktop aktivieren

Sie können definieren, welche Geräte für die Verwendung mehrerer Konfigurationen eingerichtet werden sollen. Es kann sinnvoll sein, dass ein Benutzer an seinem Arbeitsplatz-Gerät die in der OU-Struktur definierte Geräte-Konfiguration verwendet, aber auf bestimmten Geräten beispielsweise im Service-Bereich eine FollowMe-Konfiguration.

In der Geräte-Konfiguration einer OU / eines Gerätes (oder in der Basis-Geräte-Konfiguration) legen Sie fest, ob die relevanten Geräte FollowMe-Konfigurationen abrufen sollen, wenn ein entsprechender AD-Benutzer sich anmeldet.



Aktivieren Sie in der Geräte-Konfiguration für die relevanten Geräte unter **Allgemein > FollowMe-Desktop** die Option **Konfiguration für angemeldete Benutzer abrufen**.

Nach der Anmeldung eines AD-Benutzers werden dessen AD-Eigenschaften ausgewertet. Wenn der Scout Enterprise-Server eine passende FollowMe-OU findet, wird die dort definierte Konfiguration geladen.

5.4.2. Umfang der konfigurierbaren Optionen

Für FollowMe-OUs können die folgenden Eigenschaften konfiguriert werden:

- Alle Anwendungstypen mit allen Anwendungseigenschaften
- Software-Standardeinstellungen für Firefox und Chromium (Browser-Home-Verzeichnis)
- Geräte-Konfiguration mit folgenden Optionen

Desktop	Alle Optionen außer Datum und Zeit
Desktop > Erweitert	Sortiere Config Panel Systemleiste Hintergrundbild
Laufwerke	Alle Optionen
Hardware	Alle USB-Optionen
Energieverwaltung	Alle Optionen

Konfigurationswerte einer FollowMe-OU überschreiben die Konfigurationswerte der "normalen" Geräte-Konfiguration am Gerät. Für nicht aufgeführte Optionen bleiben die Werte der "normalen" Geräte-Konfiguration gültig.

Der Administrator kann für die operativen Administratoren den Umfang der konfigurierbaren Optionen von FollowMe-OUs weiter einschränken (**Sicherheit > Administratoren verwalten > Standard-Objektrechte**).

5.5. Register Allgemein

Übergeordnete Instanz verwenden

Dies ist die wichtigste Option im Register **Allgemein**. Wenn **Übergeordnete Instanz verwenden** 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](#).

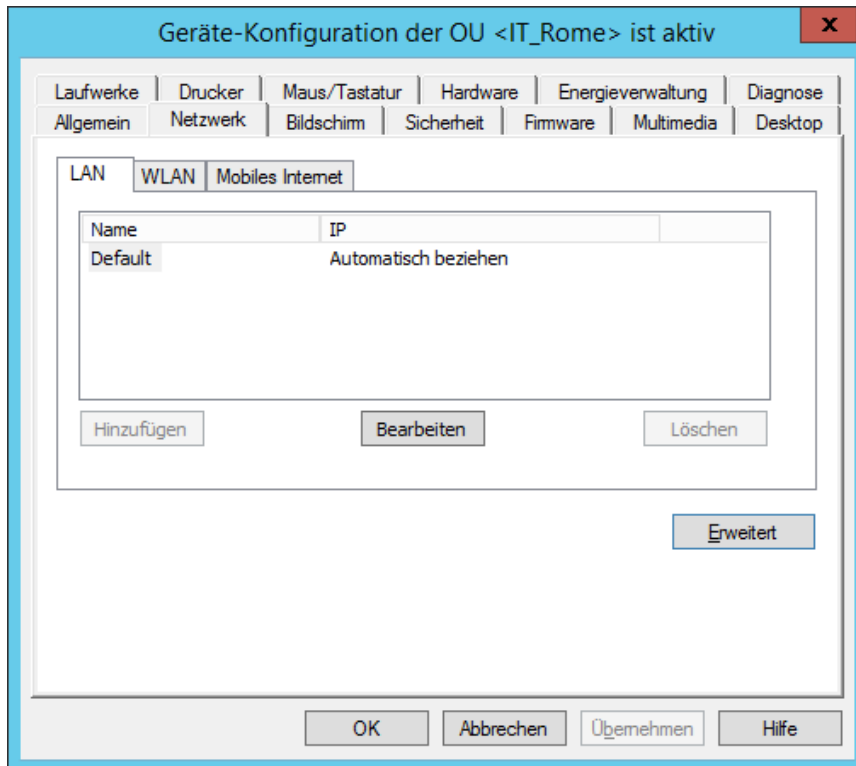
Weitere Optionen

Option	Beschreibung
Automatische Anforderung von Client-Anwendungs-Lizenzen	Berechtigt das Gerät zur automatischen Anforderung von Anwendungs-Lizenzen, wenn Lizenz-pflichtige Anwendungen installiert oder genutzt werden Dazu muss in der Scout Enterprise-Konsole die Option Automatische Zuweisung aktiv sein. Für weitere Informationen siehe Automatische Zuweisung von Anwendungs-Lizenzen in der Kurzanleitung Lizenzverwaltung .
FollowMe-Desktop / Konfiguration abrufen	Erlaubt die Verwendung mehrerer Konfigurationen auf diesem Gerät für berechtigte Benutzer Für weitere Informationen siehe FollowMe-Desktop konfigurieren .

Gerätespezifische Hardwareinformationen einzelner Geräte werden im **Eigenschaften**-Fenster der Scout Enterprise-Konsole angezeigt. Für weitere Informationen siehe [Eigenschaften-Fenster](#).

5.6. Register Netzwerk

Abhängig vom installierten Image und der eingebauten Hardware können die Benutzer mehrere Netzwerkverbindungen nutzen. In der Scout Enterprise-Konsole definieren Sie Netzwerkprofile für verschiedene Netzwerk-Typen. Als Netzwerkprofil konfigurierte Netzwerkverbindungen kann der Benutzer am Client über das entsprechende Live-Information Icon auswählen.



Folgende Netzwerkprofile stehen zur Verfügung:

- LAN (nur ein Profil, kann nicht gelöscht werden)
- Wireless LAN
- Mobiles Internet (Wireless Wide Area Network)¹



Hinweis

VPN-Netzwerkprofile werden in der Erweiterten Geräte-Konfiguration für einzelne Geräte erstellt. Für weitere Informationen siehe [VPN](#).

¹ab Scout Enterprise Management Suite 15.5 und eLux RP 6.5

5.6.1. LAN-Verbindung konfigurieren

1. Öffnen Sie für das relevante Gerät oder OU den Dialog **Geräte-Konfiguration > Netzwerk**.
2. Wählen Sie das Register **LAN** und klicken Sie für die **Default**-Verbindung auf die Schaltfläche **Bearbeiten**.
3. Bearbeiten Sie im Dialog **Netzwerkprofil bearbeiten** unter **Ethernet** folgende Felder:

Option	Beschreibung
IP-Adresse automatisch beziehen	Die IP-Adresse wird automatisch über DHCP bezogen. Definieren Sie einen Timeout-Wert in Sekunden. Legen Sie später unter Erweitert das Verhalten für fehlschlagende DHCP-Anfragen fest.
Folgende IP-Adresse verwenden	Alternativ geben Sie eine feste IP-Adresse und die zugehörigen Optionen an.



Hinweis

Wenn Sie keine DHCP-Optionen für Scout Enterprise einsetzen, empfehlen wir, unter **Erweitert** die Option **Scout Enterprise-Server DHCP-Optionen ignorieren** zu aktivieren.

4. Um Netzwerk-Geschwindigkeit und maximale Übertragungseinheit (MTU) anzupassen, bearbeiten Sie das Register **Medium**.
5. Bearbeiten Sie unter **Erweitert** folgende Optionen:

Option	Beschreibung
DHCP-Einstellungen	Legen Sie das Verhalten für fehlschlagende DHCP-Anfragen fest.
Proxy ¹	Definieren Sie einen systemweiten Proxy-Server für dieses Netzwerk-Profil, siehe Proxy-Konfiguration . Auf die hier definierte Proxy-Einstellung bezieht sich die Option <code>System-Proxy</code> in der Browser-Anwendungsdefinition.

¹ab Scout Enterprise Management Suite 15.5

6. Bearbeiten Sie unter **IEEE 802.1X-Authentifizierung** folgende Optionen:¹

Option	Beschreibung
Aktivieren	Aktivieren Sie die IEEE 802.1X-Authentifizierung grundsätzlich.
Aktivierung ohne erfolgreiche Authentifizierung erlauben (nur Ethernet) ²	Legen Sie fest, ob die IEEE 802.1X-Aktivierung auch dann fortgesetzt wird, wenn ein Timeout oder ein Authentifizierungsfehler auftritt (nur für Ethernet-Verbindungen). Wenn die Option nicht aktiv ist (Standard), kann die Aktivierung nur nach erfolgreicher Authentifizierung fortgesetzt werden.
Anzahl automatischer Verbindungsversuche ³	Anzahl der Verbindungsversuche, bevor abgebrochen wird
Anzahl Authentifizierungsversuche ⁴	Anzahl der Authentifizierungsversuche bei erfolgreicher Verbindung, bevor die Authentifizierung abgebrochen wird
Timeout Authentifizierung	Zeitspanne in Sekunden, bevor ein Authentifizierungsversuch abgebrochen wird



Hinweis

Die WPA-Verschlüsselung erfolgt über den WPA-Supplicant und die Konfigurationsdatei `wpa.conf`. Für weitere Informationen siehe [WPA-Unterstützung](#).

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

Mit **Internet-Verbindungstest** können Sie jederzeit überprüfen, ob Web-Adressen über das Internet erreichbar sind.⁵

¹Bis Scout Enterprise Management Suite 15.8 aktivieren Sie IEEE 802.1X unter **Erweitert**

²ab Scout Enterprise Management Suite 15.9

³ab Scout Enterprise Management Suite 15.9

⁴ab Scout Enterprise Management Suite 15.9

⁵ab Scout Enterprise Management Suite 15.9

5.6.2. Erweiterte Netzwerkeinstellungen

Unter **Geräte-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 abgelaufen 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, vorausgesetzt, der Scout Enterprise-Statistikservice ist installiert. 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 Hosts-Liste automatisch übertragen.

5.6.3. 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 beim Einsatz von eLux RP 5-Geräten ein Dummy-WLAN-Profil in der Geräte-Konfiguration erforderlich, das vor dem Benut-

zer versteckt werden kann.¹

Benutzer können parallel zum Corporate WLAN individuelle WLAN-Profil lokal am Client erstellen.² Für die konfigurierten WLAN-Netzwerke kann ein automatisches Verbinden je nach Umgebung oder Priorität stattfinden. Für weitere Informationen siehe [WPA-Unterstützung](#) und (für eLux RP 5) [Corporate WLAN](#).

WLAN-Profil in der Scout Enterprise-Geräte-Konfiguration erstellen (A)

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevante OU den Dialog **Geräte-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 die Systemleiste (Systray/Live-Info) gestartet werden.

4. Um bei jedem Verbindungsaufbau auf eine Internet-Verbindung zu testen, steht die Option **Internet-Verbindungstest** zur Verfügung.³ Für weitere Informationen siehe "Optionen für alle Netzwerkprofile" auf Seite 86.

¹ab eLux RP 5.6

²ab eLux RP 5.6

³ab Scout Enterprise Management Suite 15.9

5. Bearbeiten Sie folgende Optionen:

Option	Beschreibung
Medium / SSID	Service Set Identifier Name für das WLAN-Netzwerk
Medium / Timeout	Zeitspanne in Sekunden für den Verbindungsaufbau bis zum Abbruch
Medium / Kanal	Wird standardmäßig automatisch gewählt
Medium / Verschlüsselung	Art der Authentifizierung <ul style="list-style-type: none"><input checked="" type="radio"/> Keine<input checked="" type="radio"/> WPA mit Pre-shared key (PSK)<input checked="" type="radio"/> WPA2 mit Pre-shared key (PSK) Um über EAP (Extensible Authentication Protocol) zu authentifizieren, wählen Sie Keine und verwenden Sie eine WPA-Konfigurationsdatei. Für weitere Informationen siehe WPA-Unterstützung .
IP / IP-Adresse automatisch beziehen	Die IP-Adresse wird automatisch über DHCP bezogen. Definieren Sie einen Timeout-Wert in Sekunden.
IP / Folgende IP-Adresse verwenden	Alternativ geben Sie eine feste IP-Adresse und die zugehörigen Optionen an.
Erweitert / DHCP-Einstellungen	Legen Sie das Verhalten für fehlschlagende DHCP-Anfragen fest.



Hinweis

Wenn Sie keine DHCP-Optionen für Scout Enterprise einsetzen, empfehlen wir, die Option **Scout Enterprise-Server DHCP-Optionen ignorieren** zu aktivieren.

Erweitert / Proxy ¹	Definieren Sie einen systemweiten Proxy-Server für dieses Netzwerk-Profil, siehe Proxy-Konfiguration . Auf die hier definierte Proxy-Einstellung bezieht sich die Option <code>System-Proxy</code> in der Browser-Anwendungsdefinition.
--------------------------------	--

6. Bestätigen Sie mit **OK**.

¹ab Scout Enterprise Management Suite 15.5

**Hinweis**

Ein lokales WLAN-Profil am Client (B) kann mit entsprechenden Benutzerrechten analog unter eLux in der Geräte-Konfiguration erstellt werden.

**Hinweis**

Zur Überprüfung der Netzwerk-Aktivitäten am Client verwenden Sie die Diagnose-Funktion (Erweiterte Protokollstufe) und die Datei `systemd-journal.log`.¹

WLAN-Profil-Editor am Client anzeigen

– nur für eLux RP 5; unter eLux RP 6 können WLAN-Netzwerke direkt im Configuration panel angezeigt und konfiguriert werden –

Vorhandene WLAN-Netzwerke werden am Client über das Netzwerk-Symbol auf der Systemleiste 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](#).

5.6.4. WPA-Unterstützung

Zur Sicherung Ihres LAN oder 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 lokal auf den Clients gespeichert.

`wpa_supplicant` ist eine freie Software. Für weitere Informationen siehe <http://packages.debian.org/de/sid/wpasupplicant>.

¹ab eLux RP 6.4

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. Übertragen Sie die Konfigurationsdatei `wpa.conf` mit Hilfe der Scout Enterprise- Funktion **Konfigurierte Dateiübertragung** auf die Clients in folgendes Verzeichnis:

LAN	<code>setup/scep/</code>
WLAN	<code>setup/wlan/</code>

Für weitere Informationen siehe [Konfigurierte Dateiübertragung](#).



Hinweis

Für WLAN ist zusätzlich ist die Konfiguration eines Dummy-WLAN-Profiles in der Geräte-Konfiguration erforderlich. Für weitere Informationen siehe [Corporate WLAN](#).

Beispiel für eine WPA-Konfigurationsdatei mit 802.1X (WLAN)

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=1
network={
    ssid="Name des WLAN-Netzwerks"
    scan_ssid=1
    key_mgmt=WPA-EAP
    eap=TLS
    identity="Common Name wie im Zertifikat angegeben"
    priority=6
    ca_cert="/setup/cacerts/root-ca.pem"
    client_cert="/setup/cacerts/client.pem"
    private_key="/setup/cacerts/client.key"
}
```



Hinweis

Netzwerk-Profile (LAN und WLAN), die über eine `wpa.conf` zum Client übertragen werden, können am Client nicht bearbeitet werden.

Für weitere Informationen zur WPA-Konfiguration siehe die Kurzanleitung **IEEE 802.1X-Authentifizierung**.

5.6.5. 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 Gruppenzugehörigkeit, Standort oder Geräte abgestimmt werden.

Eine entsprechende WLAN-Konfiguration verteilen Sie über die WPA-Konfigurationsdatei, siehe [WPA-Unterstützung](#).

Neben dem Einsatz eines Corporate WLAN können Sie den Benutzern erlauben, zusätzliche 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.

Für eLux RP 5 ist für das Corporate WLAN die zusätzliche Definition eines Dummy-WLAN-Profiles in der Geräte-Konfiguration notwendig. Ab eLux RP 6.4 sind durch den neuen Netzwerk-Stack die unten beschriebenen Schritte nicht mehr erforderlich.

Corporate WLAN mit Dummy-Profil konfigurieren

– nur für eLux RP 5 –

1. Erstellen Sie in der Basis-Geräte-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 starten	aktiviert	obligatorisch
SSID	#DUMMY#	
Timeout		Verwenden Sie den Standardwert.
Kanal		Verwenden Sie den Standardwert.
Verschlüsselung	WPA (PSK)	
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

¹ab eLux RP Version 5.6

²ab eLux RP Version 5.6

³ab eLux RP Version 5.6

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 zusätzlich am Gerät erstellen

– nur für eLux RP 5, für eLux RP 6 siehe [WLAN-Verbindung hinzufügen](#) im **eLux**-Handbuch –

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 Systemleisten-Netzwerksymbol und die Schaltfläche **Verbinden** her.

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

5.6.6. Profil für Mobiles Internet (WWAN) erstellen

– ab Scout Enterprise Management Suite 15.5 –

Für mobile Geräte, die über eine entsprechende SIM-Karte verfügen, können Sie Profile definieren, mit denen sich die Benutzer zu einem Mobilfunknetz wie LTE oder UMTS verbinden können.

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevante OU den Dialog **Geräte-Konfiguration > Netzwerk**.
2. Wählen Sie das Register **Mobiles Internet** und klicken Sie auf **Hinzufügen**.
3. Bearbeiten Sie im Dialog **Netzwerkprofil bearbeiten** folgende Optionen:

Option	Beschreibung
Profilname	Name für das neue Profil
Automatisch verbinden	Wenn die Signalstärke ausreichend ist, versucht der Client automatisch, sich zu diesem Mobilfunknetz zu verbinden.
APN	Zugriffspunktname (Access Point Name): Adresse, mit der das Gerät die Datenverbindung ins Mobilfunknetz herstellt
PIN	PIN für die SIM-Karte (falls verwendet) Wenn Sie die Option leer lassen und die SIM-Karte eine PIN benötigt, wird die PIN bei jedem Verbindungsaufbau abgefragt.
Benutzername	Benutzername des Mobilfunkkontos
Kennwort	Kennwort des Mobilfunkkontos
Roaming	Die Datenverbindung wird beibehalten, wenn sich das Gerät außerhalb des Mobilfunkanbieter-Netzes befindet.

4. Bestätigen Sie mit **OK**.

Gesperrte SIM-Karte über Kommando entsperren

Wenn eine SIM-Karte beispielsweise nach falschen PIN-Eingaben gesperrt wurde, können Sie mit Hilfe der PUK eine neue Pin erzeugen.

1. Öffnen Sie für das relevante Gerät das Kontextmenü und wählen **Kommandos > Benutzerdefiniertes Kommando**.
2. Geben Sie folgendes Kommando ein:

```
mmcli -i 0 --puk=<PUK-Code> --pin=<PIN-Code>
```
3. Aktivieren Sie die Option **Mit Systemrechten ausführen**.
4. Klicken Sie auf **Ausführen**.

5.6.7. Optionen für alle Netzwerkprofile

Option	Beschreibung						
Name	Name für das Netzwerk-Profil						
Automatisch starten	(nicht für LAN)						
Internet-Verbindungstest ¹	<p>Das System kann bei jedem Verbindungsaufbau testen, ob über das aktuelle Netzwerk-Profil (LAN und WLAN) eine Verbindung zu Adressen im Internet aufgebaut werden kann. Wenn eine Verbindung ins Internet nicht möglich ist, wird auf die Existenz eines Captive Portal geprüft und ggf. auf dieses umgeleitet.</p> <hr/> <table><tr><td>Auto (Standard)</td><td>Der automatische Verbindungstest wird nur für WLAN-Profile durchgeführt, und nur dann, wenn kein zentraler System-Proxy definiert ist.</td></tr><tr><td>An</td><td>Für LAN- und WLAN-Profile wird ein automatischer Verbindungstest durchgeführt.</td></tr><tr><td>Aus</td><td>Es wird kein automatischer Verbindungstest durchgeführt. Das Gerät zeigt im Browser keine Inhalte an und versucht nicht, sich zu externen Diensten oder Webseiten zu verbinden.</td></tr></table> <hr/>	Auto (Standard)	Der automatische Verbindungstest wird nur für WLAN-Profile durchgeführt, und nur dann, wenn kein zentraler System-Proxy definiert ist.	An	Für LAN- und WLAN-Profile wird ein automatischer Verbindungstest durchgeführt.	Aus	Es wird kein automatischer Verbindungstest durchgeführt. Das Gerät zeigt im Browser keine Inhalte an und versucht nicht, sich zu externen Diensten oder Webseiten zu verbinden.
Auto (Standard)	Der automatische Verbindungstest wird nur für WLAN-Profile durchgeführt, und nur dann, wenn kein zentraler System-Proxy definiert ist.						
An	Für LAN- und WLAN-Profile wird ein automatischer Verbindungstest durchgeführt.						
Aus	Es wird kein automatischer Verbindungstest durchgeführt. Das Gerät zeigt im Browser keine Inhalte an und versucht nicht, sich zu externen Diensten oder Webseiten zu verbinden.						

¹ab Scout Enterprise Management Suite 15.9

5.6.8. Proxy-Konfiguration

Für jedes Netzwerk-Profil können Sie einen Proxy-Server definieren, den die Web-Clients oder Browser verwenden sollen. Der Proxy-Server kann manuell oder automatisch konfiguriert werden.

Wenn Sie den Proxy-Server in der Geräte-Konfiguration zentral definieren, kann in allen Anwendungsdefinitionen (Browser) darauf zugegriffen werden. Dieser zentrale **System-Proxy**¹ enthält die Proxy-Einstellung. Diese kann sich auf eine feste Server-Adresse beziehen, automatisch bestimmt werden oder auch **Kein Proxy** sein.

Mit einer automatischen WPAD-Konfiguration können dann beispielsweise alle Web-Clients einer Organisation komfortabel auf den oder die gleichen Proxy-Server konfiguriert werden.

In den Netzwerk-Profilen stehen unten beschriebene Optionen für den **System-Proxy** zur Verfügung.

- Scout Enterprise-Konsole: **Netzwerk > Erweitert**
- eLux RP 6: **Netzwerk-Konfiguration > Erweitert > Proxy verwenden > Proxy-Einstellungen**

Option	Beschreibung
Kein Proxy	Keinen Proxy-Server verwenden
Manuell (Proxy:Port)	<p>Festen Proxy-Server mit Portnummer festlegen</p> <p>Beispiel: <code>proxy.sampletec-01.com:3800</code></p> <p>Um Ziele zu definieren, auf die nicht per Proxy zugegriffen werden soll, geben Sie die relevanten Netzwerk-Adressen durch Semikolon getrennt in die Proxy-Ausnahmeliste ein.</p>
Auto (URL)	<p>Proxy-Auto-Config (PAC): Bestimmt für jede URL den passenden Proxy</p> <p>Beispiele:</p> <p><code>http://proxy.sampletec-01.com/proxy.pac</code></p> <p><code>http://wpad.sampletec-01.com/wpad.dat</code></p>
Passthrough-Anmeldung für Proxy (bei AD-Benutzer-Authentifizierung) ²	<p>Wenn ein zentraler System-Proxy mit AD-Authentifizierung konfiguriert ist, werden die AD-Anmeldedaten zur Authentifizierung verwendet.</p> <p>Die Proxy-Authentifizierung kann notwendig sein, wenn Sie Browser content redirection unter Citrix einsetzen.</p>
Proxy-Benutzername ³	Benutzername zur Authentifizierung an System-Proxy
Proxy-Kennwort ⁴	Kennwort zur Authentifizierung an System-Proxy

¹ab Scout Enterprise Management Suite 15.5

²ab Scout Enterprise Management Suite 15.8 und eLux RP 6.7

³ab Scout Enterprise Management Suite 15.8 und eLux RP 6.7

⁴ab Scout Enterprise Management Suite 15.8 und eLux RP 6.7



Hinweis

Wenn Sie eine Browser-Anwendung definieren, steht die Proxy-Einstellung standardmäßig auf `System-Proxy` verwenden. Damit ist die im jeweiligen Netzwerk-Profil definierte Proxy-Einstellung aktiv. Für weitere Informationen siehe [Browser-Anwendung definieren](#).

5.6.9. Internet Protocol Version 6 (IPv6)

Neben der voll umfänglichen Unterstützung des Internet Protocol Version 4 (**IPv4**) ist die Verwendung von **IPv6** für lokale Anwendungen inklusive automatischer Netzwerk-Konfiguration (DHCP, DNS, NTP) standardmäßig aktiv.¹

- Um IPv6 zu deaktivieren, definieren Sie in der Scout Enterprise-Konsole für die relevanten Clients folgenden Erweiterten Dateieintrag:

Datei	/setup/terminal.ini
Abschnitt	Network
Eintrag	DisableIPv6
Wert	true (default = false)

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

5.6.10. Firewall für eLux-Geräte

– ab eLux RP 6.8 –

Wenn Sie Ihre eLux-Geräte durch eine Firewall absichern möchten, beispielsweise um genau eine weitere Verbindung neben der Verbindung zum Scout Enterprise-Server zuzulassen, können Sie mit Hilfe des eLux Firewall-Paketes entsprechende Regeln definieren.

Dabei kommen standardmäßig **nftables** zum Einsatz; alternativ kann auch die **iptables**-Syntax verwendet werden.

Sobald das eLux-Paket **Firewall support** installiert ist, werden die Firewall-Regeln beim Systemstart angewendet. Standardmäßig dürfen dann nur Datenpakete passieren, die für die Kommunikation zum Scout Enterprise-Server erforderlich sind. Um weitere Verbindungen zu erlauben, definieren Sie Regeln, die in einer Datei zu den Geräten übertragen werden.

Wenn das **Firewall support**-Paket, aber keine Regeln am Gerät vorhanden sind, startet die Firewall nur dann, wenn zusätzlich das Feature-Paket **Strict firewall policy** installiert ist. Dieses erlaubt ausschließlich die Kommunikation zwischen dem Scout Enterprise-Server und dem Gerät über das Management-Protokoll (Port 22125).

¹ab eLux RP 6.6

Firewall-Regeln konfigurieren (nftables)



Hinweis

Das eLux-Paket **Firewall support** und die hierin enthaltene Feature-Pakete **eLux firewall plugin** und **firewall nftables programs and libraries** müssen auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Erstellen Sie die Datei `nftables.conf` nach folgendem Muster:

```
table ip filter {
    chain input {
        tcp dport 22 accept
        tcp sport 80 accept
    }
    chain output {
        tcp sport 22 accept
        tcp dport 80 accept
    }
}
```

Im Beispiel werden ausgehende `http`- und eingehende `ssh`-Verbindungen akzeptiert.

2. Übertragen Sie die Datei mit Hilfe der Funktion **Konfigurierte Dateiübertragung** auf die Geräte nach `/setup/firewall/nftables.conf`
Für weitere Informationen siehe [Erweiterte Konfiguration > Dateien](#) im **Scout Enterprise**-Handbuch.

Firewall-Regeln konfigurieren (iptables)



Hinweis

Das eLux-Paket **Firewall support** und die hierin enthaltene Feature-Pakete **eLux firewall plugin** und **Firewall iptables compatibility programs and libraries** müssen auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

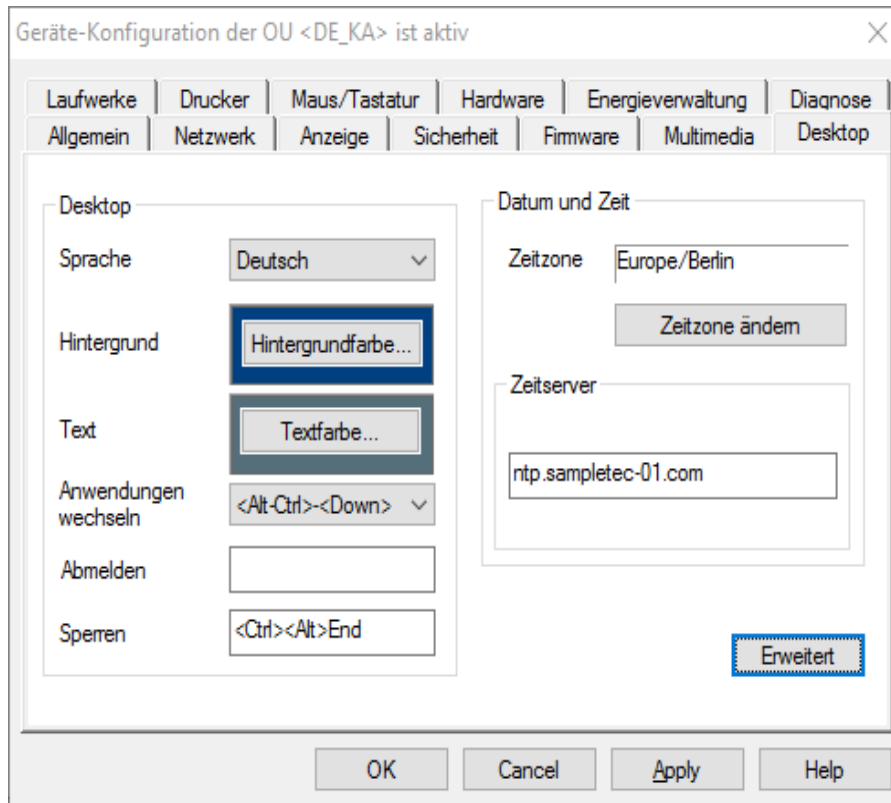
1. Erstellen Sie die Datei `rules.v4` für IPV4 oder `rules.v6` für IPV6. Verwenden Sie die **iptables**-Syntax für die Regeln.
2. Übertragen Sie die Datei mit Hilfe der Funktion **Konfigurierte Dateiübertragung** auf die Geräte nach `/setup/firewall/rules.v4` oder `/setup/firewall/rules.v6`
Für weitere Informationen siehe [Erweiterte Konfiguration > Dateien](#) im **Scout Enterprise**-Handbuch.

Alle Regel-Dateien werden bei der Diagnose-Funktion berücksichtigt und sind in der `System`-Vorlage enthalten.¹

¹ab Scout Enterprise 15.8

5.7. Register Desktop

In **Geräte-Konfiguration > Desktop** passen Sie die Oberfläche von eLux an.



5.7.1. Sprache und Farben konfigurieren

1. Öffnen Sie für das relevante Gerät oder die OU den Dialog **Geräte-Konfiguration > Desktop**.
2. Wählen Sie im Listenfeld **Sprache** die Sprache aus, mit der die Anwendungen gestartet und Bildelemente und Konfiguration dargestellt werden sollen.

Folgende Sprachen werden unterstützt: Deutsch, Englisch Französisch,¹ Spanisch²



Hinweis

Die Sprache bezieht sich auf die Anzeige der Bildelemente, nicht jedoch auf Eingabesprache und Textdienste.

Die Anwendungen müssen kompatibel zur eingestellten Sprache sein, damit sie korrekt ausgeführt werden.

Für eLux RP 5: 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.

¹ab eLux RP 6.9

²ab eLux RP 6.9

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

Für eLux RP 5: Die Hintergrundfarbe wird nur dann aktiv, wenn die Option **Klassischer Desktop** eingeschaltet ist, siehe [Erweiterte Desktop-Einstellungen](#).

4. Klicken Sie auf die Schaltfläche **Textfarbe**, um eine Textfarbe für die Anwendungssymbole auf dem Desktop auszuwählen.¹ Achten Sie auf ausreichenden Kontrast zur Hintergrundfarbe.

Für weitere Konfigurationsoptionen des eLux RP 6-Desktop siehe "eLux RP 6 User Interface" auf Seite 98.

5.7.2. Tastenkombinationen definieren

1. Öffnen Sie den Dialog **Geräte-Konfiguration > Desktop**.
2. Wählen Sie Tastenkombinationen für folgende Aktionen:

Option	Beschreibung	Definition
Anwendungen wechseln	Zwischen offenen Anwendungen oder Sitzungen wechseln Um keinen Konflikt mit der Standard-Tastenkombination ALT+TAB für den Task-Wechsel innerhalb einer Windows Sitzung zu produzieren, ist standardmäßig ALT+STRG+↑ konfiguriert.	Wählen Sie eine Option aus dem Listenfeld.
Abmelden ²	Aktuell angemeldeten Benutzer abmelden (AD-Benutzer) Danach wird der Anmelde-Dialog angezeigt.	Geben Sie die gewünschte Tastenkombination als Freitext an, siehe unten.
Bildschirm sperren ³	Kennwort-geschützten Bildschirmschoner aktivieren (AD-Benutzer) Standard: <Ctrl><Alt>End	Geben Sie die gewünschte Tastenkombination als Freitext an, siehe unten. Andernfalls ist die Standard-Tastenkombination aktiv.

Regeln zur Angabe von Tastenkombinationen

- Tastenkombinationen bestehen aus einer Kombination aus einer oder mehreren Zusatztasten (Modifier) und einer einzelnen normalen Taste
- Als normale Tasten sind erlaubt:

¹ab Scout Enterprise 15.4

²ab Scout Enterprise 15.8 and eLux RP 6.9

³ab Scout Enterprise 15.8 and eLux RP 6.9

Buchstabentasten, Zifferntasten, Funktionstasten, Windows-Logo-Tasten, ESC-Taste, Positionstasten und Tasten des Ziffernblocks wie angegeben

- Tastenkombinationen müssen in folgendem Format angegeben werden:

```
<Zusatztaste><Zusatztaste (optional)><Zusatztaste  
(optional)>weitere Taste
```

Zwischen den Tasten darf kein Leerzeichen oder anderes Zeichen stehen.

- Die Schreibweise der Tastennamen muss der Vorgabe folgen, siehe Beispiele. Um eine vollständige Liste aller erlaubten Tastennamen mit Schreibweise zu erhalten, verwenden Sie folgendes Kommando in einer eLux-Shell:

Zusatztasten (Modifier): `xmodmap -pm`

Normale Tastennamen: `xmodmap -pk`

Beispiele

Option	Beschreibung
<code><Ctrl><Alt>Escape</code>	
<code><Shift><Ctrl>l</code>	
<code><Mod4><Alt>F1</code>	Mod4 entspricht der Windows-Logo-Taste
<code><Ctrl><Mod4><Alt>End</code>	
<code><Mod4>Super_R</code>	Super_R entspricht der rechten Windows-Logo-Taste, wenn sie als Taste verwendet wird
<code><Mod5>KP_End</code>	Mod5 entspricht ALT GR KP_End entspricht der ENDE-Taste auf dem Ziffernblock.



Achtung

Wenn Sie für eLux eine Tastenkombination definieren, die bereits innerhalb einer Anwendung/Sitzung definiert ist, funktioniert diese Tastenkombination nur noch für eLux. Vermeiden Sie Konflikte durch gleiche Tastenkombinationen in unterschiedlichen Umgebungen.

5.7.3. Zeitzone und Zeitserver

In der Geräte-Konfiguration unter **Desktop > Datum und Zeit**¹ können Sie eine Zeitzone wählen und einen Zeitserver angeben.

Option	Beschreibung
Zeitzone	Klicken Sie auf Zeitzone ändern und wählen Sie die gewünschte Zeitzone aus der Liste.

¹ab eLux RP 6.2 **Configuration panel > Datum und Zeit**

Option	Beschreibung
Zeitserver	Geben Sie unter Zeitserver den entsprechenden Servernamen oder die IP-Adresse ein.

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.

Am eLux RP 5-Client klicken Sie auf die Schaltfläche **Zeitabgleich**, um die Zeit mit dem Zeitserver zu synchronisieren.

Weitere Informationen zum Windows Zeit-Service finden Sie in der Microsoft-Dokumentation.

Weitere Informationen zu NTP finden Sie unter <http://www.ntp.org>.

5.7.4. Erweiterte Desktop-Einstellungen

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

Option	Beschreibung	eLux RP 5 1
Interaktiver Desktop	Symbole, die auf dem Desktop angezeigt werden	X
Desktop schreibbar	Anwender dürfen Symbole auf dem Desktop hinzufügen.	X
Klassischer Desktop	Das Modern User Interface wird deaktiviert. Eine auf dem Desktop -Register definierte Hintergrundfarbe wird angezeigt.	X
Sortiere Configuration panel ²	Die Dialoge im Configuration panel werden in alphabetischer Reihenfolge sortiert. (standardmäßig aktiv) ³	
Windowmanager	Animierte Fenster: Der Fensterinhalt wird während des Verschiebens von Fenstern angezeigt. Maximieren/Vollbild auf einzelnen Monitor Bei mehreren angeschlossenen Monitoren können Sie jeder Anwendung (ICA und RDP) einen Monitor zuordnen.	X ⁴

²ab Scout Enterprise 15.5

³ab Scout Enterprise 15.9

⁴Ab eLux RP 6 ist die Funktionalität standardmäßig gegeben.

Option	Beschreibung	eLux RP 5 1
Systemleiste	<p>Anzeige von Symbolen auf der Systemleiste:</p> <p>Zeige Systemsteuerung:² Stellt ein Symbol zum Öffnen der Systemsteuerung auf dem Desktop zur Verfügung. Ab eLux RP 6.4 können die Benutzer die Systemsteuerung (nur Systeminformation) über das Configuration panel > Information anzeigen. Ältere eLux-Clients, die durch Scout Enterprise 15.4 verwaltet werden, benötigen einen Eintrag in der Datei <code>terminal.ini</code>, um das Symbol für die Systemsteuerung auf dem Desktop anzuzeigen (Datei: <code>/setup/terminal.ini</code>, Abschnitt: <code>Layout</code>, Eintrag: <code>ShowControlPanelIcon</code>, Wert: <code>true false</code>).</p> <p>Zeige Desktop-Symbol: Das Symbol minimiert alle geöffneten Fenster und zeigt den Desktop an. (standardmäßig aktiv)</p> <p>Zeige Live-Informationen:³ Live-Informationen zeigen aktuelle Status-Informationen, beispielsweise über USB-Geräte, ab eLux RP 6.8 über rechte Maustaste (standardmäßig aktiv)</p> <p>Zeige Config panel-Symbol:⁴ Über das Config panel-Symbol wird die Geräte-Konfiguration (Configuration panel) geöffnet. (standardmäßig aktiv)</p>	



Achtung

Nur wenn das Configuration panel angezeigt wird, kann der Administrator lokal am Gerät die Konfiguration mit dem Geräte-Kennwort entsperren.

²nur Scout Enterprise 15.2 und 15.3

³ab Scout Enterprise 15.7 und eLux RP 6.7

⁴ab Scout Enterprise 15.4

Quick Config ¹	<p>Schneller Einstieg in Config Panel-Dialoge über die Systemleiste:²</p> <p>Lautstärke: Lautstärkenregelung für Ein-/Ausgabegeräte</p> <p>Tastatur: Tastatursprache und Tastengeschwindigkeit³</p> <p>Anzeige: Bildschirm-Einstellungen</p> <p>Peripherie: Einstellungen für USB-Geräte und COM-Ports</p> <p>Netzwerk: Netzwerk-Info und -Konfiguration, Trennen/Verbinden</p> <p>Geräte-Information: Informationen über das Gerät</p> <p>Datum und Zeit: Datum- und Zeit-Einstellungen</p>
Hintergrundbild (nur Scout Enterprise)	<p>Desktop-Hintergrundbild (Falls weitere definiert: nur für den Primär-Monitor/nach AD-Anmeldung⁴)</p> <p>Wählen Sie eine Grafik-Datei über die Schaltfläche Laden aus dem Dateisystem. Die Datei wird in die Scout Enterprise-Datenbank importiert.</p> <ul style="list-style-type: none"> Folgende Dateiformate werden unterstützt: .svg, .png, .jpg⁵ Maximale Dateigröße 500 MB <p>Mit der Schaltfläche Löschen löschen Sie das Hintergrundbild wieder aus der Datenbank.</p> <p>Alternativ zu einer Datei im Dateisystem geben Sie mit URL setzen eine Web-Adresse an, über die Sie Bilder laden.⁶</p>
Hintergrundbild AD ⁷	Hintergrundbild bis zur AD-Anmeldung (Primär-Monitor)
Zusatzbild	Hintergrundbild nach AD-Anmeldung (Sekundär- und weitere Monitore)
Zusatzbild AD	Hintergrundbild bis zur AD-Anmeldung (Sekundär- und weitere Monitore)
(nur Scout Enterprise)	



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.

¹für eLux RP 5 und ab eLux RP 6.8

²in eLux RP 5 öffnet ein Konfigurations-Dialog auf der Systemleiste

³für eLux RP 5 auch Maus-Einstellungen

⁴ab Scout Enterprise 15.8

⁵kann in der Vorschau nicht angezeigt werden

⁶ab Scout Enterprise 15.8

⁷ab Scout Enterprise 15.8

Autostart	Die Systemsteuerung wird beim Systemstart nach der angegebenen Verzögerung in Sekunden aufgerufen.	X
Arbeitsflächen	Anzahl der Desktops	X

5.7.5. eLux RP 5 Modern User Interface

– nur für eLux RP 5 –



Hinweis

Das Modern UI wird ab eLux RP 6 durch eine neue Oberfläche abgelöst.

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

eLux RP Version 4.8.0 oder höher



Deaktivieren Sie in der Geräte-Konfiguration 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 relevante OU die Scout Enterprise-Funktion **Erweiterte Dateieinträge**, um die Client-Datei `/setup/terminal.ini` im Abschnitt `Layout` anzupassen. 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	<i>Name und Pfad der Grafikdatei</i>	<i>eLux-Logo</i>	Ersetzt das eLux-Logo in der oberen linken Ecke durch die angegebene Grafikdatei. Beispiel: <code>setup/public/myPic.png</code>



Hinweis

Die Grafikdatei muss für die Dateiübertragung konfiguriert sein. Für weitere Informationen, siehe [Erweiterte Geräte-Konfiguration > Dateien](#).

DesktopTextColor	<code>#<rgb></code>	<code>#ffffff</code>	Textfarbe für Anwendungssymbole
------------------	---------------------------	----------------------	---------------------------------

DesktopBackgroundColorMenu	#<rgb>	#000000	Hintergrundfarbe der Menüs
----------------------------	--------	---------	----------------------------

- Um ein Hintergrundbild im Modern User Interface anzuzeigen, konfigurieren Sie die relevante Grafikdatei in der Geräte-Konfiguration. Für weitere Informationen siehe [Erweiterte Desktop-Einstellungen](#).



Hinweis

Das Modern User Interface unterstützt die Nutzung mehrerer Monitore, wenn alle Monitore in derselben Auflösung betrieben werden.

Für weitere Informationen zum Modern User Interface siehe [Oberfläche](#) im eLux-Handbuch.

5.7.6. eLux RP 6 User Interface



Voraussetzung

eLux RP Version 6.0 oder höher

eLux RP 6-Clients kommen mit einer neuen Desktop-Oberfläche, die über eine persönliche Desktop-Ansicht verfügt und an Ihre Bedürfnisse angepasst werden kann. Für weitere Informationen siehe [eLux RP 6 User Interface](#) im eLux-Handbuch.

Layout des eLux RP 6 User Interface anpassen

- Verwenden Sie für die relevante OU die Scout Enterprise-Funktion [Erweiterte Dateieinträge](#), um die Client-Datei `/setup/terminal.ini` im Abschnitt `Layout` anzupassen. Fügen Sie folgende neue Einträge hinzu und geben Sie die gewünschten Werte an:

Eintrag	Wertebereich	Beschreibung
DesktopLogo	<i>Name und Pfad der Grafikdatei</i> none	Option 1 ersetzt das eLux-Logo in der unteren rechten Ecke durch die angegebene Grafikdatei. Beispiel: <code>setup/public/myPic.png</code> Option 2 entfernt das eLux -Logo ersatzlos. ¹



Hinweis

Um eine eigene Grafikdatei als Logo anzuzeigen, muss die Grafikdatei zum Client übertragen werden. Für weitere Informationen, siehe [Konfigurierte Dateiübertragung](#).

DesktopTextColor	#<rgb>	Textfarbe für Anwendungssymbole
------------------	--------	---------------------------------

¹ab eLux RP 6.5

DesktopHighlightedTextColor	#<rgb>	Textfarbe für Anwendungssymbole, wenn der Mauszeiger darauf zeigt
DesktopTitleTextColor	#<rgb>	Titelfarbe eines Ordners/Registers (All Applications, StoreFront Store-Name)
DesktopSearchTextColor	#<rgb>	Textfarbe im Suchfeld
DesktopSearchBackgroundColor	#<rgb>	Hintergrundfarbe im Suchfeld
DesktopSearchIconColor	#<rgb>	Farbe des Lupen-Symbols (Suche)
DesktopSortIconColor	#<rgb>	Farbe des Sortieren-Symbols (A-Z)

- Um ein Hintergrundbild anzuzeigen, konfigurieren Sie die relevante Grafikdatei in den **Erweiterten Desktop-Einstellungen** der Geräte-Konfiguration. Für weitere Informationen siehe [Erweiterte Desktop-Einstellungen](#).



Hinweis

Das Hintergrundbild ersetzt die auf dem Register **Desktop** definierte Hintergrundfarbe.

- Um eine feste Hintergrundfarbe für den Desktop festzulegen, verwenden Sie die Option **Hintergrund** auf der Registerkarte **Desktop**.

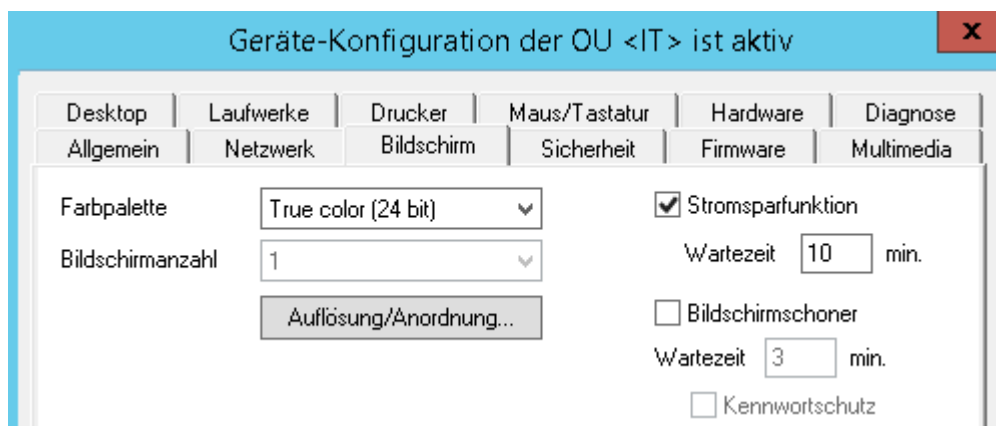
Wenn Sie einen Hintergrund mit Farbverlauf einstellen möchten, verwenden Sie die RGB-Werte R 102, G 138, B 185.

- Um die Position der Systemleiste zu konfigurieren,¹ definieren Sie folgenden Eintrag in der Datei `/setup/terminal.ini` im Abschnitt `Layout`:

Eintrag	Wertebereich	Beschreibung
SystembarPosition	0 1	0: unterer Bildschirmrand 1: oberer Bildschirmrand

¹ab eLux RP 6.8

5.8. Register Anzeige

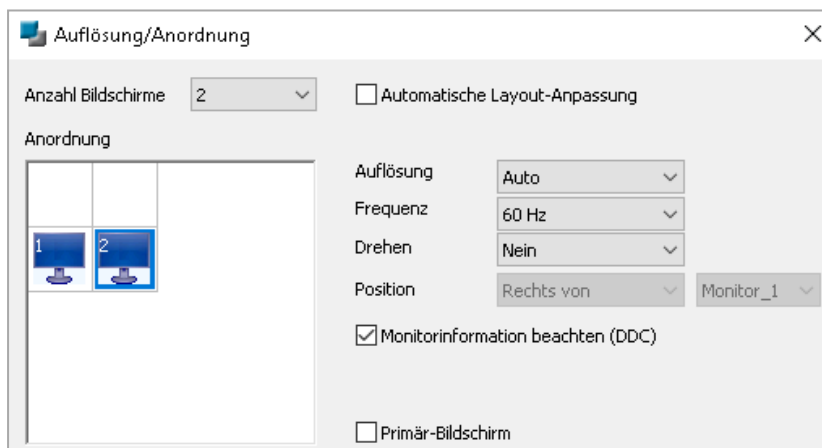


Hinweis

Die Energiesparfunktionen befinden sich ab Scout Enterprise Management Suite 15.3 im Register **Energieverwaltung**.

5.8.1. Anzeige-Einstellungen

In **Geräte-Konfiguration > Anzeige** können Sie die Farbtiefe festlegen und einen Bildschirmschoner definieren. Für weitere Grundeinstellungen verwenden Sie den Dialog **Auflösung/Anordnung**.



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 Bildschirmen an den Thin Client besteht keine Gewährleistung für den Betrieb der Thin Clients, da diese Konstellationen kein Bestandteil funktionaler Abnahmetests sind.

Anzeige konfigurieren

1. Markieren Sie im Dialog **Auflösung/Anordnung** ein blaues Bildschirm-Symbol.
2. Legen Sie für den markierten Bildschirm 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 Bildschirm unterstützten Werte abrufen und berücksichtigt, aktivieren Sie für den markierten Bildschirm die Option **Monitorinformation beachten (DDC)**.
Wenn Sie die Option deaktivieren, wird das Feld **Anschlusstyp** aktiv.
4. Um den markierten Bildschirm als Primär-Bildschirm zu definieren, aktivieren Sie die Option **Primär-Bildschirm**.
5. Bestätigen Sie mit **OK** und **Übernehmen**.



Achtung

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

5.8.2. Multimonitorbetrieb

Bis zu acht Bildschirme ¹ können angeordnet und konfiguriert werden.

Mehrere Bildschirme konfigurieren

1. Klicken Sie in **Geräte-Konfiguration > Anzeige** auf die Schaltfläche **Auflösung/Anordnung...**, um den gleichnamigen Dialog zu öffnen.

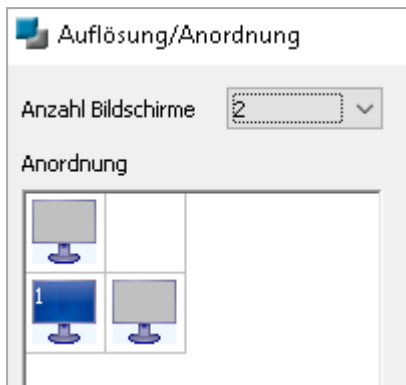
*Im Feld **Bildschirmanzahl** ist standardmäßig 1 Bildschirm angegeben. Dieser Bildschirm wird im Feld **unterhalb** als blaues Bildschirm-Symbol mit einer 1 dargestellt. Standardmäßig ist der erste Bildschirm als Primär-Bildschirm definiert (siehe Option im unteren Bereich).*

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

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

¹ab Scout Enterprise Management Suite 14.9, vorher maximal vier Bildschirme

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



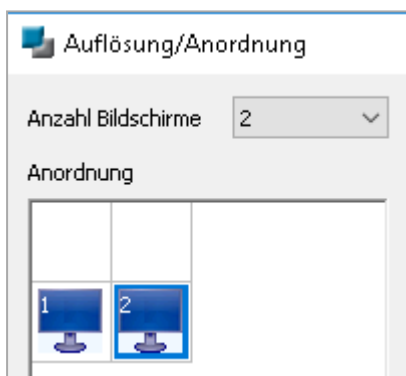
3. Doppelklicken Sie auf das graue Bildschirm-Symbol, das die Position Ihres zweiten Bildschirms bezeichnet.

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



Hinweis

Alternativ klicken Sie mit der rechten Maustaste auf eine Monitor-Position, um ihr einen Monitor zuzuordnen.



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

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

5. Um das Layout automatisch anzupassen, nachdem einer der Bildschirme entfernt wird, aktivieren Sie die Option **Automatische Layout-Anpassung**.¹

Wenn die Option nicht aktiv ist, wird das aktuelle Layout unabhängig von der tatsächlichen Situation beibehalten.

¹ab Scout Enterprise Management Suite 15.9



Hinweis

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

Eine Fünf-Bildschirm-Konfiguration wird von folgenden Geräten unterstützt: Fujitsu FUTRO S940 und Fujitsu FUTRO S9010.

Anordnung aller Bildschirme frei definieren

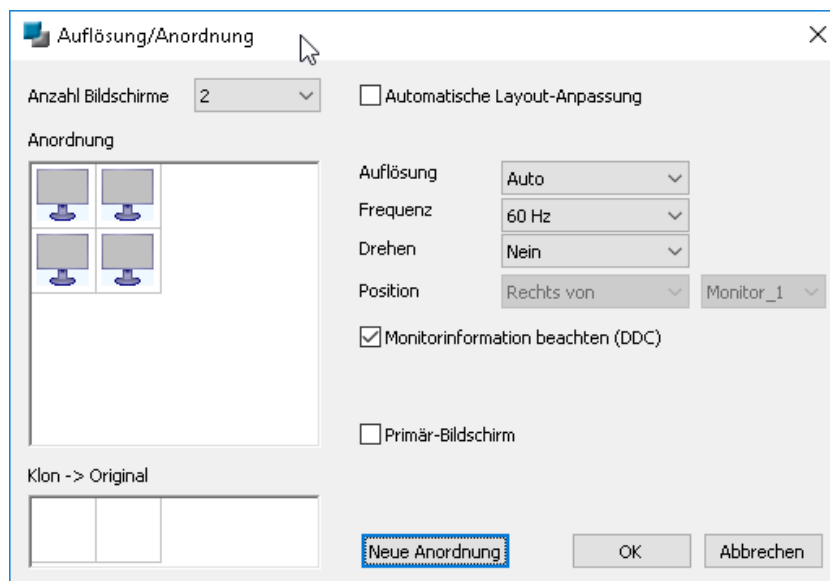
Wenn Sie die Position des ersten Bildschirms selbst definieren möchten, verwenden Sie ein neues Layout.

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

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

2. Klicken Sie auf **Neues Layout**.¹

Für die gewählte Bildschirmzahl werden alle möglichen Bildschirm-Positionen als graue Bildschirm-Symbole angezeigt:



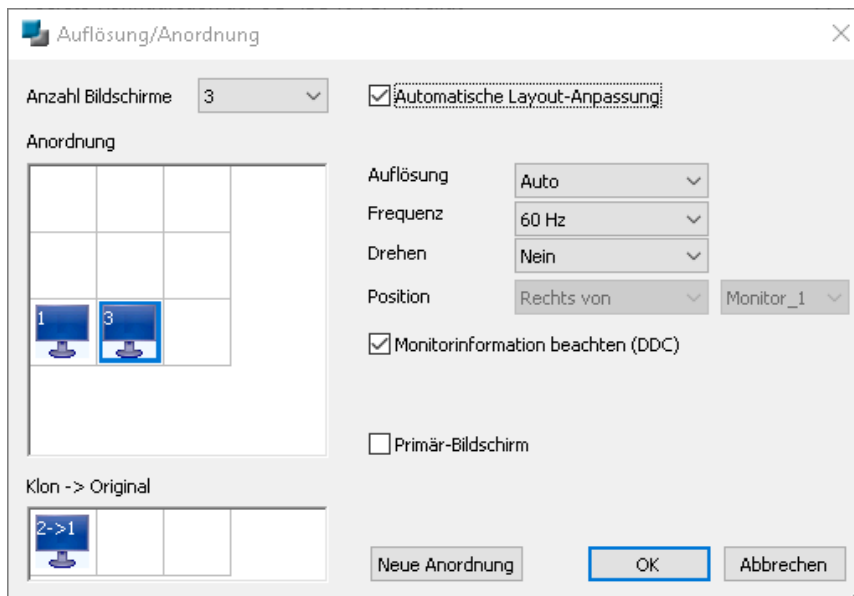
3. Doppelklicken Sie auf die relevante Bildschirm-Position für den ersten Bildschirm. Doppelklicken Sie anschließend auf die relevanten Bildschirm-Positionen für die weiteren Bildschirme.

¹bis Scout Enterprise Management Suite 14.9: Klicken Sie mit der rechten Maustaste in den weißen Bereich neben den Bildschirm-Symbolen und wählen Sie im Kontextmenü **Neues Layout**.

Bildschirme klonen (Mehrschirmbetrieb)

Wenn mehr als ein Bildschirm angegeben ist, konfiguriert das System die Bildschirme standardmäßig zur Nutzung eines erweiterten Desktops (zusammenhängende Arbeitsoberfläche über alle Bildschirme). Alternativ können Sie für einen Bildschirm nach der Definition den Mehrschirmbetrieb oder Klon-Modus (gleiche Anzeige auf mehreren Bildschirmen) aktivieren:

- ▶ Klicken Sie mit der rechten Maustaste auf das zuletzt definierte blaue Bildschirm-Symbol und wählen Sie im Kontextmenü **Klon von x**.



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

5.8.3. Bildschirmschoner

Bildschirmschoner konfigurieren

1. Wählen Sie unter **Anzeige > Einstellungen für Bildschirmschoner**, ob Sie einen schwarzen Bildschirm, einen bestimmten Bildschirmschoner oder mehrere Bildschirmschoner verwenden möchten.
2. Markieren Sie abhängig von der gewählten Option einen oder mehrere Bildschirmschoner aus der Liste. Um mehrere Einträge zu markieren, drücken Sie die UMSCHALT- oder STRG-Taste.



Hinweis

Der Listeneintrag **HTML** erlaubt die Konfiguration einer Webseite.¹

3. Konfigurieren Sie jeden Bildschirmschoner mit Hilfe der Einstellungen auf der rechten Seite.

Bildschirmschoner aktivieren

Bis Scout Enterprise Management Suite 15.2 und eLux RP 6.2:

- ▶ Aktivieren Sie im Register **Bildschirm** die Option **Bildschirmschoner**. Geben Sie im Feld **Wartezeit** die Wartezeit in Minuten an, bevor sich der Bildschirmschoner einschalten soll.

Ab Scout Enterprise Management Suite 15.3 und eLux RP 6.3:

- ▶ Konfigurieren Sie im Register **Energieverwaltung** Ihre Profile mit der Option **Bildschirmschoner aktivieren nach** und geben Sie eine Wartezeit in Minuten an.

Bildschirmsperre am Gerät einschalten

Wenn der Bildschirmschoner aktiviert ist, kann der eLux-Benutzer die Bildschirmsperre vor der konfigurierten Wartezeit mit einer Tastenkombination einschalten:

- ▶ Drücken Sie STRG+ALT+ENDE

Kennwortschutz für Bildschirmschoner



Hinweis

Wenn die Benutzer-Authentifizierung eingeschaltet ist, ist der Kennwortschutz automatisch aktiv und kann nicht ausgeschaltet werden.²

Bis Scout Enterprise Management Suite 15.2 und eLux RP 6.2:

- ▶ Aktivieren Sie im Register **Bildschirm** die Option **Kennwortschutz**. Der Kennwortschutz erfordert, dass die **Benutzer-Authentifizierung** eingeschaltet ist.

¹ab Scout Enterprise 15.8

²ab Scout Enterprise Management Suite 15.3 und eLux RP 6.3

Das Kennwort für den Bildschirmschoner ist mit dem Wert aus `$ELUXPASSWORD` vorbelegt. Für weitere Informationen siehe [Anwendungsmöglichkeiten für Benutzervariablen](#).

Der Bildschirmschoner wird nach der definierten Zeitspanne aktiv und das System ist gesperrt. Durch Drücken einer Taste oder Mausbewegung wird der Dialog zum Entsperren angezeigt. Dieser Dialog bietet den Benutzern folgende Optionen:

Option	Schaltfläche	Beschreibung
Der angemeldete Benutzer entsperrt den Bildschirm durch Eingabe seines Kennwortes / Smartcard	Entsperren	Standardfall
Eine andere Person hinterlässt dem angemeldeten Benutzer eine Nachricht	Nachricht	<p>Der Bildschirm bleibt gesperrt. Der angemeldete Benutzer erhält nach dem Entsperren des Bildschirms eine Benachrichtigung mit der hinterlassenen Nachricht.</p> <p>Diese Funktion ist standardmäßig aktiv und kann durch folgenden Erweiterten Dateieintrag deaktiviert werden:¹ Datei: <code>/setup/terminal.ini</code>, Abschnitt: <code>xscreensaver_dialog</code>, Eintrag: <code>MessageEnabled</code>, Wert: <code>false</code></p>
Ein anderer Benutzer authentifiziert sich, um den vorherigen Benutzer abzumelden (und sich anzumelden), das Gerät neu zu starten oder herunterzufahren. ²	Abmelden	<p>Sinnvoll, wenn Geräte von mehreren Benutzern verwendet werden:</p> <p>Geräte, die in angemeldetem Zustand verlassen wurden und daher blockiert sind, können wieder genutzt werden.</p> <p>Sobald sich der neue Benutzer authentifiziert hat, werden die Schaltflächen Neu starten, Herunterfahren und Abmelden aktiv. In jedem Fall wird der angemeldete Benutzer abgemeldet.</p> <p>Diese Funktion ist standardmäßig deaktiviert und kann durch folgenden Erweiterten Dateieintrag aktiviert werden: Datei: <code>/setup/terminal.ini</code>, Abschnitt: <code>xscreensaver_dialog</code>, Eintrag: <code>ShowSysCommandButtons</code>, Wert: <code>true</code></p>

¹ab eLux RP 6.8

²ab eLux RP 6.8



Achtung

Datenverlust kann entstehen, wenn die Option **Abmelden** mit anschließendem Neustart, Herunterfahren oder Abmelden durchgeführt wird. Der angemeldete Benutzer wird ungeachtet eventuell ungespeicherter Dokumente oder Daten abgemeldet.

Download von Grafikdateien für Bildschirmschoner

– ab eLux RP 6.5 –

Der Scout Enterprise-Administrator kann optional den direkten Download von Grafikdateien zum Gerät in das Bilderverzeichnis des Bildschirmschoners konfigurieren. Dazu wird das Tool **FileFetch** eingesetzt, das via **wget** die Grafikdateien herunterlädt.



Voraussetzung

- Das eLux-Paket **FileFetch** muss auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.
- Im angegebenen Verzeichnis des Webserver befinden sich Grafikdateien vom Typ `.gif` oder `.jpg` oder `.png`.
Der Dateiname der Grafikdateien ist numerisch. Beispiele: `0001.jpg`, `0002.jpg`, `0003.png`, `0004.gif`

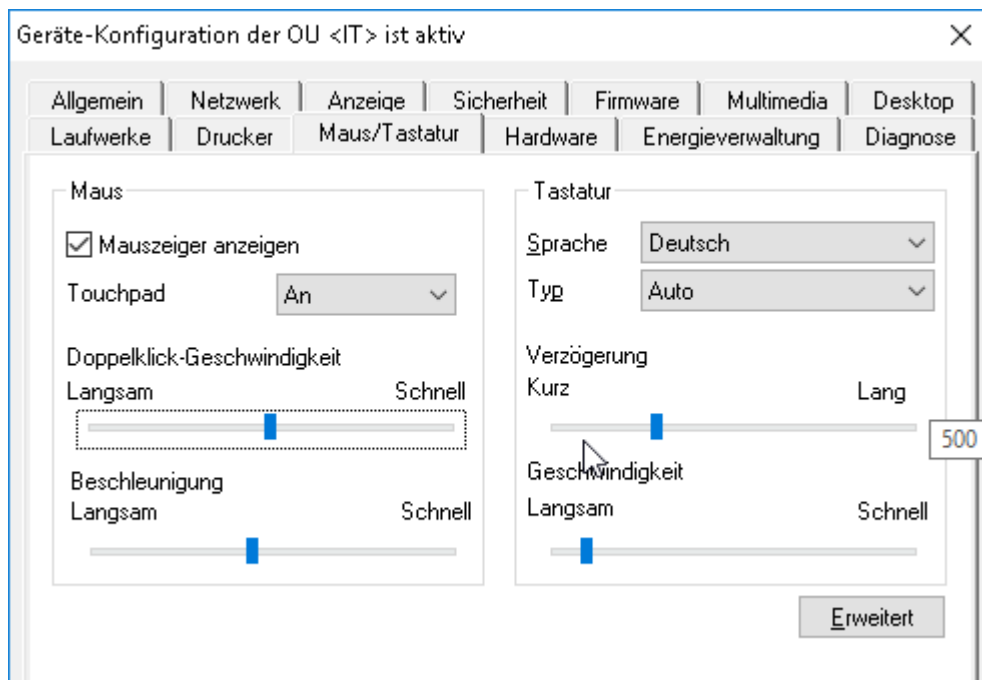
- ▶ Konfigurieren Sie für die relevanten Clients den Web-Server und das Verzeichnis der Grafikdateien auf dem Webserver. Verwenden Sie hierzu die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole:

Datei	/setup/terminal.ini
Abschnitt	FileFetch
Eintrag	URL
Wert	URL des Webserver mit Verzeichnis Beispiel: <code>http://webserver.mydomain.de/eluxng/pictures</code>

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

*Das **FileFetch** Tool prüft bei jedem Neustart des Thin Clients, ob neue Grafikdateien vom Web-Server heruntergeladen werden müssen.*

5.9. Register Maus/Tastatur



5.9.1. Maus konfigurieren

- Bearbeiten Sie im Register **Maus/Tastatur** unter **Maus** folgende Felder:

Option	Beschreibung
Mauszeiger anzeigen	Standardmäßig wird der Mauszeiger angezeigt. Der Maustyp wird automatisch erkannt. ¹
Touchpad ² (für mobile Geräte)	An Aktiviert das Touchpad (Standard) Aus Schaltet das Touchpad aus Auto Schaltet das Touchpad aus, sobald eine Maus eingesteckt wird
Doppelklick-Geschwindigkeit	Die Doppelklick-Geschwindigkeit definiert den Zeitintervall zwischen zwei Klicks, die als Doppelklick gewertet werden sollen.
Beschleunigung	Je schneller der Mauszeiger ist, desto geschmeidiger sind die Bewegungen.

¹ab Scout Enterprise Management Suite Version 15.0

²ab Scout Enterprise Management Suite Version 15.9 und eLux RP 6.9.0

5.9.2. Tastatur konfigurieren

► Bearbeiten Sie im Register **Maus/Tastatur** unter **Tastatur** folgende Felder:

Option	Beschreibung
Sprache	Tastatursprache (Layout)
Typ	Wenn der Eintrag auf <code>Auto</code> steht (Standard), wird die Tastatur automatisch vom System erkannt.
Verzögerung	Die Verzögerung steuert, wie lange eine Taste gedrückt gehalten werden muss, bis ein Zeichen wiederholt wird.
Geschwindigkeit	Die Geschwindigkeit steuert, wie schnell ein Zeichen wiederholt wird, wenn eine Taste gedrückt gehalten wird.

5.9.3. Erweiterte Maus- und Tastaturkonfiguration

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

Option	Beschreibung						
Linkshändig	Vertauscht die Funktion der Maustasten.						
Tot-Tasten	<p>Sogenannte Deadkey-Tasten oder Tot-Tasten lösen erst in Kombination mit einer zweiten Taste die Anzeige eines Zeichens aus. Beispielsweise funktionieren Akzent-Tasten als Tot-Tasten und ermöglichen so die korrekte Eingabe von Buchstaben mit Akzenten (` + A => à).</p> <p>Nicht alle Hardwareplattformen und Anwendungen unterstützen diese Option.</p>						
Konsolenwechsel	Der Benutzer kann per Tastenkombination 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 .						
Erweitertes Tastaturlayout	Aktiviert Multimedia- und andere Tasten mit Sonderfunktionen auf der Tastatur						
Num-Taste	<table><tr><td>An</td><td>Schaltet den Nummernblock der Client-Tastatur beim Gerätestart ein und ermöglicht das Eingeben von Zahlen über den Nummernblock (Standard)</td></tr><tr><td>Aus</td><td>Schaltet den Nummernblock der Client-Tastatur beim Gerätestart aus</td></tr><tr><td>Auto¹</td><td>Schaltet den Nummernblock bei mobilen Geräten aus und bei anderen Geräten ein</td></tr></table>	An	Schaltet den Nummernblock der Client-Tastatur beim Gerätestart ein und ermöglicht das Eingeben von Zahlen über den Nummernblock (Standard)	Aus	Schaltet den Nummernblock der Client-Tastatur beim Gerätestart aus	Auto ¹	Schaltet den Nummernblock bei mobilen Geräten aus und bei anderen Geräten ein
An	Schaltet den Nummernblock der Client-Tastatur beim Gerätestart ein und ermöglicht das Eingeben von Zahlen über den Nummernblock (Standard)						
Aus	Schaltet den Nummernblock der Client-Tastatur beim Gerätestart aus						
Auto ¹	Schaltet den Nummernblock bei mobilen Geräten aus und bei anderen Geräten ein						

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

Die Änderungen werden beim nächsten Systemstart aktiv.

¹ab Scout Enterprise Management Suite 15.3

5.10. Register Firmware

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

The screenshot shows the 'Geräte-Konfiguration der OU <IT> ist aktiv' window with the 'Firmware' tab selected. The window has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: Laufwerke, Drucker, Maus/Tastatur, Hardware, Energieverwaltung, Diagnose, Allgemein, Netzwerk, Bildschirm, Sicherheit, Firmware (selected), Multimedia, and Desktop. The Firmware tab contains the following settings:

- Protokoll: HTTP (dropdown)
- Proxytyp: Statisch (Consumer) (dropdown)
- Server: websrv.sampletec-01.com (text field)
- Provider: 192.168.59.14 (text field)
- Benutzer: (empty text field)
- Kennwort: (password field with dots)
- Pfad: eluxng/___CONTAINER_ (dropdown)
- Image-Datei: IT_630.idf (dropdown)
- URL: http://websrv.sampletec-01.com/eluxng/___CONTAINER_/IT_630.idf
- Auf neue Version beim Start prüfen: ☐
- Bestätigung für Update erforderlich: ☐
- Auf neue Version beim Ausschalten prüfen: ☐
- Buttons: Erinnerung..., Sicherheit..., Elias...

At the bottom of the window are four buttons: OK, Abbrechen, Übernehmen, and Hilfe.

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



Hinweis

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

5.10.1. Firmware-Update konfigurieren



Hinweis

Aus den Feldern **Protokoll**, **Server**, **Pfad** und **Image-Datei** wird eine URL erzeugt, die von den Clients zum Firmware-Update verwendet wird. Die URL wird unterhalb des **Pfad**-Feldes angezeigt.

1. Öffnen Sie in der Scout Enterprise-Konsole für das relevante Gerät oder OU den Dialog **Geräte-Konfiguration > Firmware**. Am eLux RP 6-Client wählen Sie im **Configuration Panel** den Dialog **Firmware**.¹
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)	<p>IP-Adresse und Port (fix 3128) des Proxy-Servers</p> <p>Format: <code>IP-Adresse:Port</code></p> <p>Beispiel: <code>192.168.10.100:3128</code></p> <p>Ab Scout Enterprise Management Suite 15.3 können Sie direkt die Rolle für den statischen Proxy (Provider/Consumer) oder den Eintrag auf <code>Dynamisch</code> setzen.</p>
Benutzer und Kennwort (optional)	Benutzername und Kennwort für den Zugriff auf den eLux-Software-Container des FTP-Servers, wenn erforderlich
Pfad	<p>Verzeichnispfad der eLux Software-Pakete auf dem Web/FTP-Server</p> <p>Verwenden Sie Slashes / als Trennzeichen zwischen den Verzeichnissen.</p> <p>Beispiel: <code>eluxng/UC_RP6_X64</code> entspricht dem IIS-Webserver-Verzeichnis <code>W:\inetpub\wwwroot\eluxng\UC_RP6_X64\</code></p> <p>Wenn Sie ELIAS 18 einsetzen, setzen Sie den bei der ELIAS 18-Installation angegebenen Pfadnamen ein.</p> <p>Beispiel: <code>elias/UC_PR6_X64</code></p> <p>Wenn mehrere eLux-Versionen eingesetzt werden, kann das Container-Verzeichnis durch das Container-Makro parametrisiert werden.</p>

¹Für eLux RP 5: **Systemsteuerung > Firmware**.

Option	Beschreibung
Image-Datei	<p>Name der Imagedefinitions-Datei (IDF) auf dem Webserver, die die Clients für das Firmware-Update verwenden sollen</p> <p>Je nach Berechtigung kann ein IDF-Name eingegeben werden oder das IDF wird aus dem Listenfeld ausgewählt. Für weitere Informationen siehe Auswahl der Imagedefinitions-Datei.</p> <p>Wenn unterschiedliche BIOS-Implementierungen eingesetzt werden (UEFI und non-UEFI), kann im IDF-Namen das Base System-Makro verwendet werden.</p>
Auf neue Version beim Start / Ausschalten prüfen	<p>Der Thin Client prüft automatisch beim Ein- oder Ausschalten, ob Firmware-Updates verfügbar sind.</p> <p>Zusätzlich kann die Funktion Bestätigung für Update erforderlich aktiviert werden, damit der Anwender das Update bei Bedarf verhindern kann.</p> <p>Für weitere Informationen siehe Update automatisch bei Systemstart oder Ausschalten.</p>
Schaltfläche ELIAS...	Das Tool ELIAS wird gestartet und öffnet die im Feld Image-Datei angegebene Imagedefinitions-Datei.
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 .

- Testen Sie die **Firmware**-Einstellungen an einem Client. Klicken Sie dazu auf die Schaltfläche **Update** auf der Systemleiste im erweiterten Command panel (eLux RP 6) oder in der Systemsteuerung unter **Setup > Firmware** (eLux RP 5). Für weitere Informationen siehe [Firmware-Update einspielen](#) im eLux-Handbuch.

Wenn die Parameter korrekt sind, wird eine Verbindung zum Scout Enterprise-Server hergestellt und die Notwendigkeit eines Updates geprüft.

5.10.2. Auswahl der Imagedefinitions-Datei

Imagedefinitionsdateien (IDF) werden auf dem Webserver im eLux-Container bereitgestellt und müssen in der Geräte-Konfiguration für das Firmware-Update der Clients angegeben werden.

In der Geräte-Konfiguration kann der Administrator je nach Objektrechten einen IDF-Namen frei eingeben oder muss ein IDF aus der vordefinierten Liste auswählen.

Die Auswahl der IDFs und der Container-Pfad kann im Vorfeld definiert werden. Für weitere Informationen siehe [Vordefinierte IDFs und Container](#).

Objektrechte für die Felder Image-Datei und Pfad setzen



Voraussetzung

Die Administratorenverwaltung ist eingeschaltet.

1. Wählen Sie für die relevante OU den Kontextmenü-Eintrag **Objektrechte...**
2. Markieren Sie einen Administrator / Administratorengruppe und klicken Sie auf **Objektrechte bearbeiten...**
3. Ändern Sie für **Geräte-Konfiguration > Firmware** den Zugriff für die Objektrechte durch Doppelklick oder Leertaste:

Image-Datei (vordefiniert)	<p>Der Administrator kann ein IDF aus dem Listefeld Image-Datei auf dem Firmware-Register auswählen.</p> <p>Das Listefeld enthält vordefinierte IDF-Dateien (siehe unten). Wenn keine vordefinierten IDFs vorhanden sind, zeigt das Listefeld die zuletzt verwendeten IDFs an.</p>
Image-Datei (benutzerdefiniert)	<p>Der Administrator kann den Namen des gewünschten IDF unabhängig vom Listefeld eingeben.</p> <p>Der Name darf keine Leerzeichen enthalten, Groß-/Kleinschreibung ist zu berücksichtigen und die Dateiendung <code>.idf</code> muss angegeben werden.</p> <p>Beispiel: <code>myImage.idf</code></p>
Pfad (vordefiniert)	<p>Der Administrator kann einen Pfad aus dem Listefeld Pfad auf dem Firmware-Register auswählen.</p> <p>Das Listefeld enthält vordefinierte Pfade (siehe unten). Wenn keine vordefinierten Pfade vorhanden sind, zeigt das Listefeld die zuletzt verwendeten Pfade an.</p>
Pfad (benutzerdefiniert)	<p>Der Administrator kann den Container-Pfad unabhängig vom Listefeld eingeben.</p> <p>Der Pfad muss einem Software-Container auf dem Web-Server entsprechen.</p>

4. Bestätigen Sie mit **OK**.

Für weitere Informationen siehe [Administratorenrechte](#).

IDFs und Container vordefinieren

1. Wählen Sie den Menübefehl **Optionen > Erweiterte Optionen > Vordefinierte IDFs**.

Alle IDF-Dateien werden angezeigt, die in der aktuellen Client-Infrastruktur über alle Clients bisher verwendet wurden.
2. Aktivieren Sie für alle IDFs, die Sie den operativen Administratoren zur Auswahl in der Firmware-

Konfiguration zur Verfügung stellen möchten, die Option **Gültig**.

3. Um neue IDF-Namen hinzuzufügen, die ebenfalls zur Verfügung stehen sollen, klicken Sie auf die Schaltfläche **Hinzufügen** und bearbeiten den neuen Eintrag.
4. Um einen Container-Pfad vorzudefinieren, klicken Sie in der unteren Liste auf **Hinzufügen** und bearbeiten den neuen Eintrag. Lassen Sie die Option **Gültig** aktiv.
5. Bestätigen Sie mit **Übernehmen** und **OK**.

*Alle gültigen IDFs und Container-Pfade stehen in der Geräte-Konfiguration unter **Firmware** im Listenfeld **Image-Datei** zur Verfügung und können von berechtigten Administratoren verwendet werden.*

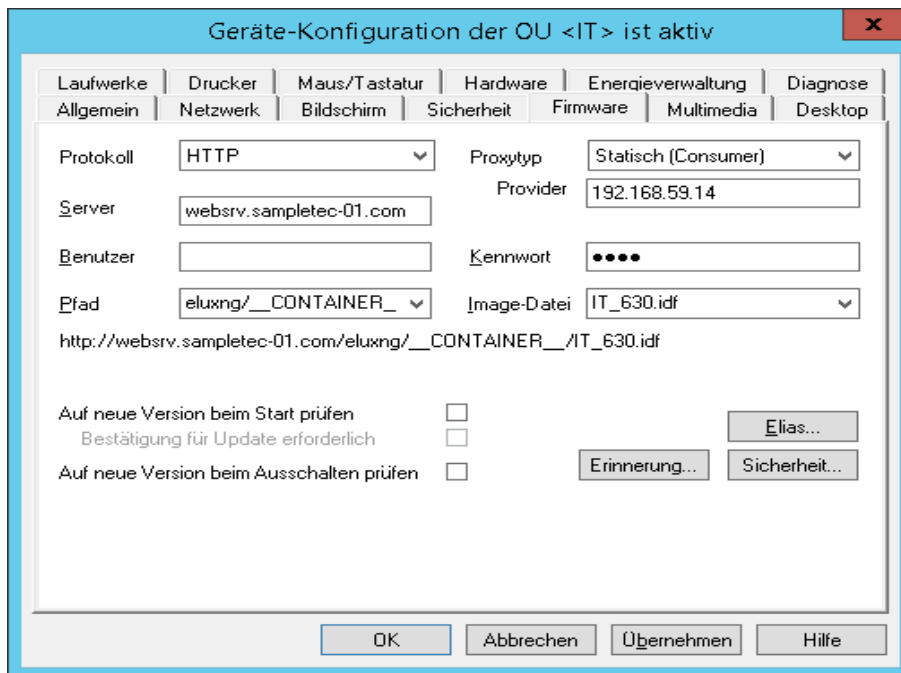


Hinweis

IDFs und Container-Pfade werden systemseitig nicht darauf überprüft, ob sie physikalisch auf dem Webserver vorhanden sind.

5.10.3. Unterschiedliche eLux-Versionen

Standardmäßig wird in einer neu installierten Scout Enterprise-Konsole oder eLux-Systemsteuerung in der Geräte-Konfiguration **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 RP 5 und eLux RP 6 betreiben, müssen die eLux RP 5-Clients auf den `UC_RP5`-Container zugreifen und die eLux RP 6-Clients auf den `UC_RP6_X64`¹-Container. Um alle Clients mit der jeweils richtigen Software zu versorgen, verwenden Sie in der Geräte-Konfiguration **Firmware** > **Pfad** aller Clients das Container-Makro `__CONTAINER__`. Das Container-Makro wird von den Clients entsprechend ihrer installierten eLux-Version entweder nach `UC_RP5` oder nach `UC_RP6_X64` aufgelöst. Damit kann für beide Plattformen ein gleichnamiges IDF verwendet werden, welches zuvor über ELIAS für eLux RP 5 und für eLux RP 6 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 Containernamen auf dem Webserver entsprechen.

¹ab eLux RP 6.3

ELIAS 18-Container

Bei Verwendung von ELIAS 18 können Sie das Container-Makro nutzen, wenn Sie Ihre Container entsprechend benennen:

UC_RP5	eLux RP 5
UC_RP6	eLux RP 6.1 und eLux RP 6.2 (32-Bit)
UC_RP6_X64	eLux RP 6.3 und neuere Versionen (64-Bit)

Für weitere Informationen siehe [Container erstellen](#) im **ELIAS 18**-Handbuch.

Schreibweise des Container-Makronamens

Wenn Sie 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.

5.10.4. Unterschiedliche BIOS-Implementierungen (UEFI)

– Für eLux RP 6.2 und ältere Versionen –



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`).

Ab eLux RP 6.3 wird immer der 64-Bit-Kernel verwendet und das System erkennt automatisch ob es sich um UEFI oder non-UEFI handelt.

Damit Geräte mit unterschiedlichen BIOS-Implementierungen über eine gemeinsame Firmware-Konfiguration aktualisiert werden können, steht das Base System-Makro¹ `__BM__` 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). Geräte mit eLux RP 6.3 oder höher ignorieren das Base System-Makro im Image-Namen.

Firmware-Update mit Base System-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 .Geräte ohne UEFI. Der IDF-Dateiname muss demjenigen für UEFI-Geräte entsprechen, darf jedoch die Zeichenfolge `EFI` nicht enthalten.
Beispiel: `karc.id`

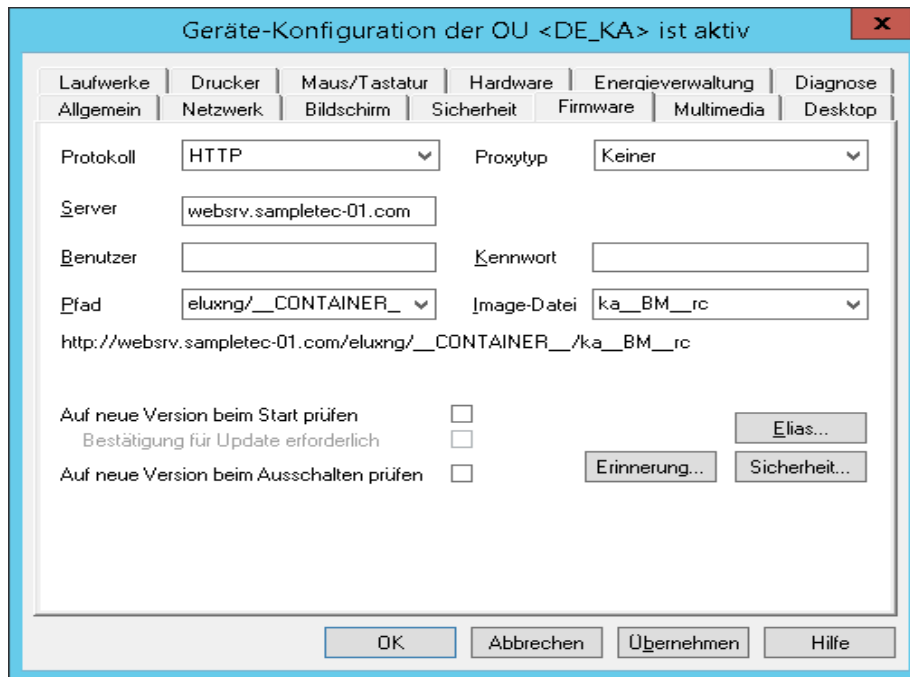


Hinweis

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 **Geräte-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 Base System-Makro ein. Die Dateierweiterung `.idf` und der Rest des Dateinamens müssen erhalten bleiben.

¹früher: BIOS-Makro



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 Base System-Makro entsprechend ihrer BIOS-Implementierung auf (mögliche Werte: `EFI` | `<none>`). Im Beispiel oben werden folgende URLs erzeugt:

UEFI-Geräte (x64)	<code>http://websrv.docu.sampletec.com/eluxng/UC_RP6/kaEFIrc.idf</code>
-------------------	---

Geräte ohne UEFI (x86)	<code>http://websrv.docu.sampletec.com/eluxng/UC_RP6/karc.idf</code>
------------------------	--

Geräte mit eLux RP 6.3 oder höher	<code>http://websrv.docu.sampletec.com/eluxng/UC_RP6/karc.idf</code>
-----------------------------------	--

Das System erkennt automatisch ob es sich um UEFI oder non-UEFI handelt

Besonderheit für HP t630

Der HP t630 kann mit 64 Bit-Kernel auch ohne UEFI genutzt werden.¹ Dazu löst der HP t630 das Makro `__BM__` nach dem Wert `x64` auf. Für das Beispiel oben wird folgende URL erzeugt:

¹ab eLux RP 5.7 und eLux RP 6.2

HP t630 ohne UEFI (x64)	http://webserv.docu.sampletec.com/eluxng/UC_RP6/kax64rc.idf
----------------------------	---



Hinweis

Der HP t630 ist nur für den 64-Bit Linux-Kernel freigegeben, UEFI (x64) oder non-UEFI (x64).

Auswirkungen des Base System-Makro auf Clients mit alter eLux RP-Firmware

Clients mit einem älteren Firmware-Stand als eLux RP .5.3 können das Base System-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 RP 4 oder eLux RP 5-Versionen im Container `UC_RP` oder `UC_RP5` zusätzlich unter einem Dateinamen, der das nicht aufgelöste Base System-Makro enthält.

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

Schreibweise des Base System-Makronamens

Achten Sie auf folgende Schreibweise:

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



Hinweis

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

5.10.5. Firmware-Sicherheit durch Signatur

Die Firmware-Konfiguration in der Scout Enterprise-Konsole oder am Client kann so eingestellt werden, dass der Client vor jedem Update die Signaturen für die Imagedefinitions-Datei (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. Wenn das IDF oder eines der zu installierenden eLux Software-Pakete eine ungültige oder nicht prüfbare Signatur besitzt, schlägt das Update fehl.



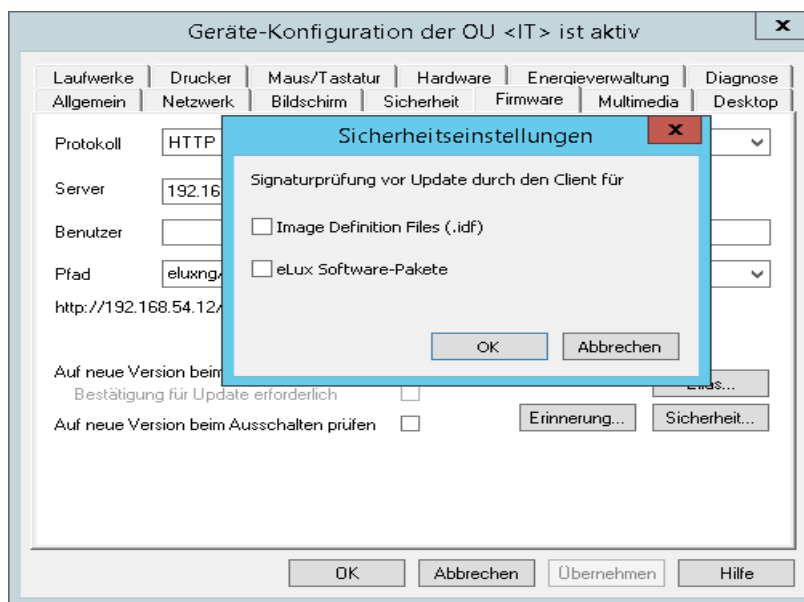
Achtung

Die Signaturprüfung von eLux Software-Paketen erfordert eine Update-Partition auf dem Client. Bei Geräten ohne Update-Partition kann die Signaturprüfung ausschließlich für Imagedefinitions-Dateien (IDF) erfolgen, jedoch nicht für eLux Software-Pakete. Für weitere Informationen zur Update-Partition siehe [eLux-Partitionen](#).

Signaturprüfung vor Update einschalten

1. Klicken Sie in der Scout Enterprise-Konsole in **Geräte-Konfiguration > Firmware** auf die Schaltfläche **Sicherheit...**

Am eLux RP 6-Client wählen Sie **Configuration panel > Firmware > Signaturen überprüfen**.



*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** und **Übernehmen**.



Hinweis

In eLux befinden sich beide Optionen direkt auf dem **Firmware**-Register (eLux RP 5) bzw. **Firmware**-Dialog (eLux RP 6).

*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.*

Zertifikate

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 Enterprise-Funktion **Dateien (Erweiterte Optionen)** oder **Erweiterte Geräte-Konfiguration**¹⁾ konfigurieren. Für die von Unicon bereitgestellten eLux-Pakete werden die erforderlichen Zertifikate bereits mit dem BaseOS zur Verfügung gestellt.

Für weitere Informationen zum Erstellen von IDF-Signaturen siehe [Image signieren](#) im **ELIAS 18-**Handbuch.

¹früher: Erweiterte Einstellungen

5.10.6. 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.

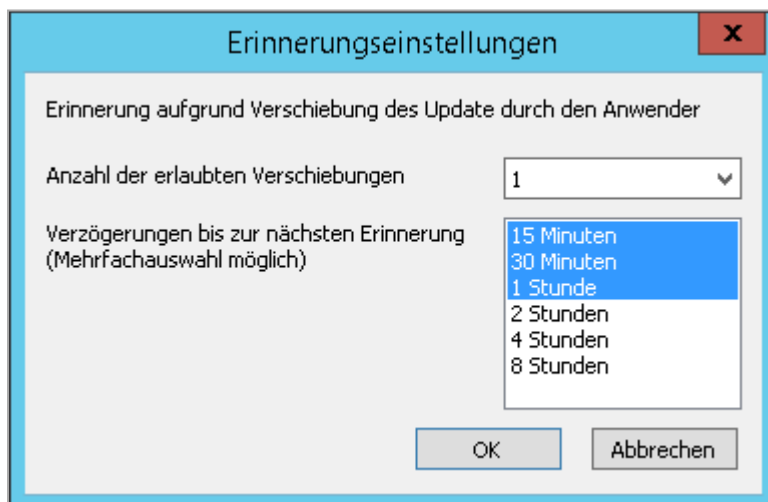
Darüber hinaus kann im Report-Generator das Feld **Updatestatus** nach dem Wert **Verschoben** ausgewertet werden (neben den Stati **Erfolgreich**, **Nicht erfolgreich** und **Nicht notwendig**).

Verschiebung von Firmware-Updates durch den Anwender konfigurieren

1. Klicken Sie in **Geräte-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.



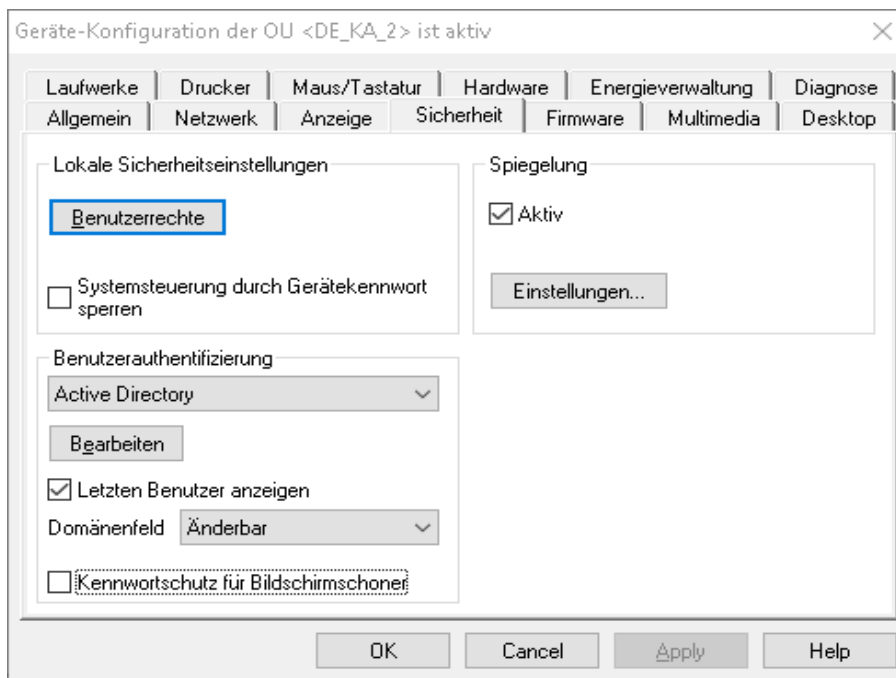
Die Möglichkeit zur Verschiebung von Firmware-Updates ist aktiviert. Wenn der Administrator ein Update-Kommando mit aktivierter Option **Benutzer informieren für** konfiguriert, erhält der Anwender eine Systemmeldung mit der Option zum Verschieben des Updates. Für weitere Informationen siehe [Auswirkungen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

5.11. Register Sicherheit



5.11.1. Benutzerrechte ändern

Der eLux RP-Client stellt in der Version 5 mit der Systemsteuerung die Register **Setup** mit den Funktionen der Geräte-Konfiguration und **Konfiguration** zur Definition von Anwendungen zur Verfügung. Ab eLux RP 6.3 befinden sich Geräte-Konfiguration und Anwendungsdefinition im **Configuration panel**.

Um zu verhindern, dass Anwender lokal am Client fehlerhafte oder ungewünschte Konfigurationen vornehmen, können Sie die Benutzerrechte für alle aufgeführten Funktionen deaktivieren oder einschränken. Zusätzlich werden allgemeine Funktionen wie beispielsweise **Abmelden** angezeigt. Eine Funktion kann entweder zugelassen oder gesperrt bzw. versteckt werden.

Funktionen und Optionen, die Sie zur Bearbeitung sperren, werden am Client abgeblendet.



Hinweis

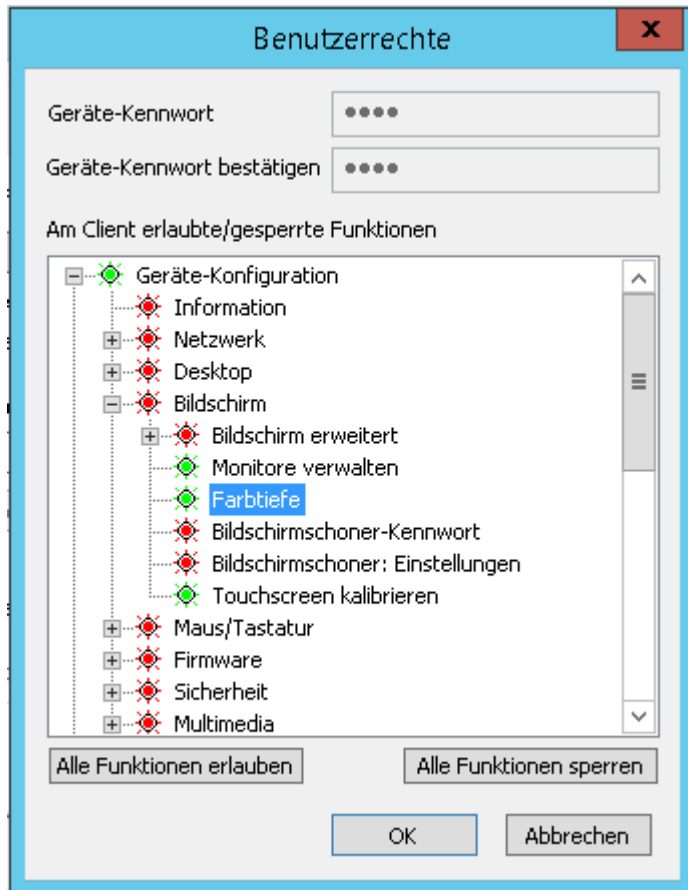
Wenn Sie die individuelle Konfiguration einzelner Funktionen der Geräte-Konfiguration zulassen, können Sie die betroffenen Felder oder Register vor dem Überschreiben durch eine aktualisierte Geräte-Konfiguration in Scout Enterprise schützen. Für weitere Informationen siehe [Lokale Geräte-Konfiguration schützen](#).

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.

Benutzerrechte für die Geräte-Konfiguration bearbeiten

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

Am eLux RP 6-Client wählen Sie im Configuration panel **Sicherheit > Benutzerrechte**.



Der Knoten **Geräte-Konfiguration**¹ bezieht sich auf die Geräte-Konfiguration der Clients und entspricht den Registern und Feldern der Systemsteuerung (eLux RP 5) bzw. des Configuration panels (eLux RP 6).

Zusätzlich finden Sie in den Benutzerrechten unter **Sicherheit > Scout Enterprise-Einstellungen**² Funktionen für die Felder **Info1**, **Info2** und **Info3**, die in der Scout Enterprise-Konsole im **Eigenschaften**-Fenster eines Gerätes und am Client im **Configuration panel** unter **Information** (eLux RP 6)³ angezeigt werden.⁴

2. Erweitern Sie die relevanten Knoten unterhalb von **Geräte-Konfiguration**⁵.

¹bis eLux RP 6.2 und Scout Enterprise 15.2: Setup

²am RP 6-Client unter Sicherheit > Info 1-3

³am eLux RP 5-Client im Systray unter Geräteinformation

⁴Ab eLux RP 6.5 wird für alle drei Info-Felder nur noch ein Benutzerrecht verwendet (Sicherheit > Info1-3).

⁵bis eLux RP 6.2 und Scout Enterprise 15.2: Setup

3. Verändern Sie den Status der relevanten Funktionen per Doppelklick oder Leertaste.

Am eLux RP 6-Client klicken Sie auf die relevante Option, um **änderbar** oder **versteckt** zu wählen.

Zugelassene Funktionen werden in der Scout Enterprise-Konsole und am eLux RP 5-Client 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**.

Am eLux RP 6-Client wählen Sie im Configuration panel **Sicherheit > Benutzerrechte**.

2. Verändern Sie den Status der unter **Anwendungsdefinition**¹ untergeordneten Funktionen per Doppelklick oder Leertaste, je nachdem, ob die Benutzer Anwendungsdefinitionen erstellen, bearbeiten oder löschen dürfen.

Am eLux RP 6-Client klicken Sie auf die relevante Option, um **änderbar** oder **versteckt** zu wählen.

3. Wenn Sie den Knoten **Anwendungsdefinition**² sperren, wird das Register **Konfiguration** in der Client-Systemsteuerung (eLux RP 5) bzw. das Register **Anwendungen** im Configuration panel (eLux RP 6) ausgeblendet und die Benutzer können die Anwendungsdefinitionen nicht sehen.



Hinweis

Wenn Sie die **Lokale Geräte-Konfiguration schützen**, aber die drei Funktionen für die Anwendungen sperren, empfehlen wir auch den übergeordneten Knoten **Anwendungsdefinition**³ zu sperren, um sicherzustellen, dass die Anwendungsdefinitionen korrekt aktualisiert werden.

Zugelassene Funktionen werden in der Scout Enterprise-Konsole und am eLux RP 5-Client grün dargestellt, gesperrte Funktionen werden rot dargestellt.

Die veränderten Benutzerrechte werden beim nächsten Neustart der Clients aktiv.

¹bis eLux RP 6.2 und Scout Enterprise 15.3: Konfiguration

²bis eLux RP 6.2 und Scout Enterprise 15.3: Konfiguration

³bis eLux RP 6.2 und Scout Enterprise 15.3: Konfiguration

5.11.2. Lokale Sicherheitseinstellungen

Systemsteuerung durch Geräte-Kennwort sichern

– nur Scout Enterprise-Konsole, ab Version 15.2 –

Für eLux RP 5-Clients können Benutzer je nach definierten Benutzerrechten über die Systemsteuerung auf die Anwendungsdefinition und die Geräte-Konfiguration zugreifen. Ab Version 15.2 können Sie bereits das Öffnen der Systemsteuerung durch die Eingabe des Geräte-Kennwortes sichern.

- ▶ Aktivieren Sie im Register **Sicherheit** unter **Lokale Sicherheitseinstellungen** die Option **Systemsteuerung durch Geräte-Kennwort sperren**.



Hinweis

Sie können außerdem das Symbol zum Öffnen der Systemsteuerung ausblenden. Für weitere Informationen siehe die Systemleisten-Einstellungen unter [Erweiterte Desktop-Einstellungen](#).

5.11.3. Benutzer-Authentifizierung konfigurieren



Hinweis

Das eLux-Paket **User authentication modules** muss auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

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

Keine	schaltet Benutzerauthentifizierung aus
Active Directory	Active Directory (Microsoft Verzeichnis-Dienst)
AD + Smartcard	Smartcard über Active Directory

Am eLux RP 6-Client aktivieren Sie zunächst unter **Sicherheit > Benutzer-Authentifizierung** die Benutzer-Authentifizierung. Dann wählen Sie unter **Authentifizierungstyp** zwischen **Active Directory** und **AD + Smartcard**.

2. Klicken Sie auf **Bearbeiten**.² Legen Sie Server, eine Serverliste oder Domänen fest. Wenn gewünscht, definieren Sie Benutzervariablen. Für weitere Informationen siehe [Benutzervariablen](#).
Bestätigen Sie mit **Übernehmen** and **OK**.
3. Um die Benutzer bei der Anmeldung zu unterstützen, aktivieren Sie die Option **Letzten Benutzer anzeigen**.
4. Wählen Sie im Listenfeld **Domänenfeld**, ob die Benutzer die Domäne ändern dürfen oder ob die Domäne ausgeblendet werden soll.
5. Für Clients mit eLux RP 6.2 und früheren Versionen können Sie die Option **Kennwortschutz für Bildschirmschoner** aktivieren. Ab eLux RP 6.3 ist der Kennwortschutz des Bildschirmschoners automatisch aktiv, wenn die Benutzerauthentifizierung eingeschaltet ist.
6. Bestätigen Sie mit **OK**.

Wenn Sie die Benutzer-Authentifizierung aktiviert 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 Geräte-Kennwort anmelden und ggf. Einstellungen korrigieren.

¹früher: Zugangsberechtigung

²Am eLux RP 6-Client finden Sie alle Optionen im gleichen Dialog.

Active Directory (AD)

Sie können mehrere Domänen definieren, aus denen der Benutzer im Anmelde-Dialog neben der Standard-Domäne auswählen kann. Die Domänen-Einträge können mit einem sprechenden Namen angezeigt werden.



Hinweis

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

User authentication modules >= 3.0.0-8

Security libraries >= 1.6.0.2-2

BaseOS eLux RP >= 5.4.0-1

Register AD-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	<p>IP-Adresse oder Name des Domänen-Controllers</p> <p>Mehrere Domänen/Server können durch Leerzeichen getrennt angegeben werden</p> <p>Beispiel: Example: <code>int.sampletec-01.com dev.sampletec-01.com</code></p> <p>Wenn sich der Server in einem anderen Subnetz als der Client befindet, muss der Fully Qualified Domain Name (FQDN) angegeben werden.</p> <p>Wenn Sie mehrere Domänen-Einträge definieren,² kann der Benutzer aus einem Listefeld wählen. Die Domänen werden mit ihrem Anzeigenamen angezeigt. Der oberste Eintrag ist die Standard-Domäne im AD-Anmelde-Dialog am Client. Anwendungen können so definiert werden, dass sie nur in einer Domäne angezeigt werden.</p>



Hinweis

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

¹ab Scout Enterprise Management Suite Version 14.8

²ab Scout Enterprise Management Suite Version 14.8

Register Benutzervariablen

Auf der Basis von LDAP-Attributen können Sie lokale Variablen definieren und in der Geräte-Konfiguration oder Anwendungsdefinition einsetzen. Für weitere Informationen siehe [Benutzervariablen](#).

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.

Register Automatische Anmeldung

– ab Scout Enterprise 15.9 –

Mit Hilfe von vordefinierten Anmeldedaten können beispielsweise Terminals im Kiosk-Modus unter einem AD-Service-Konto laufen.

Benutzername, Kennwort und Domäne können als Variablen gesetzt werden.

Active Directory + Smartcard



Hinweis

Damit Smartcard-Reader verwendet werden können, muss die relevante Middleware auf den Clients installiert sein. **sc/interface** von Cryptovision ist Smartcard-Middleware, die Smartcards und andere Krypto-Token mit Anwendungsprogrammen verbindet. Sie unterstützt mehr als 90 Kartenprofile. Für weitere Informationen siehe die Cryptovision-Webseite. Um **sc/interface** zu verwenden, muss das eLux-Paket **Cryptovision sc/interface PKCS11** auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

Register Smartcard

Option	Beschreibung
Verhalten beim Ziehen der Smartcard	Wenn Sie die Option <code>Bildschirm sperren</code> wählen, überprüfen Sie, ob in den Bildschirmschoner -Einstellungen die Option Kennwortschutz aktiviert ist ¹
Anmeldung mit Benutzer+Kennwort erlauben	Smartcard-Anwendung erlaubt alternativ die Anmeldung mit Benutzername/Kennwort über die ESC-Taste (eLux RP 5) bzw. den Link Benutzername & Kennwort (eLux RP 6).

¹ab eLux RP 6.3 automatisch

Option	Beschreibung
Benutzer+Kennwort / Dialog standardmäßig anzeigen ¹	Die Anmeldung kann trotz Smartcard-Konfiguration über Benutzer+Kennwort erzwungen werden. Diese Option setzt voraus, dass Anmeldung mit Benutzer+Kennwort erlauben eingeschaltet ist.

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 beim nächsten Neustart zum Client übertragen.

Register Benutzervariablen

Auf der Basis von LDAP-Attributen können Sie lokale Variablen definieren und in der Geräte-Konfiguration oder Anwendungsdefinition einsetzen. Für weitere Informationen siehe [Benutzervariablen](#).

Für die Register **AD-Verzeichnis**, **Serverprofil** und **Automatische Anmeldung** siehe [Active Directory \(AD\)](#).

5.11.4. Zusätzliche Optionen für AD-Benutzer

Wenn Sie Active Directory zur Benutzer-Authentifizierung verwenden, melden sich die Benutzer mit ihrem AD-Domänen-Konto und -Kennwort am Client an. Die Anwendungen zur Backend-Verbindung (Citrix, RDP, VMware) unterstützen die Passthrough-Anmeldung.

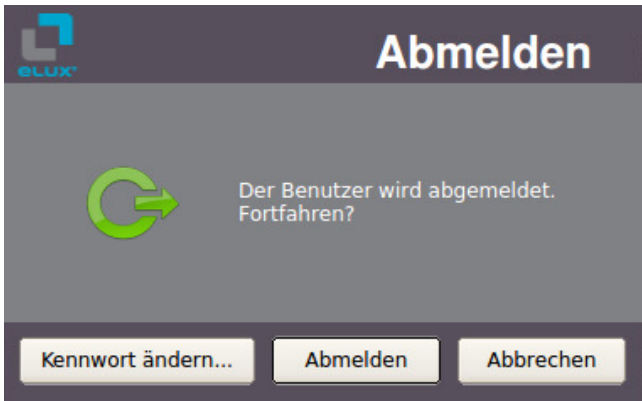
Am Client wird der angemeldete Benutzer im Configuration panel unter **Information** angezeigt.²

Kennwort ändern

Um das Kennwort zu ändern, verwenden die Benutzer das eLux-Kommando **Abmelden** (eLux RP 6) oder die **Beenden**-Schaltfläche der Systemsteuerung (eLux RP 5).

¹ab Scout Enterprise Management Suite 15.5 und eLux RP 6.6

²ab eLux RP 6.4



eLux RP 6



eLux RP 5

Kennwortschutz für Bildschirmschoner



Hinweis

Wenn die Benutzer-Authentifizierung eingeschaltet ist, ist der Kennwortschutz automatisch aktiv und kann nicht ausgeschaltet werden.¹

Bis Scout Enterprise Management Suite 15.2 und eLux RP 6.2:

- ▶ Aktivieren Sie im Register **Bildschirm** die Option **Kennwortschutz**. Der Kennwortschutz erfordert, dass die [Benutzer-Authentifizierung](#) eingeschaltet ist.

Das Kennwort für den Bildschirmschoner ist mit dem Wert aus `$ELUXPASSWORD` vorbelegt. Für weitere Informationen siehe [Anwendungsmöglichkeiten für Benutzervariablen](#).

Der Bildschirmschoner wird nach der definierten Zeitspanne aktiv und das System ist gesperrt. Durch Drücken einer Taste oder Mausbewegung wird der Dialog zum Entsperren angezeigt. Dieser Dialog bietet den Benutzern folgende Optionen:

Option	Schaltfläche	Beschreibung
Der angemeldete Benutzer entsperrt den Bildschirm durch Eingabe seines Kennwortes / Smartcard	Entsperren	Standardfall

¹ab Scout Enterprise Management Suite 15.3 und eLux RP 6 3

Option	Schaltfläche	Beschreibung
Eine andere Person hinterlässt dem angemeldeten Benutzer eine Nachricht	Nachricht	<p>Der Bildschirm bleibt gesperrt. Der angemeldete Benutzer erhält nach dem Entsperren des Bildschirms eine Benachrichtigung mit der hinterlassenen Nachricht.</p> <p>Diese Funktion ist standardmäßig aktiv und kann durch folgenden Erweiterten Dateieintrag deaktiviert werden:¹ Datei: <code>/setup/terminal.ini</code>, Abschnitt: <code>xscreensaver_dialog</code>, Eintrag: <code>MessageEnabled</code>, Wert: <code>false</code></p>
Ein anderer Benutzer authentifiziert sich, um den vorherigen Benutzer abzumelden (und sich anzumelden), das Gerät neu zu starten oder herunterzufahren. ²	Abmelden	<p>Sinnvoll, wenn Geräte von mehreren Benutzern verwendet werden:</p> <p>Geräte, die in angemeldetem Zustand verlassen wurden und daher blockiert sind, können wieder genutzt werden.</p> <p>Sobald sich der neue Benutzer authentifiziert hat, werden die Schaltflächen Neu starten, Herunterfahren und Abmelden aktiv. In jedem Fall wird der angemeldete Benutzer abgemeldet.</p> <p>Diese Funktion ist standardmäßig deaktiviert und kann durch folgenden Erweiterten Dateieintrag aktiviert werden: Datei: <code>/setup/terminal.ini</code>, Abschnitt: <code>xscreensaver_dialog</code>, Eintrag: <code>ShowSysCommandButtons</code>, Wert: <code>true</code></p>



Achtung

Datenverlust kann entstehen, wenn die Option **Abmelden** mit anschließendem Neustart, Herunterfahren oder Abmelden durchgeführt wird. Der angemeldete Benutzer wird ungeachtet eventuell ungespeicherter Dokumente oder Daten abgemeldet.

Service-App

– ab eLux RP 6.4 –

AD-Benutzern können Sie die Möglichkeit geben, eLux ohne Anmeldung im Service-Modus zu starten. Dazu definieren Sie eine Service-App, die mit der **Service**-Schaltfläche aus dem Anmelde-Dialog heraus gestartet werden kann. Für weitere Informationen siehe [Service-App definieren](#).

¹ab eLux RP 6.8

²ab eLux RP 6.8

Configuration panel aus Anmelde-Dialog öffnen

– ab eLux RP 6.5 –

AD-Benutzern können Sie die Möglichkeit geben, vor der Anmeldung auf das Configuration panel zuzugreifen. So können sich Benutzer zu einem WLAN oder VPN verbinden oder die Sprache ändern, bevor sie sich anmelden.

- ▶ Erlauben Sie für die relevanten Clients unter **Sicherheit > Benutzerrechte** ganz unten das Benutzerrecht **Configuration panel aus Anmelde-Dialog starten**.

Nach dem nächsten Gerätestart wird im AD-Anmelde-Dialog unten links die Schaltfläche zum Öffnen

des Configuration panel angezeigt:



Die Benutzer können auf die freigeschalteten Optionen der Geräte-Konfiguration zugreifen.



Hinweis

Standardmäßig ist das Benutzerrecht **Configuration panel aus Anmelde-Dialog starten** ausgeschaltet.

5.11.5. Benutzervariablen



Hinweis

Um Benutzervariablen verwenden zu können, müssen die Pakete **User authentication modules** und **Open LDAP** auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

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

Vorgegebene Benutzervariablen sind:

```
$ELUXUSER  
$ELUXDOMAIN  
$ELUXPASSWORD
```

Diese werden beim Anmelden eingetragen, wenn die **Benutzer-Authentifizierung** eingeschaltet ist.

Anwendungsmöglichkeiten für Benutzervariablen



Hinweis

Diese Funktion kann nur verwendet werden, wenn die Benutzer-Authentifizierung über Active Directory konfiguriert ist.

Benutzervariablen werden mit dem `$`-Zeichen eingeleitet. Sie können in den folgenden Feldern verwendet werden:

Befehl	Funktion	Benutzervariable
STRG + ALT + ENDE Start > Sperren ¹	Manuelle Aktivierung der Bildschirmsperre	<code>\$ELUXPASSWORD</code>

Geräte-Konfiguration

	Feld	Benutzervariable
Laufwerke	Benutzername	<code>\$ELUXUSER</code>
	Kennwort	<code>\$ELUXPASSWORD</code>
	Verzeichnis, Server, Freigabename	Jede <code>\$ELUX</code> -Variable
	Browser Homeverzeichnis	Jede <code>\$ELUX</code> -Variable

¹bis eLux RP 5

	Feld	Benutzervariable
Energieverwaltung 1	Bildschirmschoner aktivieren	\$ELUXPASSWORD

Anwendungsdefinition

	Feld	Benutzervariable
Citrix	Server	Jede \$ELUX-Variable
RDP	Benutzername	\$ELUXUSER
VMwareView	Kennwort	\$ELUXPASSWORD
	Domäne	\$ELUXDOMAIN
Browser	Proxy-Typ, Proxy-Port	Jede \$ELUX-Variable
Tarantella	Server	Jede \$ELUX-Variable
Lokale / Benutzerdefinierte Anwendung	Parameter für alle Programme, die über die Kommandozeile aufgerufen werden Beispiel: eluxrdp /v:int.sampletec-01.com /u:\$ELUXUSER /p:\$ELUXPASSWORD	Jede \$ELUX-Variable

Neue Benutzervariablen definieren



Hinweis

Diese Funktion kann nur verwendet werden, wenn die Benutzer-Authentifizierung über Active Directory konfiguriert ist.

Sie können eigene Benutzervariablen als lokale Variablen auf der Basis von LDAP-Attributen definieren. Die Variablendefinition hat die Form `Lokale Variable = LDAP-Variable`

1. Wählen Sie in **Geräte-Konfiguration > Sicherheit** im Feld **Benutzer-Authentifizierung**² entweder `Active Directory (AD)` oder `Active Directory + Smartcard` als Authentifizierungsmethode.
2. Klicken Sie auf **Bearbeiten**.

¹bis Scout Enterprise 15.2: Register Bildschirm

²früher Zugangskonfiguration

-
3. Bearbeiten Sie unter **Benutzer-Authentifizierung > Benutzervariablen** folgende Felder:

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

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



Hinweis

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

5.11.6. Spiegelung konfigurieren

1. Schalten Sie im Register **Sicherheit > Spiegelung** die Option **Aktivieren** ein.
2. Klicken Sie auf **Einstellungen...**, um die Spiegelung zu konfigurieren.

Option	Beschreibung
Kennwort (optional)	Wenn Sie ein Spiegelungskennwort definieren, wird das Kennwort vor dem Starten einer Spiegelungssitzung abgefragt. Das Kennwort muss mindestens 6 Zeichen und maximal 8 Zeichen lang sein.
Nur Lesezugriff	Erlaubt nur lesenden Zugriff
Benutzer muss bestätigen innerhalb	Vor der Spiegelung muss der Benutzer bestätigen. Legen Sie fest, wieviele Sekunden die Anfrage angezeigt werden soll, bevor der Verbindungsversuch abgebrochen wird. ¹
Spiegelungssitzung protokollieren	Protokolliert die Spiegelungssitzung
Verschlüsselte Datenübertragung	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 ²	Sobald die Verbindung abbricht, findet eine automatische Abmeldung statt.

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

Für weitere Informationen siehe [Spiegelung](#).



Hinweis

Eine Spiegelungssitzung kann vom Gespiegelten jederzeit abgebrochen werden.

¹ab Scout Enterprise Management Suite 15.2

²ab Scout Enterprise Management Suite 14.8

5.12. 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.

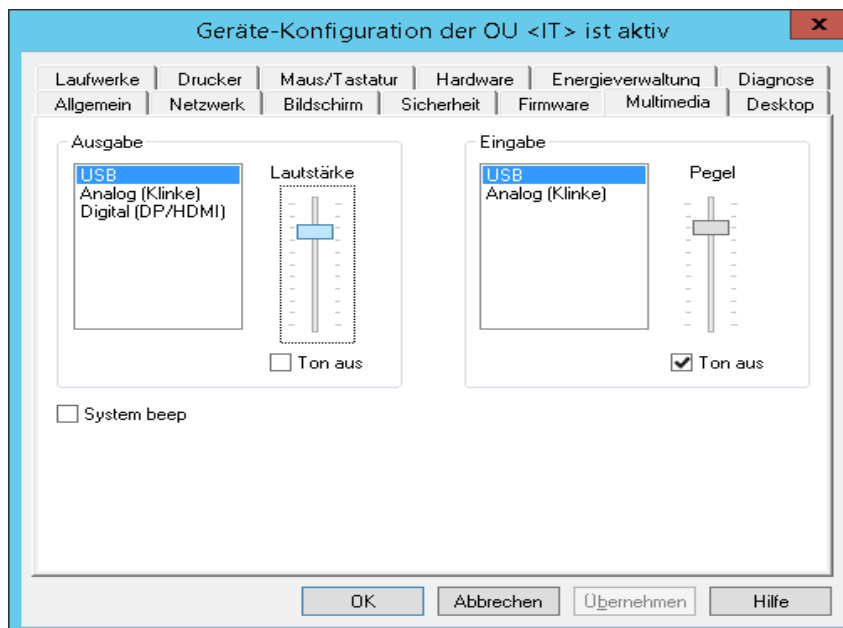
Die angeschlossenen **Eingabe**-Geräte werden nach ihrem Anschluss gruppiert:

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)
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.
System beep	Akustische Systemrückmeldung beim Ausschalten des Thin Client
Priorität der Geräteklassen	Durch Drag-und-Drop können Sie die Priorität der Geräteklassen für Ausgabe- und Eingabegeräte ändern. Der oberste Eintrag hat die höchste Priorität.

5.13. 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.

5.13.1. 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, muss das Paket **Network drive share** und das hierin enthaltene Feature-Paket **Linux Key Management Utilities**¹ 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.

Beispiel: /smb/share

¹ab eLux RP 5.3

**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](#).

5.13.2. 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-Geräte werden die Mountpoints chronologisch zugewiesen. Das erste Gerät erhält den Mountpoint /media/usbdisk, das zweite /media/usbdisk0 usw.

Angeschlossene Geräte werden mit Mountpoint im Systray (eLux RP 5) bzw. als Live-Information (eLux RP 6) in der Systemleiste angezeigt.

**Hinweis**

Aus Sicherheitsgründen muss die lokale Nutzung über die Option **Massenspeichergeräte erlauben** im Register [Hardware](#)¹ aktiviert werden.

¹ab eLux RP 6.2 Register Peripherie

Für verwaltete eLux RP 5-Clients kann die Anzeige in der Scout Enterprise-Konsole über die relevante Option im Register **Desktop > Erweitert > Taskleiste** unterdrückt werden.

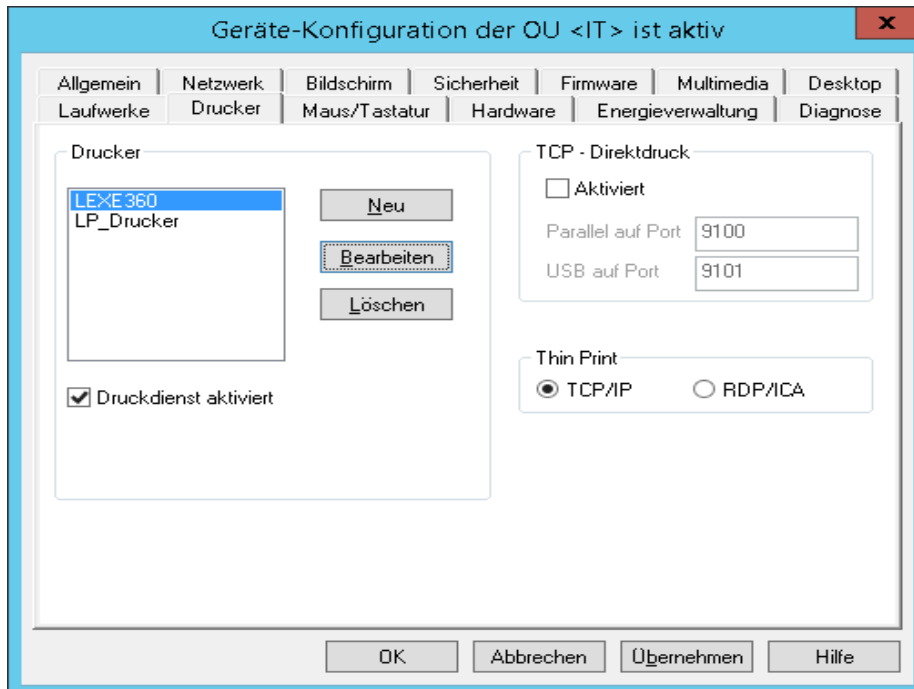


Hinweis

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 Anwendungs-Einstellungen](#).

5.14. Register Drucker

eLux 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. Neben den Protokollen LPR und TCP-Direktdruck stehen auch proprietäre Protokolle zur Verfügung.



In der Scout Enterprise-Konsole unter **Geräte-Konfiguration > Drucker > Neu** können Sie Drucker mit logischen Namen definieren und konfigurieren. In eLux RP 5 öffnen Sie die Systemsteuerung und **Setup > Drucker**.

5.14.1. Lokal angeschlossenen Drucker definieren

1. Klicken Sie in der Geräte-Konfiguration im Register **Drucker** auf **Neu**.
2. Geben Sie im Dialog **Drucker definieren** einen Namen für den Drucker ein.
3. Wählen Sie im Feld **Druckeranschluss**, wie der Drucker mit dem Client verbunden ist.
4. Legen Sie im Feld **Filter** fest, ob ein Filter verwendet werden soll. Um über eine Linux-Shell zu drucken, wählen Sie den `Text`-Filter. Für weitere Informationen zu den Filtern siehe [Netzwerkdrucker definieren](#).
5. Bestätigen Sie mit **OK** und **Übernehmen**.

5.14.2. Netzwerkdrucker definieren

1. Klicken Sie in der Geräte-Konfiguration im Register **Drucker** auf **Neu**.

The screenshot shows the 'Drucker definieren' dialog box. The 'Name' field is set to 'LEXE360'. Under the 'Verbindung' section, 'Druckeranschluss' is set to 'Netzwerk', 'Filter' is set to 'PCL2', 'Baud-Rate' is set to '<System>', 'Druckeradresse' is '172.18.164.125', and 'Druckerqueue' is 'raw0'. Under 'Am Server', 'Treibernamen' is set to 'Lexmark E360dn XL'. The 'thinprint' section has the 'Verbinden' checkbox unchecked. The 'OK' and 'Abbrechen' buttons are at the bottom.

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

Option	Beschreibung
Kein	Die Druckdaten werden ungefiltert an den Drucker weitergeleitet.
Text	ermöglicht das Drucken aus einer lokalen Shell
PCL2	ermöglicht das Drucken an nicht-Postscript-fähige Drucker im PCL-Format Wenn nicht aus einer Citrix-Sitzung gedruckt wird, muss der angeschlossene Drucker eine der folgenden Sprachen unterstützen: PCL2 , PS (Postscript) oder PDF .

5. Geben Sie im Feld **Druckeradresse** die IP-Adresse des Servers ein.
6. Geben Sie in das Feld **Druckerqueue** den Freigabenamen des Druckers ein.
7. Geben Sie im Feld **Treibernamen** den Treibernamen für den Drucker ein. Dieser Treiber wird für das Drucken aus einer Windows-Sitzung verwendet.



Achtung

Der Druckertreibername 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 und Leerzeichen.

Für weitere Informationen siehe [Citrix auto-created Printers](#).

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

Für weitere Informationen siehe das Handbuch Ihres Druckers.

5.14.3. Drucker freigeben

Alle in **Geräte-Konfiguration > Drucker** definierten Drucker können Sie zur Nutzung für andere Systeme über LPD innerhalb des Netzwerks freigeben.

1. Aktivieren Sie in **Geräte-Konfiguration > Drucker** die Option **Druckdienst aktiviert**.
2. Aktivieren Sie den Windows LPD-Dienst (Line Printer Demon).

Die Option sorgt dafür, dass der Druckdienst am Client gestartet wird. Auf alle Drucker, die in der Liste definiert sind, können Druckaufträge von Geräten aus dem Netzwerk ausgegeben werden.

Die Drucker werden vom CUPS-Server kontrolliert.

5.14.4. Standarddrucker wählen

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevante OU oder Gerät die **Erweiterte Geräte-Konfiguration¹ > Drucker**.
2. Wählen Sie aus der Liste **Standarddrucker auswählen** einen Drucker aus.

Alle bereits definierten Drucker für dieses Element werden in der Liste angezeigt.

¹früher: Erweiterte Einstellungen

5.14.5. CUPS

Der CUPS-Server wird standardmäßig auf den Clients installiert (**Print Environment (CUPS)**-Paket) und ermöglicht das Drucken aus lokalen Anwendungen und die Nutzung lokal angeschlossener Drucker.

Das Common UNIX Printing System™ (CUPS™) ist ein kostenfreies Produkt von Easy Software/Apple. Es bietet eine gemeinsame Druckerschnittstelle in lokalen Netzwerken und eine dynamische Druckererkennung und -gruppierung. Für weitere Informationen siehe www.cups.org.

Der CUPS-Server kann auf serielle und parallele Ports, USB und Netzwerk (LPD) ausgeben.

Das CUPS-Drucksystem 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. Wenn kein PostScript-Drucker vorhanden ist, müssen Sie am CUPS-Server einen Filter installieren, beispielsweise **PostScript zu PCL**.

CUPS Web-Interface zur Druckverwaltung



Hinweis

Das eLux-Paket **Print Environment (CUPS)** und das hierin enthaltene Feature-Paket **Web administration service** muss auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

Der Benutzer kann in einem lokalen Browser mit folgender URL das CUPS-Web-Interface aufrufen und Druckaufträge verwalten:

`http://localhost:631`

Das Web-Interface kann außerdem vom Administrator zur Konfiguration des CUPS-Servers genutzt werden. Dafür ist die Eingabe der Credentials für das lokale Administrator-Konto (`LocalLogin` und Geräte-Kennwort) erforderlich.

5.14.6. Citrix auto-created Printer

Citrix bietet die Möglichkeit, Drucker automatisch für die Dauer einer Sitzung einzurichten (**auto-created printer** oder **dynamic printer mapping**). Beim Anmelden über die Citrix-Verbindung wird eine Druckerdefinition am Citrix-Server erstellt. Die Druckerdefinition steht nur dem angemeldeten Benutzer zur Verfügung und wird mit der Abmeldung gelöscht.

Citrix verwendet entweder den jeweils angegebenen Druckertreiber oder, falls nicht vorhanden, den universellen Citrix-Druckertreiber.

Lokalen Drucker clientseitig für die automatische Druckereinrichtung konfigurieren

1. Geben Sie unter **Geräte-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.

Wenn eine Citrix-Verbindung zum Citrix-Server gestartet wird, sieht der Benutzer in den Drucker-Einstellungen die automatisch erstellten Client-Drucker.

Wenn der spezifische Treiber nicht am Anwendungsserver installiert ist oder der Name nicht identisch ist, wird der universelle Citrix-Drucker verwendet.

Citrix Universal Printing

Den universellen Citrix-Drucker und weitere Druckereinstellungen können Sie mit Administratorrechten am Citrix-Server konfigurieren. Für weitere Informationen siehe die **Citrix Product Documentation**.

5.14.7. TCP-Direktdruck

Die Druckdaten können direkt über TCP/IP empfangen und auf die parallele Schnittstelle oder die USB-Schnittstelle zum Drucker geschickt werden. Die Daten werden nicht für den Druck aufbereitet und es wird kein Druckerspooler verwendet. Die Flusskontrolle übernimmt TCP/IP.

TCP-Direktdruck konfigurieren

1. Aktivieren Sie in **Geräte-Konfiguration > Drucker** unter **TCP-Direktdruck** die Option **Aktiviert**.
2. Geben Sie die verwendete Portnummer zur Kommunikation an.
Die Standard-Portnummern sind:
9101 für USB-Drucker
9100 für Parallelport-Drucker



Hinweis

Beachten Sie, dass die angegebenen Ports am Client geöffnet werden.

Wenn Sie aus einer Windows-Sitzung drucken wollen, wählen Sie als Druckeranschluss einen Standard-TCP/IP-Port und geben 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`.

5.14.8. ThinPrint

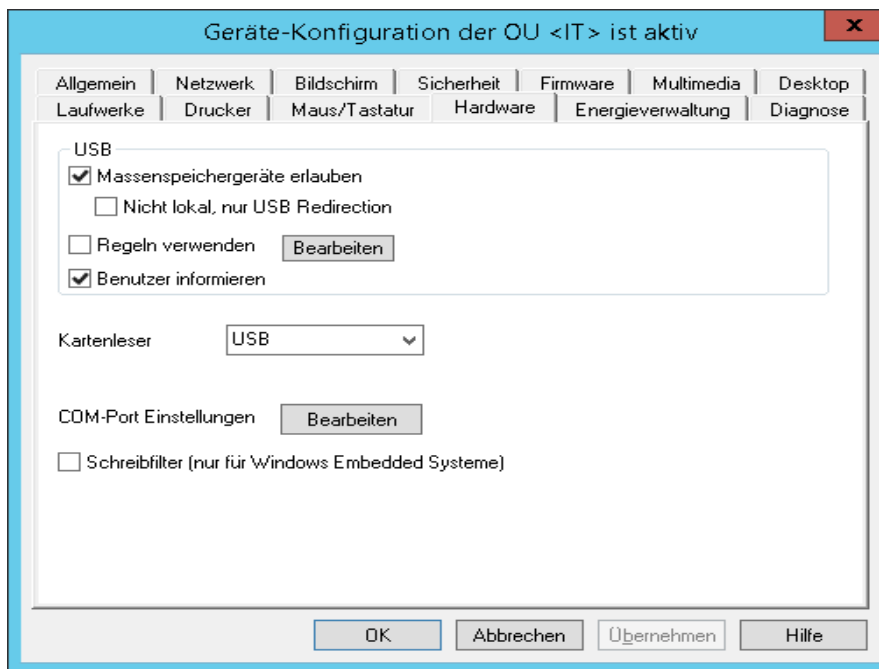
ThinPrint von der ThinPrint GmbH ermöglicht optimiertes Drucken im Netzwerk auf verschiedenen Plattformen. ThinPrint ist ein Druckprotokoll, das im Gegensatz zu TCP-Direktdruck, LPR oder CUPS eine Begrenzung der Bandbreite erlaubt. Es empfiehlt sich daher zum Einsatz in Netzwerken mit geringer Bandbreite (WAN).

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 konfigurieren

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

5.15. Register Hardware



5.15.1. USB-Massenspeicher und Kartenleser

Option	Beschreibung
Massenspeichergeräte erlauben	<p>Erlaubt die Verwendung angeschlossener USB-Massenspeichergeräte</p> <p>Wenn die lokale Nutzung von USB-Geräten über Mountpoints erlaubt ist, werden USB-Geräte auf der Systemleiste im Systray (eLux RP 5) bzw. als Live-Information (eLux RP 6) auf der Systemleiste ¹ angezeigt.</p>
Nicht lokal, nur USB Redirection ²	<p>Beschränkt die Verwendung von USB-Massenspeichergeräten auf die USB-Geräteumleitung (USB Redirection) innerhalb einer Verbindung zu einem Backend. Es steht kein Mountpoint zur lokalen Nutzung auf dem eLux-Client zur Verfügung.</p>
Regeln verwenden	<p>Beschränkt die Verwendung von USB-Massenspeichergeräten gemäß definierter USB-Regeln:</p> <p>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 Smart-card-Reader verwendet werden.</p>

¹ab eLux RP 6.4

²ab eLux RP 5.4

Option	Beschreibung
Bearbeiten	Öffnet den Dialog USB-Regeln : Definieren Sie Regeln, um bestimmte Geräte-Modelle explizit zu erlauben oder verweigern.
Kartenleser	Aktiviert Kartenleser auf dem ausgewählten Anschluss
Benutzer informieren	Beim Anschließen und Entfernen eines USB-Massenspeichergerätes wird eine Systray-Meldung (eLux RP 5) bzw. Live-Information-Meldung (eLux RP 6) ¹ 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

Damit Smartcard-Reader verwendet werden können, muss die relevante Middleware auf den Clients installiert sein. **sc/interface** von Cryptovision ist Smartcard-Middleware, die Smartcards und andere Krypto-Token mit Anwendungsprogrammen verbindet. Sie unterstützt mehr als 90 Kartenprofile. Für weitere Informationen siehe die Cryptovision-Webseite.

Um **sc/interface** zu verwenden, muss das eLux-Paket **Cryptovision sc/interface PKCS11** auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

¹ab eLux RP 6.4

5.15.2. USB-Regeln zur Verwendung von USB-Geräten definieren

1. Öffnen Sie für die relevante OU oder Gerät **Geräte-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 am Client im **USB-Geräte Info**-Dialog der Taskleiste (eLux RP 5) oder im Configuration Panel unter **Peripherie > USB > Information** (eLux RP 6):

Peripherie	
USB	^
Einstellungen	v
Information	^
Optical Mouse	v
USB Keyboard	v
JetFlash	^
Produktname JetFlash	
Herstellername Transcend Information, Inc.	
Seriennummer DA43E690	
Produkt-ID	1000
Hersteller-ID	8564
Typ Massenspeicher	
Mountpoints Freier Speicherplatz /media/usbdisk 7.27 GB von 7.27 GB	

5. Bestätigen Sie mit **OK**.

Beispiele für Regeln

Regel	Code
Nur ein bestimmtes USB-Stick-Modell zulassen	<pre>ALLOW: VID=0781 PID=5151 # USB-Stick-Modell zulassen (Beispiel: SanDisk Cruzer Micro) DENY: CLASS=08 # Alle Geräte der Klasse MASSENSPEICHER verweigern</pre>
Nur ein bestimmtes Smartcard-Modell verweigern	<pre>DENY: VID=18a5 PID=0302 # Smartcard-Modell verweigern (Beispiel: Omnikey CardMan 3821) ALLOW: CLASS=0B # Alle Geräte der Klasse SMARTCARD zulassen</pre>
Alle Drucker, Massenspeicher und Smartcard-Geräte verweigern	<pre>DENY: CLASS=07 # Alle Geräte der Klasse DRUCKER ver- weigern DENY: CLASS=08 # Alle Geräte der Klasse MASSENSPEICHER verweigern DENY: CLASS=0B # Alle Geräte der Klasse SMARTCARD ver- weigern</pre>
Alle Geräte verweigern	<pre>DENY: # Alle Geräte verweigern</pre>

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 Hersteller-spezifischen 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.

5.15.3. Regeln für die USB-Geräteumleitung (Redirection) definieren

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

1. Erfassen Sie die relevanten USB-Filterregeln in der entsprechenden Konfigurationsdatei:

Anwendung	Konfigurationsdatei	Beispiele
Citrix	/setup/ica/usb.conf	ALLOW: VID=0781 PID=5151 DENY: CLASS=08
VMware	/setup/elux/.vmware/default-config	viewusb.ExcludeFamily = "storage" viewusb.IncludeVidPid = "vid-0781_pid-5151"

2. Um die Konfigurationsdateien zum Client zu übertragen, verwenden Sie die Scout Enterprise-Funktion **Konfigurierte Dateiübertragung**. Für weitere Informationen siehe [Konfigurierte Dateiübertragung](#).

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

5.15.4. Sicheres 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.

Der Benutzer kann am Client das USB-Symbol auf der Systemleiste im Systray (eLux RP 5) bzw. in der Live-Information (eLux RP 6) mit der rechten Maustaste anklicken und **Sicher entfernen** wählen.

Tastenkombination zum Entfernen aller eingesteckter USB-Geräte definieren

In der Scout Enterprise-Konsole können Sie eine Tastenkombination definieren, mit der die Benutzer alle eingesteckten USB-Massenspeicher in einem Schritt sicher entfernen können. Die folgende Anleitung verwendet als Beispiel die Tastenkombination ALT+WINDOWS+S

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Konfiguration > Erweiterte Dateieinträge**.
2. Definieren Sie folgenden Eintrag:

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

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

5.15.5. Bluetooth Audio-Geräte aktivieren

– ab eLux RP 6.6 –

Die Verwendung von Bluetooth Audio-Geräten kann zentral über die Konsole erlaubt werden. Die Benutzer können dann im eLux Config panel nach entsprechenden Geräten suchen lassen und sich verbinden.

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Konfiguration > Erweiterte Dateieinträge**.
2. Definieren Sie folgenden Eintrag:

Datei	/setup/terminal.ini
Abschnitt	Bluetooth
Eintrag	Enabled
Wert	true

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

Für weitere Informationen siehe auch [Bluetooth Audio-Geräte verbinden](#) im **eLux**-Handbuch.

5.16. Register Diagnose

Im Register **Diagnose** konfigurieren Sie die Gerätediagnose-Funktion, mit der Sie Diagnosedateien vom Client anfordern können:

Option	Beschreibung
Protokollierungsstufe	Die erweiterte Protokollierung (Ein) bewirkt, dass im Zuge der Gerätediagnose vordefinierte Skript-Befehle auf dem Client ausgeführt werden und Konfigurations- und Logdateien in größerem Umfang vom Client angefordert werden. Falls Sie den technischen Support von Unicon benötigen, schalten Sie diese Option ein, bevor Sie Diagnosedateien anfordern.



Hinweis

Verwenden Sie die erweiterte Protokollierungsstufe ausschließlich als temporäre Geräte-Konfiguration. Andernfalls laufen Sie Gefahr, an die Flashspeicher-Kapazitätsgrenze des Thin Clients zu stoßen.

Dateien senden an	Ziel für die vom Client angeforderten Diagnosedateien
-------------------	---

Die Gerätediagnose wird über ein Online-Kommando ausgeführt. Für weitere Informationen siehe [Gerätediagnose](#).

5.17. Register Energieverwaltung

– ab Scout Enterprise Management Suite 15.3 –

Insbesondere bei Verwendung von mobilen Endgeräten sind Optionen zum Energiesparen wichtig. Das Register **Energieverwaltung** erlaubt Ihnen, mit Hilfe von Profilen Einstellungen vorzudefinieren, die beim Setzen des jeweiligen Profils aktiv werden:

- **Hohe Leistung:** Schwerpunkt auf hoher Leistung, kann aber mehr Energie verbrauchen
- **Energie sparen:** Spart Energie durch Absenken der Leistung und Dimmen oder Ausschalten des Bildschirms

Die Profile zur Energieverwaltung können Sie entweder explizit aktivieren oder für mobile Geräte über die Option **Auto** vom System wählen lassen: Wenn das Gerät an der Stromversorgung angeschlossen ist, wird das Profil **Hohe Leistung** aktiviert, ohne Stromversorgung das Profil **Energie sparen**.

Beide Profile können zusätzlich für die Zeit außerhalb der Arbeitszeiten angepasst werden.¹ Durch einen strikteren Einsatz der Energiespar-Optionen außerhalb der Arbeitszeiten können Sie den Energieverbrauch zusätzlich optimieren. Hinterlegen Sie dafür Ihre Arbeitszeiten, um die Profile für **Außer-**

¹ab Scout Enterprise 15.8

halb der Arbeitszeit zu aktivieren. Die Umschaltung der Profile zwischen **Arbeitszeit** und **Außerhalb der Arbeitszeit** basiert auf den von Ihnen definierten Arbeitszeiten.

Profil zur Energieverwaltung setzen

- Wählen Sie auf dem Register **Energieverwaltung** im Listenfeld **Aktives Profil zur Energieverwaltung** das gewünschte Profil oder die Option `Auto`.

*Die im Profil definierten Einstellungen werden aktiv. Die Option `Auto` aktiviert das Profil **Hohe Leistung**, wenn das Gerät an der Stromversorgung angeschlossen ist und das Profil **Energie sparen**, wenn das Gerät ohne Stromversorgung ist.*

Profil-unabhängige Optionen

Option	Beschreibung
Benachrichtigung bei Akku-Stand	Für Geräte ohne Stromversorgung: Akkustand in Prozent, ab dem der Benutzer benachrichtigt wird
Benutzer vor Wechsel in Standby-Modus abmelden ¹	Die Benutzer müssen sich nach der Aktivierung aus dem Standby-Modus neu anmelden.

¹ab Scout Enterprise 15.8

5.17.1. Profil zur Energieverwaltung konfigurieren



Hinweis

Wenn Sie Ihre Arbeitszeiten definieren, können Sie auch festlegen, welche Energiespar-Optionen außerhalb der Arbeitszeit angewendet werden sollen.¹ Wenn Sie keine Arbeitszeiten definieren, sind die Energiespar-Optionen durchgehend gültig (24/7).

Energieverwaltungsprofile bearbeiten

Hohe Leistung (Während Arbeitszeit) | Hohe Leistung (Außerhalb Arbeitszeit)

Energie sparen (Während Arbeitszeit) | Energie sparen (Außerhalb Arbeitszeit)

Bildschirm-Helligkeit

☒ Bildschirm ausschalten nach 1 min.

☒ Bildschirmschoner aktivieren nach 1 min.

☒ Bei Leerlauf nach 10 min. Aktion Standby-Modus

Aktion bei 'Computer zuklappen' Standby-Modus

Aktion bei 'Netzschalter drücken' Herunterfahren

Aktion bei 'Power/Sleep-Taste drücken' Standby-Modus

OK Cancel

1. Klicken Sie neben **Profil für Energieverwaltung** auf **Bearbeiten** und wählen dann das Register für das gewünschte Profil.²
Für Profile, die außerhalb der Abseitszeit gelten, definieren Sie zunächst Ihre Arbeitszeiten.¹

¹ab Scout Enterprise 15.8

2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Bildschirm-Helligkeit	Bildschirm-Helligkeit in Prozent für das ausgewählte Profil Zeigen Sie über den Schieberegler um die Prozentzahl anzuzeigen.
Bildschirm ausschalten nach	Legt fest, ob nach der angegebenen Anzahl von Minuten der Bildschirm ausgeschaltet wird, wenn der Benutzer das Gerät nicht verwendet (Leerlauf)
Bildschirmschoner aktivieren nach	Legt fest, ob nach der angegebenen Anzahl von Minuten der Bildschirmschoner aktiviert wird, wenn der Benutzer das Gerät nicht verwendet (Leerlauf)
Bei Leerlauf nach – Aktion	Legt fest, ob bei Leerlauf nach der angegebenen Anzahl von Minuten die ausgewählte Aktion durchgeführt wird: ¹ Herunterfahren Standby-Modus
Bei Leerlauf nach (Benutzer abgemeldet)	Wenn der Benutzer abgemeldet ist und das Gerät im Leerlauf ist, wird nach der angegebenen Anzahl von Minuten die oben ausgewählte Aktion durchgeführt. ²
Aktion bei 'Computer zuklappen'	Aktion, die durchgeführt wird, wenn der Benutzer den Computer zuklappt: Keine Aktion Bildschirm ausschalten Herunterfahren Standby-Modus
Aktion bei 'Netzschalter drücken'	Aktion, die durchgeführt wird, wenn der Benutzer den Netzschalter des Computers drückt: Keine Aktion Bildschirm ausschalten Herunterfahren Standby-Modus

¹ab Scout Enterprise 15.9: Standardmäßig wechselt das Gerät nach 20 Minuten in den Standby-Modus (für Hohe Leistung-Profile)

²ab Scout Enterprise 15.9: Standardmäßig wechselt das Gerät nach 20 Minuten in den Standby-Modus (für Hohe Leistung-Profile)

Option	Beschreibung
Aktion bei 'Power/Sleep-Taste drücken' ¹	Aktion, die durchgeführt wird, wenn der Benutzer die Power/Sleep-Taste auf seiner Tastatur drückt (setzt eine entsprechende Tastatur voraus): ² Keine Aktion Herunterfahren Standby-Modus ³



Hinweis

Der Standby-Modus entspricht **Suspend to RAM (S3)**. Für weitere Informationen siehe [Standby-Modus](#).

3. Bestätigen Sie mit **OK**.

¹ab Scout Enterprise 15.8

²ab Scout Enterprise 15.8, früher: Wählen Sie erst im Listenfeld **Profil zur Energieverwaltung** das gewünschte Profil und klicken dann auf **Bearbeiten**.

5.17.2. Arbeitszeiten definieren

– ab Scout Enterprise Management Suite 15.8 –



Voraussetzung

Benutzerrecht **Arbeitszeit definieren**

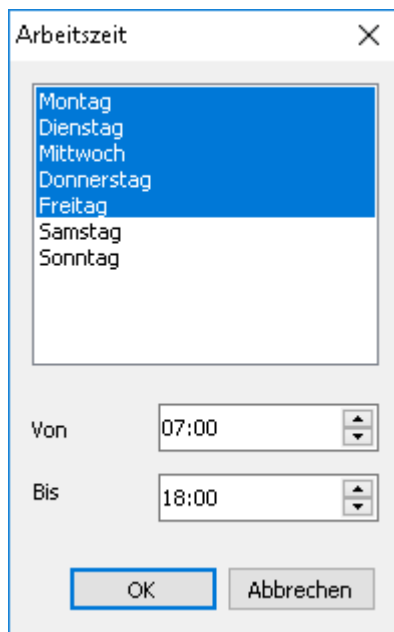
1. Klicken Sie auf dem Register **Energieverwaltung** neben **Arbeitszeiten** auf **Bearbeiten**.
2. Markieren Sie alle Wochentage, die Werktage sind und für die Arbeitszeiten relevant sind. Um mehrere Einträge zu markieren, drücken Sie die UMSCHALT- oder STRG-Taste.
3. Wählen Sie die früheste Uhrzeit für den Arbeitsbeginn (**Von**). Diese Uhrzeit bezieht sich auf alle definierten Werktage.
4. Wählen Sie die späteste Uhrzeit für das Arbeitsende (**Bis**). Diese Uhrzeit bezieht sich auf alle definierten Werktage.

¹ab Scout Enterprise 15.5

²Wenn die Taste nicht vorhanden ist, hat die Konfiguration keine Auswirkung.

³Standard

5. Bestätigen Sie mit **OK**.



Sobald Sie Arbeitszeiten definiert haben, werden die Profile **Hohe Leistung** und **Energie sparen** jeweils in Unterprofile für **Arbeitszeit** und **Außerhalb der Arbeitszeit** aufgeteilt. Das Umschalten zwischen beiden Unterprofilen basiert auf den von Ihnen definierten Arbeitszeiten.

5.17.3. Standby-Modus (Suspend)

– ab Scout Enterprise Management Suite 15.3 und eLux RP 6.3 –

Der Standby-Modus entspricht **Suspend to RAM (S3)**.

Der Benutzer kann sein Gerät mit Hilfe einer Schaltfläche im erweiterten Command panel in den Standby-Modus setzen. Der Standby-Modus kann auch vom System aktiviert werden bei entsprechender Konfiguration der Energieverwaltungs-Optionen.

Wenn das Gerät in den Standby-Modus geht, bleibt der eLux-Benutzer standardmäßig angemeldet. Wenn er das Gerät wieder aktiviert, kann der Benutzer direkt weiterarbeiten. Dies setzt voraus, dass das Backend entsprechend konfiguriert ist: Mit dem Trennen der Anwendungen darf kein automatisches Abmelden des Benutzer erfolgen.

Wenn Sie erreichen möchten, dass sich die Benutzer nach dem Standby-Modus wieder anmelden und neu authentifizieren müssen, verwenden Sie in der **Geräte-Konfiguration > Energieverwaltung** die Option **Benutzer vor Standby-Modus abmelden**.¹ Der Benutzer wird dann abgemeldet und erhält beim Aktivieren des Gerätes aus dem Standby-Modus den eLux-Anmeldedialog.



Hinweis

In der Scout Enterprise-Konsole wird der Status eines Gerätes im Standby-Modus mit **Ausgeschaltet (Suspended)** angezeigt.

¹ab Scout Enterprise 15.8 und eLux RP 6.7

5.18. Problembehandlung Geräte-Konfiguration

Die im folgenden beschriebenen Problemlösungen beziehen sich in erster Linie auf die Scout Enterprise-Konsole.

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.	<p>Verhindern Sie die Registrierung als Eingabekomponenten durch einen Eintrag in der <code>terminal.ini</code>.</p> <p>Die grundsätzliche Funktionalität der Bedienelemente wird dadurch nicht beeinträchtigt.</p> <p>Für weitere Informationen siehe Registrierung von USB-MultiMedia-Komponenten unterdrücken.</p>								
Die Tonwiedergabe von Multimedia-USB-Geräten, die über DisplayPort an eLux RP 5-Geräten mit AMD-Prozessor angeschlossen sind, funktioniert nicht.	Die Tonwiedergabe über DisplayPort ist deaktiviert.	<p>Aktivieren Sie die Tonwiedergabe durch einen Eintrag in der <code>terminal.ini</code>. Verwenden Sie die Funktion Erweiterte Dateieinträge der Scout Enterprise-Konsole:</p> <table><tr><td>Datei</td><td><code>/setup/terminal.ini</code></td></tr><tr><td>Abschnitt</td><td><code>Screen</code></td></tr><tr><td>Eintrag</td><td><code>Radeon.Audio</code></td></tr><tr><td>Wert</td><td><code>true</code></td></tr></table> <p>Alternativ verwenden Sie ein separates Audio-Kabel.</p>	Datei	<code>/setup/terminal.ini</code>	Abschnitt	<code>Screen</code>	Eintrag	<code>Radeon.Audio</code>	Wert	<code>true</code>
Datei	<code>/setup/terminal.ini</code>									
Abschnitt	<code>Screen</code>									
Eintrag	<code>Radeon.Audio</code>									
Wert	<code>true</code>									
Monitor über DisplayPort mit AMD GPU: Nach Ändern auf niedrigere Auflösung bringt der Monitor eine Out of range -Fehlermeldung.	Die Auflösung interferiert auf diesem Monitor mit der konfigurierten Tonwiedergabe über DisplayPort.	<p>Deaktivieren Sie die Tonwiedergabe über DisplayPort. Dadurch wird der Monitor-Fehler korrigiert. Verwenden Sie die Funktion Erweiterte Dateieinträge der Scout Enterprise-Konsole:</p> <table><tr><td>Datei</td><td><code>/setup/terminal.ini</code></td></tr><tr><td>Abschnitt</td><td><code>Screen</code></td></tr><tr><td>Eintrag</td><td><code>Radeon.Audio</code></td></tr><tr><td>Wert</td><td><code>false</code></td></tr></table>	Datei	<code>/setup/terminal.ini</code>	Abschnitt	<code>Screen</code>	Eintrag	<code>Radeon.Audio</code>	Wert	<code>false</code>
Datei	<code>/setup/terminal.ini</code>									
Abschnitt	<code>Screen</code>									
Eintrag	<code>Radeon.Audio</code>									
Wert	<code>false</code>									

Fehler / Problem	Ursache	Lösung								
Bei Verwendung 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 <code>calibrator</code> und starten die Anwendung.								
Nur eLux RP 5.7.x: Im Dual-Monitor-Betrieb , wenn der zweite Monitor auf vertikal konfiguriert ist, werden die Desktop-Symbole nicht (korrekt) angezeigt.	Für manche Auflösungen können bei vertikaler Ausrichtung des zweiten Monitors und Bezug auf den unteren Bildschirmbereich die Desktop-Symbole auf dem Primär-Monitor nicht angezeigt werden.	<div>Ab eLux RP 5.7.3000: Konfigurieren Sie mit Hilfe eines neuen Parameters die vertikale Ausrichtung auf den oberen Bildschirmbereich (<code>top</code>). Verwenden Sie die Funktion Erweiterte Dateieinträge der Scout Enterprise-Konsole:</div> <table><tr><td>Datei</td><td><code>/setup/terminal.ini</code></td></tr><tr><td>Abschnitt</td><td><code>Screen</code></td></tr><tr><td>Eintrag</td><td><code>VerticalAlignment</code></td></tr><tr><td>Wert</td><td><code>top</code></td></tr></table> <div>Standardmäßig steht der Wert auf <code>bottom</code>.</div>	Datei	<code>/setup/terminal.ini</code>	Abschnitt	<code>Screen</code>	Eintrag	<code>VerticalAlignment</code>	Wert	<code>top</code>
Datei	<code>/setup/terminal.ini</code>									
Abschnitt	<code>Screen</code>									
Eintrag	<code>VerticalAlignment</code>									
Wert	<code>top</code>									
Allgemeine 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 Image-definitions-Datei.								

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

²für 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.	<p>Um einzelne Gerätetypen von der Hardwarebeschleunigung auszuschließen², erstellen Sie eine Blacklist, die Sie mit der Scout Enterprise-Funktion Dateien auf die Clients übertragen und lokal speichern:</p> <pre>/setup/hwaccBlacklist</pre> <p>Listen Sie in der Textdatei <code>hwaccBlacklist</code> 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.</p> <p>Beispiel:</p> <pre>FUTRO S920 D3314-B1 HP t620 Dual Core TC</pre> <p>Für alle in der Blacklist aufgeführten Gerätetypen wird die Hardwarebeschleunigung deaktiviert.</p>
AD-Anmeldung an eLux RP 6.x funktioniert nicht.	Port 389 wurde für den Authentifizierungsserver konfiguriert.	Definieren Sie keinen Port für den Authentifizierungsserver.



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.

5.18.1. Registrierung von USB-MultiMedia-Komponenten unterdrücken

Die Registrierung von USB-Geräten als Eingabegeräte kann durch einen Eintrag in der `terminal.ini` verhindert werden.

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Geräte-Konfiguration > Erweiterte Dateieinträge**.
2. Definieren Sie folgenden Eintrag:

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

²für eLux RP 5.6 und spätere Versionen

Datei	/setup/terminal.ini
Abschnitt	Xorg
Eintrag	IgnoreUsbInput
Wert (VendorID) oder	<p>VendorID_1:ProdID_1,VendorID_2:ProdID_2 Beispiel: 0b0e:034c,047f:c01e</p> <p>Achtung: Verwenden Sie für die Hexadezimalwerte nur Kleinbuchstaben!</p> <p>Einzelne Zeichen können Sie durch das Wildcard-Zeichen ? ersetzen.¹ Beispiel: 0b0e:???? filtert auf alle Produkte eines Vendors.</p>
Wert (VendorName)	<p>Alternativ zur VendorID können Sie auf den Vendor-Namen filtern:² Beispiel: Jabra,Netcom</p> <ul style="list-style-type: none"> • Leerzeichen oder Schrägstriche im Vendor-Namen müssen durch einen Unterstrich _ ersetzt werden. • Der Vendor-Name kann als Kurzform angegeben werden. Beispiel: Netcom findet GN Netcom und GN Netcom A/S. • Vendor-Namen können ODER-verknüpft werden: Beispiel: Jabra Sennheiser <p>Hinweis: Um Vendor-Namen oder IDs zu ermitteln, verwenden Sie folgenden Befehl:</p> <pre>udevadm info --export-db grep -Ew "(NAME ID_VENDOR)"</pre>

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).



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.

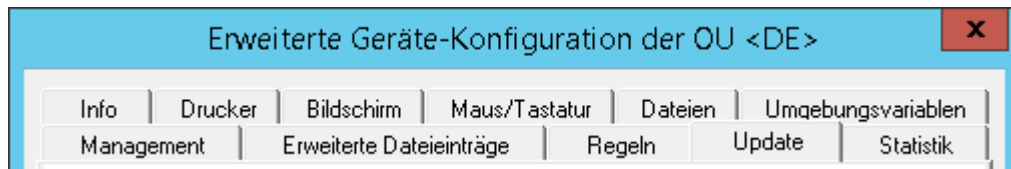
¹ab eLux RP 6.3 und eLux RP 5.7.2000

²ab eLux RP 6.2 und eLux RP 5.7.2000

6. Erweiterte Geräte-Konfiguration und Erweiterte Optionen

Die Einstellungen der Geräte-Konfiguration, die Sie entweder global in **Optionen > Basis-Geräte-Konfiguration** oder in der Geräte-Konfiguration für bestimmte OUs bzw. Geräte festgelegt haben, können Sie folgendermaßen ergänzen:

- Optionen für einzelne Geräte oder OUs in der **Erweiterten Geräte-Konfiguration**¹ überschreiben und ergänzen



Die **Erweiterte Geräte-Konfiguration** wird auf OU- oder Geräte-Ebene angewendet.

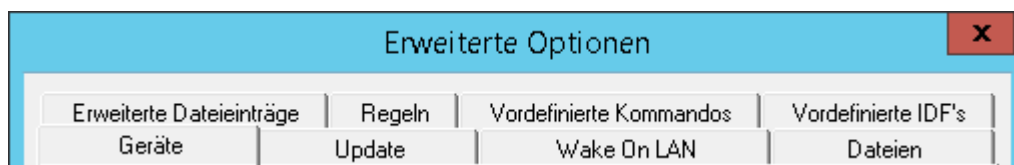
- ▶ Öffnen Sie das Kontextmenü für die relevante OU oder Gerät und wählen Sie den Eintrag **Erweiterte Geräte-Konfiguration...**²



Hinweis

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

- Weitere Optionen im Dialog **Erweitere Optionen** auf alle Geräte anwenden



Die **Erweitere Optionen** werden auf alle Geräte angewendet.

- ▶ Wählen Sie im Scout Enterprise-Menü **Optionen > Erweiterte Optionen**.

Manche Funktionen wie **Dateien** (Konfigurierte Dateiübertragung), **Erweiterte Dateieinträge** und **Update**-Optionen befinden sich in beiden Dialogen. Verwenden Sie die **Erweiterte Geräte-Konfiguration...**, um die Funktion auf bestimmte Geräte anzuwenden. Verwenden Sie die **Erweitere Optionen**, um die Funktion auf alle Geräte anzuwenden.

¹früher: Erweiterte Einstellungen

²früher: Erweiterte Einstellungen

6.1. Geräte

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

Option	Beschreibung
Maximale Pingzeit (Millisekunden)	Maximale Antwortzeit des Clients auf einen <code>ping</code> -Befehl
Maximale Suchzeit (Sekunden)	Maximale Gesamtdauer für die zu suchenden Geräte, bis Discovery abgebrochen wird.
Lokale Konfiguration (nicht-gesperrte Felder) beibehalten ¹	<p>Nicht gesperrte Felder der Geräte-Konfiguration sind zur lokalen Benutzerkonfiguration freigegeben und werden nicht von Scout Enterprise überschrieben. Beim nächsten Laden der Konfiguration werden nur die gesperrten Felder aktualisiert (Geräte-Konfiguration > Register Sicherheit).</p> <p>Die Werte der erlaubten Felder können auch dann erhalten werden, wenn der Client auf den Grundzustand gesetzt wird.²</p> <p>Für weitere Informationen siehe Lokale Konfiguration schützen.</p>



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 [Lokale Konfiguration schützen](#).

Standard-OU	OU, in die neue Geräte standardmäßig eingeordnet werden
OU von Geräten durch OU-Filter zuweisen	<p>Aktiviert den OU-Filter für neue Geräte</p> <p>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.</p>
Konfigurationstransfer für neue Geräte sperren	Die Konfiguration für neue Geräte wird nicht aktualisiert, solange die Kontextmenü-Option Konfigurationstransfer gesperrt ist.
Automatischen OU-Wechsel von Geräten erlauben	Erlaubt die automatische Zuordnung von Geräten über DHCP

¹früher: Nur gesperrte Felder werden am Client aktualisiert

²ab Scout Enterprise 15.7 und eLux RP 6.7

Nur bekannte Geräte akzeptieren	Der Scout Enterprise-Server nimmt nur neue Geräte mit bekannter MAC-Adresse an. Für weitere Informationen siehe Geräteprofil reservieren .
Hostnamen des Gerätes 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 Geräte-Konfiguration > Management)
Namensschablone nur für neue Geräte anwenden	Namensschablone wird nicht beim Verschieben oder Umziehen von Geräten angewendet

6.2. Update/Auslieferung

– nicht für einzelne Geräte verfügbar –

Option	Beschreibung
Maximale Anzahl paralleler Updates oder Auslieferungen	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 System-spezifisch.

6.3. Management

– nur für einzelne Geräte und OUs verfügbar –

Option	Beschreibung
Hinweis	Freitext-Feld für interne Kommentare Kann im Eigenschaften -Fenster angezeigt werden

Option	Beschreibung
Sichtbarkeit – nur für OUs –	Die Sichtbarkeit bezieht sich auf die Liste der OUs, die ein neuer Client bei der Verbindung zum Scout Enterprise-Server anfordert, um eine OU auszuwählen. Eine ausgeblendete OU wird in der Liste nicht angezeigt. Eine eingeblendete OU kann in der Liste ausgewählt und kann durch Kennwort geschützt werden.
Eintragung neuer Geräte – nur für OUs –	Bei der automatischen Geräteerfassung können neu hinzugefügte Geräte einer vordefinierten Namensschablone unterworfen werden. Die globalen Funktionen für Gerätenamen in den Erweiterten Optionen befinden sich im Register Geräte . Für weitere Informationen siehe Geräte .
OU-Filter ignorieren – nur für einzelne Geräte –	Wenn der OU-Filter eingeschaltet ist (Erweiterte Optionen > Geräte), werden neue Geräte gemäß den gesetzten Kriterien OUs zugeordnet. Einzelne Geräte können vom OU-Filter ausgenommen werden. Das Verschieben von Geräten innerhalb der Baumstruktur aktiviert die Option automatisch.

6.4. Vordefinierte IDF's und Container

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

Über vordefinierte IDF-Dateien und Container-Pfade können Sie die erlaubten Parameter für Firmware-Updates, die von operativen Administratoren ausgeführt werden, einschränken.



Hinweis

Zur sinnvollen Nutzung dieser Funktionen konfigurieren Sie die Objektrechte in der Administratorenverwaltung entsprechend. Für weitere Informationen siehe [Auswahl der Imagedefinitions-Datei](#).

Vordefinierte IDF's

Mit dieser Funktion beschränken Sie die Auswahl gültiger IDF-Dateien im **Firmware**-Register der Geräte-Konfiguration.

Option	Beschreibung
Image-Name	Zeigt alle IDF-Dateien, die in der aktuellen Client-Infrastruktur über alle Clients bereits verwendet wurden (alle IDF's, die in der Scout Enterprise-Datenbank verfügbar sind)
Gültig	Legt fest, ob die IDF-Datei im Firmware -Register im Feld Image-Datei angeboten wird
Verwendet	Zeigt die Anzahl der Clients, die das Image verwenden
Zugewiesen	Zeigt die Anzahl der Clients, denen das Image zugewiesen wurde

Option	Beschreibung
Hinzufügen	Erzeugt einen neuen Listeneintrag für eine neue IDF-Datei Bearbeiten Sie den Eintrag anschließend.
Löschen	Löscht die markierte IDF-Datei

Zusätzlich zu den vordefinierten Einträgen im Feld **Image-Datei** der Geräte-Konfiguration kann ein Administrator neue Einträge (IDF-Dateien) als Freitext hinzufügen, wenn er über das entsprechende Objektrecht verfügt.

Für weitere Informationen siehe [Auswahl der Imagedefinitions-Datei](#).

Vordefinierte Container

Um festzulegen, dass operative Administratoren für Firmware-Updates nur auf den definierten Web-Server zugreifen können, beschränken Sie den Container-Pfad im **Firmware**-Register der Geräte-Konfiguration.

Option	Beschreibung
Pfad-Name	Zeigt die bereits hinzugefügten Container-Pfade
Gültig	Legt fest, ob der Pfad im Firmware -Register im Feld Pfad angeboten wird
Hinzufügen	Erzeugt einen neuen Listeneintrag, den Sie anschließend bearbeiten
Löschen	Löscht den markierten Pfad

6.5. Vordefinierte Kommandos

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

Benutzerdefinierte Kommandos können zentral vordefiniert und den Administratoren zur Fernverwaltung als fertige Kommandos zur Verfügung gestellt werden.

Aktive vordefinierte Kommandos werden unter **Kommandos > Vordefiniertes Kommando...** im Listenfeld **Auswahl** angezeigt und können auf einzelne Geräte, auf OUs oder auf Dynamische Gerätegruppen angewendet werden.

Zusätzlich können für Standard-Kommandos Voreinstellungen definiert werden.

Für weitere Informationen zur Definition siehe [Vordefinierte Kommandos](#).

6.6. 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, 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 Verwendung einer IP-Broadcastadresse für das Subnetz muss als globale Einstellung konfiguriert werden.

Erweiterte Optionen

Erweiterte Dateieinträge | Regeln | Vordefinierte Kommandos | Vordefinierte IDF's

Geräte | Update | Wake On LAN | Dateien

Subnetzmaske oder Servername
/255.255.255.0

Protokolleinstellungen

☒ Eine IP-Broadcastadresse für das Subnetz generieren

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 in den Erweiterten Optionen)	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.

6.7. VPN

– nur für einzelne Geräte verfügbar –



Hinweis

Das Register **VPN** ist nur in der **Erweiterten Geräte-Konfiguration** 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
- 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.

6.7.1. Cisco AnyConnect einrichten



Hinweis

Bis eLux RP 5.7 und eLux RP 6.5 muss das eLux-Paket **VPN System** und das hierin enthaltene Feature-Paket **Cisco AnyConnect** auf den Clients installiert sein.

Ab eLux RP 6.6 muss das eLux-Paket **Cisco AnyConnect** auf den Clients installiert sein.

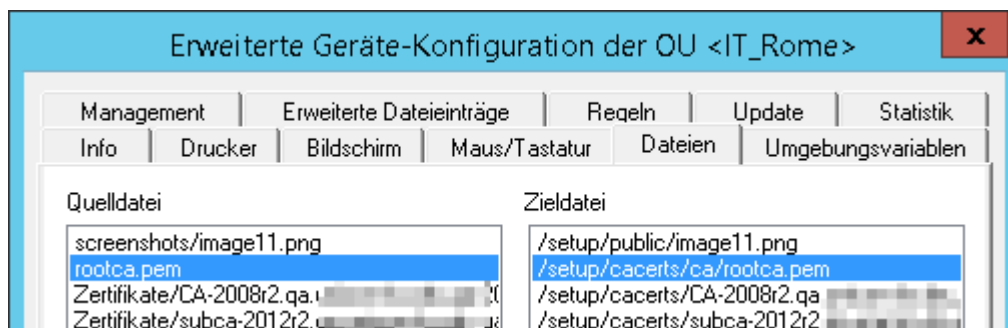
Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Übertragen Sie das Root-Zertifikat auf die Clients nach `/setup/cacerts/ca`. Wenn Sie die Scout Enterprise-Funktion **Konfigurierte Dateiübertragung** verwenden, tragen Sie die Zielfeld mit Zielpfad `/setup/cacerts/ca` ein.



Hinweis

Cisco AnyConnect akzeptiert nur Zertifikatsdateien im Format `.pem`.

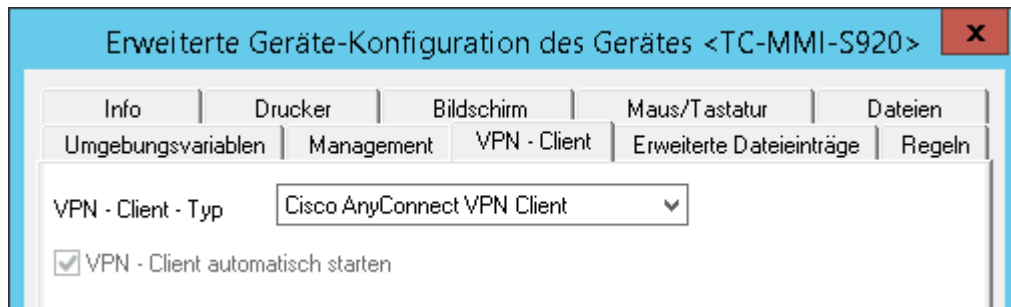




Hinweis

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

2. Öffnen Sie in der Scout Enterprise-Konsole für das relevante Gerät **Erweiterte Geräte-Konfiguration¹ > VPN-Client** und wählen `Cisco AnyConnect VPN Client` aus dem Listenfeld.



3. Führen Sie einen Neustart am Client durch. Möglicherweise benötigt der Client einen weiteren Neustart, um die VPN-Konfiguration lokal zu aktivieren.

Konfigurationsdatei

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/.cisco/profile/2` übertragen. Hier können Sie beispielsweise die Server-Adresse des Backends konfigurieren.

6.7.2. OpenVPN einrichten



Hinweis

Bis eLux RP 5.7 und eLux RP 6.5 muss das eLux-Paket **VPN System** und das hierin enthaltene Feature-Paket **OpenVPN** auf den Clients installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

Ab eLux RP 6.6 ist **OpenVPN** integraler Bestandteil des eLux-Betriebssystems.

1. Übertragen Sie die `.ovpn`-Konfigurationsdatei und die Zertifikate auf die Clients nach `/setup/openvpn`. Wenn Sie die Scout Enterprise-Funktion **Konfigurierte Datei-übertragung** verwenden, tragen Sie Quelldatei und Zieldatei **mit** Dateierweiterung und den Zielpfad `/setup/openvpn` ein. Wenn Sie per USB-Stick übertragen, entpacken Sie die `.zip`-Datei im Zielverzeichnis `/setup/openvpn`.
2. Öffnen Sie in der Scout Enterprise-Konsole für das relevante Gerät **Erweiterte Geräte-**

¹früher: Erweiterte Einstellungen

²ab eLux RP 6.4. Für frühere Versionen: `/setup/elux/.anyconnect`

Konfiguration¹ > VPN-Client und wählen **OpenVPN Client**.

Erweiterte Geräte-Konfiguration des Gerätes <TC-MMI-S920>

Info | Drucker | Bildschirm | Maus/Tastatur | Dateien

Umgebungsvariablen | Management | **VPN - Client** | Erweiterte Dateieinträge | Regeln

VPN - Client - Typ: OpenVPN

☒ VPN - Client automatisch starten

Konfiguration: openvpn_TC-STec4-03

3. Aktivieren Sie die Option **VPN-Client automatisch starten**.
4. Fügen Sie im Feld **Konfiguration** den Namen der OpenVPN-Konfigurationsdatei **ohne** die Dateierweiterung `.ovpn` ein.

Nach dem nächsten Geräte-Neustart wird die VPN-Konfigurationsdatei auf das Gerät übertragen und mit einem weiteren Neustart aktiviert. Der OpenVPN-Anmeldedialog wird angezeigt und der Benutzer kann sich verbinden.



Hinweis

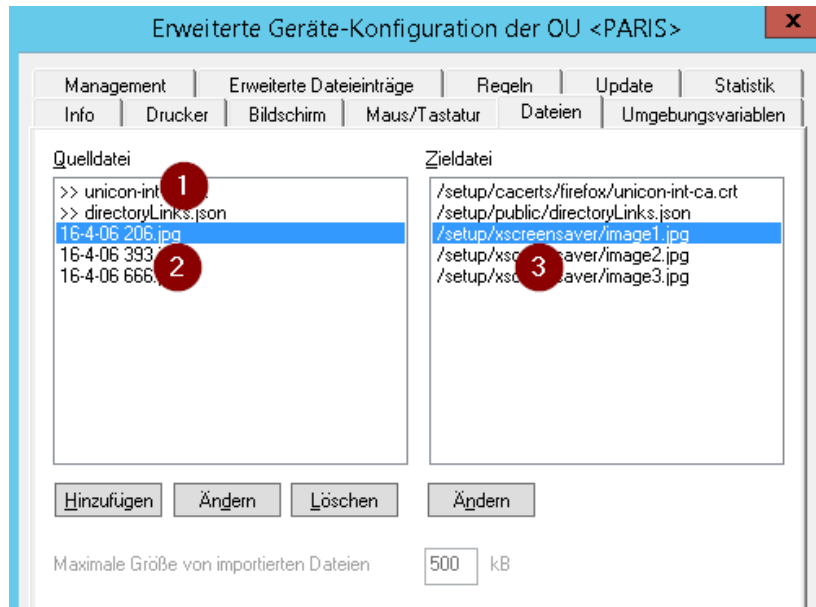
Der OpenVPN-Client kann unter eLux nur mit einer validen `.ovpn`-Konfigurationsdatei verwendet werden. Achten Sie auf korrekte Konfigurationseinträge. eLux akzeptiert das Setzen einer weiteren Default-Route über die `.ovpn`-Konfigurationsdatei nicht. Manche Firewall-Hersteller bieten unterschiedliche Konfigurationsdateien für verschiedene Betriebssysteme mit und ohne Default-Route an. Beispielsweise enthält die Sophos-Konfigurationsdatei für Android/iOS diese Default-Route nicht und kann für eLux verwendet werden.

¹früher: Erweiterte Einstellungen

6.8. 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 werden in die Scout Enterprise-Datenbank importiert¹ und werden automatisch mit dem SQL-Datenbank-Backup gesichert.



Legende

- 1 Einträge aus einer übergeordneten OU oder aus der globalen Dateiliste werden durch das Zeichen >> gekennzeichnet.²

Um die Herkunft anzuzeigen, zeigen Sie mit dem Mauszeiger über den Eintrag.

- 2 Die Quelldateien wurden aus dem Dateisystem ausgewählt.

- 3 Für die Zielfile definieren Sie das relevante Verzeichnis auf dem Client und optional einen abweichenden Dateinamen.

Beispiel: Bilddateien werden als Bildschirmschoner auf die Clients kopiert.

Dateien für den Transfer definieren

1. Wenn Sie Dateien für alle Geräte definieren möchten (globale Dateiliste), wählen Sie **Optionen > Erweiterte Optionen**. Auf dieser Ebene können Sie auch Zielfilevorlagen erstellen, die auf den unteren Ebenen genutzt werden sollen.

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 den Eintrag **Erweiterte Geräte-Konfiguration...**³


¹Bis Scout Enterprise Management Suite 15.1 können alternativ Dateien im Dateisystem referenziert werden.

²ab Scout Enterprise Management Suite 15.4

³früher Erweiterte Einstellungen

**Hinweis**

Eine individuelle Dateiliste dominiert die globale Dateiliste.

2. Wählen Sie das Register **Dateien** und klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Um die Quelldatei aus dem Dateisystem auszuwählen, klicken Sie im Dialog **Dateien hinzufügen** auf die Schaltfläche ¹.

*Ein neuer Eintrag wird für die Listen **Quelldatei** und **Zieldatei** angelegt.*

4. Passen Sie unter **Zieldatei** den Pfad und Dateinamen für die Zielposition am Client an. Der Dateiname auf dem Thin Client muss nicht mit dem der Quelldatei identisch sein.

Wenn konfiguriert, wählen Sie alternativ eine Zieldateivorlage aus dem Listenfeld **Vorlage**. Pfad und Dateiname der Zieldatei können dann nicht mehr geändert werden.

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

Quelle und Ziel sind definiert. Der Dateitransfer erfolgt beim nächsten Startvorgang der Clients. Ein erneuter Dateitransfer erfolgt nur dann, wenn Sie die Konfiguration ändern.

Importierte Quelldateien wiederverwenden

Bereits importierte Quelldateien können Sie für den Dateitransfer in anderen OUs wiederverwenden.

1. In der Erweiterten Geräte-Konfiguration der Quell-OU im Register **Dateien** klicken Sie mit der rechten Maustaste auf den relevanten Eintrag in der Liste **Quelldatei**.
2. Um den Eintrag in den Zwischenspeicher zu kopieren, wählen Sie im Kontextmenü die Option **Kopieren**.
3. Öffnen Sie die Erweiterte Geräte-Konfiguration der Ziel-OU und das Register **Dateien**.
4. Klicken Sie mit der rechten Maustaste in die Liste **Quelldatei** und wählen Sie im Kontextmenü die Option **Einfügen**.

Übertragene Dateien löschen

Auf den Client übertragene Dateien können Sie mit der Funktion **Konfigurierte Dateiübertragung** nicht entfernen.

- Um alle übertragenen Dateien zu entfernen, setzen Sie den Client in den Grundzustand.

¹Bis Scout Enterprise Management Suite 15.1 aktivieren Sie außerdem unter **Quelldatei** die Option **Datei in Datenbank importieren**.

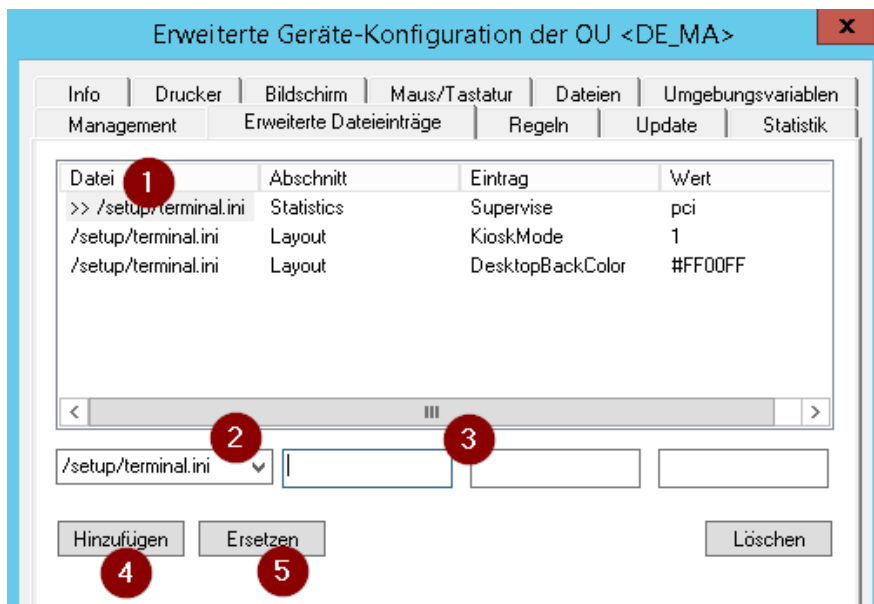
6.9. Erweiterte Dateieinträge

Mit Hilfe des Registers **Erweiterte Dateieinträge** können Sie Parameter in `.ini`-Dateien definieren, die nicht über die graphische Oberfläche gesetzt werden können, beispielsweise zusätzliche Layout-Parameter.

Für die `.ini`-Dateien gilt folgendes:

- Eine `.ini`-Datei besteht aus mindestens einem Abschnitt. Jeder Abschnitt besteht aus null oder mehreren Schlüsselwörtern. Den Schlüsselwörtern sind null oder mehrere Werte zugeordnet.
- Ein Abschnitt wird durch einen symbolischen Namen in eckigen Klammern eingeleitet.
- Jedes Schlüsselwort und der zugehörige Wert stehen in 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.

6.9.1. Individuelle Dateieinträge hinzufügen



Legende

- 1 Einträge aus einer übergeordneten OU oder aus den globalen **Erweiterten Optionen** werden durch das Zeichen >> gekennzeichnet.¹
Um die Herkunft anzuzeigen, zeigen Sie mit dem Mauszeiger über den Eintrag.
- 2 Für einen neuen Eintrag wählen Sie die relevante Datei aus oder geben Pfad und Dateinamen ein.
- 3 Für den neuen Eintrag legen Sie anschließend Abschnitt, Eintrag und Wert fest.
- 4 Mit **Hinzufügen** übernehmen Sie den neuen Eintrag.
- 5 Mit **Ersetzen** übernehmen Sie den neuen Eintrag **und** ersetzen den in der Liste markierten Eintrag.

1. Wählen Sie in der Scout Enterprise-Konsole **Optionen > Erweiterte Optionen**.
Oder:
Öffnen Sie für die relevante OU das Kontextmenü und wählen Sie **Erweiterte Geräte-Konfiguration...**²
2. Wählen Sie das Register **Erweiterte Dateieinträge**.
3. Bearbeiten Sie die Felder unter der Liste:

¹ab Scout Enterprise Management Suite 15.4

²früher: Erweiterte Einstellungen

Option	Beschreibung
Datei	Tragen Sie den vollständigen Pfad und Namen der zu bearbeitenden Datei ein oder wählen Sie aus der Dropdown-Liste: Terminal: /setup/terminal.ini Citrix: /setup/ica/wfclient.ini und /setup/ica/appsrv.ini Cisco VPN: /setup/ciscovpn/sample.pcf
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**.
5. Bestätigen Sie mit **Übernehmen** und **OK**.

Die neuen Einträge werden beim nächsten Neustart in die .ini-Datei der Clients geschrieben.

6.9.2. 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 vorhandenen Wert.
3. Klicken Sie auf **Ersetzen**.

Die neuen Werte werden beim nächsten Neustart in die .ini-Datei des Clients geschrieben.

6.9.3. 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.

6.9.4. 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.

6.10. 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 Listefeld Für OUs und Geräte ist die Option <code>Übergeordnete Aktion verwenden</code> standardmäßig aktiv.
Am Gerät eine Meldung für <x> Sekunden einblenden	Geben Sie eine Zeitspanne in Sekunden ein, um den Benutzer zu informieren
Beim ersten Kontakt mit dem Manager folgende Aktion durchführen	Wählen Sie <code>Update durchführen</code> , um sicherzustellen, dass neue Geräte sofort auf dem aktuellen Software-Stand sind

Sonderfall Kiosk-Modus

Wenn Sie den Browser im Kiosk-Modus einsetzen um auf Citrix-Anwendungen zuzugreifen, greift die Option **Nach dem Beenden der letzten Anwendung folgende Aktion durchführen** nicht. In diesem Fall haben Sie die Möglichkeit einen Eintrag in der `terminal.ini`-Datei zu setzen, der die Aktion festlegt, die nach dem Schließen der letzten Citrix-Anwendung ausgeführt werden soll.¹

- Definieren Sie mit Hilfe der Scout Enterprise-Funktion [Erweiterte Dateieinträge](#) folgenden Eintrag:

Datei	/setup/terminal.ini	
Abschnitt	Global	
Eintrag	ActionAfterLastWfica	
Wert	0	Use parent action
	1	Restart
	2	Shutdown
	4	Logoff
	8	Lock
	16	VPN disconnected

¹ab eLux RP 5.7 und eLux RP 6.2

6.11. Umgebungsvariablen

– nur für einzelne Geräte und OUs verfügbar –

Umgebungsvariablen können lokal am Client eingesetzt werden und enthalten Zeichenketten.

Umgebungsvariable definieren

1. Wählen Sie in der **Erweiterte Geräte-Konfiguration...**¹ das Register **Umgebungsvariablen**.
*Die Liste zeigt bereits definierte Variablen. Einträge aus einer übergeordneten OU werden durch das Zeichen >> gekennzeichnet.*²
2. Klicken Sie auf die Schaltfläche **Neu**.
3. Geben Sie eine Variable in folgendem Format ein:
`Variablenname=Wert`
und bestätigen Sie mit **OK**.
Die neue Variable wird in der Liste angezeigt.
4. 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>`.

¹früher: Erweiterte Einstellungen

²ab Scout Enterprise Management Suite 15.4

6.12. TPM 2.0-Unterstützung

– ab eLux RP 6.7 –

Ein im Thin Client verbauter TPM 2.0-Chip kann für grundlegende Sicherheitsfunktionen verwendet werden:

- **Verschlüsselung der Setup-Partition**

Die Setup-Partition auf dem Flash-Speicher des Thin Clients enthält Gerätekonfiguration, Anwendungsdefinitionen und dient als Speicherort für Zertifikate. Diese Daten können Sie über das TPM 2.0-Modul verschlüsseln.

- **Speichern des privaten Schlüssels für SCEP Client-Zertifikate im TPM 2.0-Modul**

Wenn Sie SCEP einsetzen, wird der private Schlüssel auf Geräten mit TPM 2.0 standardmäßig im TPM 2.0-Modul gespeichert. Für weitere Informationen siehe [Zertifikate für SCEP](#) in der Kurzanleitung **IEEE 802.1X-Authentifizierung mit Unterstützung von SCEP**.

Setup-Partition über TPM 2.0 verschlüsseln

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Geräte die **Erweiterte Konfiguration > Erweiterte Dateieinträge**.
2. Definieren Sie folgenden Eintrag:

Datei	/setup/terminal.ini		
Abschnitt	Security		
Eintrag	CryptSetupPartition		
Wert	true	Standardmäßig steht der Wert auf false.	

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

Sobald die neue Konfiguration aktiv ist, erfolgt die Verschlüsselung automatisch mit dem nächsten Neustart der Clients. Der hierfür relevante Schlüssel ist im TPM 2.0-Modul gespeichert.

Bei Thin Clients ohne TPM 2.0-Modul hat der Konfigurationsparameter keine Auswirkung.

Wenn neue Clients mit TPM 2.0-Chip in die Scout Enterprise-Verwaltung aufgenommen werden (Onboarding) und die Ziel-OU ist mit `CryptSetupPartition` konfiguriert, ist sichergestellt, dass die in der Scout Enterprise-Konsole hinterlegten Konfigurationsdaten erst nach der Verschlüsselung der Setup-Partition lokal am Thin Client gespeichert werden.



Hinweis

Ob die Setup-Partition eines Gerätes verschlüsselt ist, kann in im Eigenschaften-Fenster eines Gerätes angezeigt werden.

Verschlüsselung der Setup-Partition über TPM 2.0 aufheben

- ▶ Setzen Sie den erweiterten Dateieintrag `CryptSetupPartition` auf den Wert `false`.
oder
- ▶ Setzen Sie die Geräte zurück auf den Grundzustand. Verwenden Sie dazu das Kommando **Grundzustand** mit der Option **Scout Enterprise Server-Adresse am Client löschen**.



Hinweis

Ein Downgrade auf eine eLux-Version ohne TPM 2.0-Unterstützung ist nur mit unverschlüsselter Setup-Partition möglich.

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 [Image erstellen](#) im **ELIAS 18-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

Für weitere Informationen über Regeln, die beim Schließen der letzten Anwendung ausgeführt werden, siehe [Regeln](#).

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 <code>\$ELUXUSER</code> , <code>\$ELUXPASSWORD</code> und <code>\$ELUXDOMAIN</code> 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.*

¹ab Scout Enterprise Management Suite Version 14.7



Hinweis

Die Eigenschaften einer markierten Anwendung können Sie in der Scout Enterprise-Konsole im **Eigenschaften-Fenster (Ansicht > Fenster > Eigenschaften)** anzeigen, aber nicht bearbeiten.

Für jeden Administrator können die Objektrechte auf einzelne Anwendungstypen gesteuert werden.¹ Die erweiterten Einstellungen und die freien Parameter können getrennt berechtigt werden.

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.

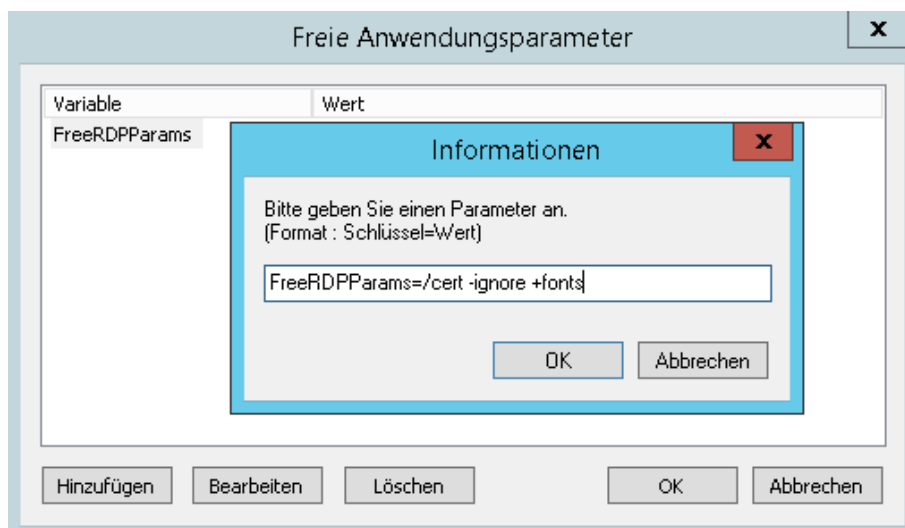
1. Öffnen Sie die **Anwendungseigenschaften** der relevanten Anwendung.
2. Klicken Sie auf die Schaltfläche **Freie Parameter**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie einen oder mehrere Parameter in folgendem Format ein.

```
FreeRDPPParams=<Parameter> <Parameter> <Parameter>...
```

Trennen Sie mehrere Parameter durch Leerzeichen.

4. Bestätigen Sie zweimal mit **OK**.

Scout Enterprise speichert die definierten Parameter mit der Anwendungsdefinition. Die Parameter werden in die `\setup\sessions.ini`-Datei für die entsprechende Anwendung eingefügt.



Hinweis

Der Zugriff auf die freien Parameter kann über die Objektrechte eingeschränkt werden.²

¹ab Scout Enterprise Management Suite Version 15.5

²ab Scout Enterprise Management Suite Version 15.5

Welche Parameter zur Verfügung stehen, entnehmen Sie der Beschreibung der jeweiligen Anwendungsdefinition.

Folgende Parameter können Anwendungs-übergreifend verwendet werden:

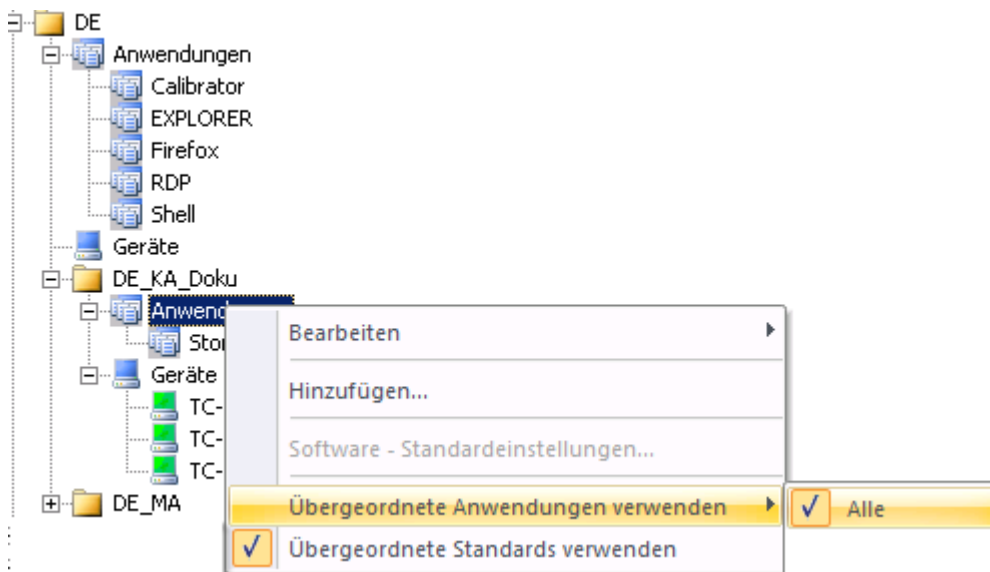
Parameter	Werte	Beschreibung
pinned ¹	true	Die Anwendung wird auf der Systemleiste angeheftet.

¹ab eLux RP 6.8

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.



Hinweis

Die Vererbung der ausgewählten Anwendungen geht verloren, wenn Sie die OU in eine andere übergeordnete OU verschieben.

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*.

OU Geräte/Anwendungen				
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. Vorlagen für Anwendungen definieren

– ab Scout Enterprise 15.7 –

Als Administrator können Sie für jeden Anwendungstyp eine Vorlage erstellen, beispielsweise eine Browser-Vorlage: In der Vorlage geben Sie Werte vor, die die Benutzer beim Erstellen einer Browser-Anwendung ausgefüllt vorfinden sollen. Wenn Sie in Ihrer Browser-Vorlage den Browser-Typ `Firefox` und als `Proxy System-Proxy` vorgeben, sind in der Folge für alle Benutzer auf allen Ebenen `Firefox` und `System-Proxy` bereits gesetzt, wenn sie eine neue Browser-Anwendung erstellen.

Die vordefinierten Werte können überschrieben werden. Wenn Sie die Objektrechte für die erweiterten Einstellungen oder freien Parameter eines Anwendungstyps deaktivieren, bleiben diese Werte jedoch bestehen, da für die relevanten Benutzer bei der Anwendungsdefinition kein Zugriff darauf besteht.


Anwendungs-Vorlagen werden auf der obersten Ebene definiert. Für jeden Anwendungstyp kann genau eine Vorlage definiert werden.

Anwendungsvorlage erstellen




Voraussetzung

Administratoren-Basisrecht: `Basis-Anwendungen` bearbeiten

1. Klicken Sie in der Organisationsstruktur auf der obersten Ebene mit der rechten Maustaste auf  **Anwendungen**.
2. Wählen Sie im Kontextmenü **Anwendungsvorlagen definieren...**
*Der Dialog **Definition von Anwendungsvorlagen** öffnet. Jedes Register enthält die Anwendungseigenschaften eines Anwendungstyps.*
3. Wechseln Sie zu dem Register, das den gewünschten Anwendungstyp enthält.
4. Bearbeiten Sie alle Optionen, die Sie vordefinieren möchten.
5. Bestätigen Sie mit **Übernehmen** und **OK**.

Jede neue Anwendungsdefinition für diesen Anwendungstyp enthält die vordefinierten Werte.


Anwendungsvorlage bearbeiten oder zurücksetzen

1. Klicken Sie in der Organisationsstruktur auf der obersten Ebene mit der rechten Maustaste auf  **Anwendungen** und wählen Sie **Anwendungs-Vorlagen definieren...**
*Der Dialog **Definition von Anwendungsvorlagen** enthält für jeden Anwendungstyp ein Register mit den Anwendungseigenschaften. Nicht-leere Felder enthalten Werte, die bei der Erstellung von neuen Anwendungen dieses Typs übernommen werden.*
2. Bearbeiten Sie für den relevanten Anwendungstyp die Optionen, die Sie ändern möchten.
3. Um alle von Ihnen vordefinierten Werte für einen Anwendungstyp zu entfernen, klicken Sie auf **Zurücksetzen**.

7.1.6. 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**.

7.1.7. 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.



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.

¹ab Scout Enterprise Management Suite Version 15.0

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.

7.1.8. Anwendungssymbol definieren

Sie können eigene Anwendungssymbole definieren, um sie am Client-Desktop anzuzeigen. Als Grafikdateien werden ab Scout Enterprise Management Suite 15.2 hochauflösende Formate vom Typ `.svg` und `.png` unterstützt. Diese lösen die Bitmap-Formate `.xpm`, `.ico` und `.gif` ab, die bis Scout Enterprise Management Suite 15.1 verwendet werden konnten.

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.

7.1.9. 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.

7.1.10. Service-App definieren

– ab eLux RP 6.4 –



Hinweis

Die Benutzer-Authentifizierung über Active Directory muss konfiguriert sein.

Wenn Sie AD einsetzen, können Sie den Benutzern die Möglichkeit geben, eLux ohne Anmeldung im Service-Modus zu starten. Der AD-Anmelde-Dialog bietet dann eine zusätzliche **Service**-Schaltfläche, die eLux in einem geschütztem Modus (Service-Modus) startet. Im Service-Modus bietet eLux nur die definierten Service-Apps auf dem Desktop. Im Configuration panel ist nur der Dialog **Information** sichtbar.

Sie können eine oder mehrere Service-Apps definieren.

1. Um eine Service-App zu definieren, öffnen Sie die **Anwendungseigenschaften** der relevanten Anwendung.
2. Klicken Sie auf **Freie Parameter** und fügen Sie folgenden Parameter hinzu:

```
ServiceApp=true
```

3. Bestätigen Sie die Änderung.

*Nachdem der Parameter zum Client übertragen wurde, enthält der AD-Anmelde-Dialog eine Schaltfläche **Service**.*



7.1.11. Anwendung auf eine Anmelde-Domäne begrenzen

– ab eLux RP 6.4 –



Hinweis

Die Benutzer-Authentifizierung über Active Directory muss konfiguriert sein.

Wenn die Benutzer sich an mehreren AD-Domänen anmelden können, kann die Anzeige einer Anwendung auf eine bestimmte Domäne begrenzt werden. Diese Option wird über einen freien Parameter in der Anwendungsdefinition gesetzt.

1. Öffnen Sie die **Anwendungseigenschaften** der relevanten Anwendung.
2. Klicken Sie auf **Freie Parameter** und fügen Sie folgenden Parameter hinzu:

```
ShowInDomain=<AD-Anmelde-Domäne>
```

Die AD-Anmelde-Domäne kann eine der Domänen sein, die in der Geräte-Konfiguration unter **Sicherheit > Benutzer-Authentifizierung > AD-Verzeichnis** angegeben sind.

Beispiel:

`int.sampletec-01.com`

3. Bestätigen Sie die Änderung.

Nachdem der Parameter zum Client übertragen wurde, wird die relevante Anwendung nur angezeigt, wenn der Benutzer sich an der angegebenen AD-Domäne anmeldet.

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 Anwendungstyp **ICA** ist veraltet und wird nur bis XenApp 6.x von Citrix unterstützt.

Voraussetzungen

- Das Software-Paket **Citrix Workspace app for Linux** oder **Citrix Receiver for Linux** muss auf den Clients installiert sein.
- Für eine Verbindung via HTTPS beim Anwendungstyp **Storefront**, **Self Service** und **PNagent** müssen die entsprechenden Root- und Intermediate-Zertifikate auf den Clients vorhanden sein.
 - Root-Zertifikate müssen nach `/setup/cacerts` übertragen werden.
 - Intermediate-Zertifikate müssen nach `/setup/cacerts/intcerts` übertragen werden.

Für weitere Informationen zur Konfiguration der Zertifikate siehe [Zertifikate](#).

- Für eine Verbindung via HTTPS beim Anwendungstyp **Browser** müssen die entsprechenden Root- und Intermediate-Zertifikate auf den Clients vorhanden sein.
 - Firefox: Root-Zertifikate und Intermediate-Zertifikate müssen nach `/setup/cacerts/firefox` übertragen werden.
 - Chromium: Root-Zertifikate und Intermediate-Zertifikate 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 Anwendungstyp **StoreFront** können sich Benutzer zu einem Citrix 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.

Die Citrix-Ressourcen eines oder mehrerer Stores können gemeinsam mit anderen konfigurierten eLux-Anwendungen wie **RDP**- oder **Browser**-Sitzungen über eine gemeinsame Benutzeroberfläche, das eLux Modern User Interface (eLux RP 5) oder das eLux RP 6 User Interface, genutzt werden. Für weitere Informationen siehe [eLux Modern UI](#) oder [eLux RP 6 User Interface](#).

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 den Anwendungstyp **StoreFront**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung, wird in der Scout Enterprise-Konsole angezeigt
Verwende Provisioning-Datei (.cr) ¹	<p>Geben Sie den Namen der Provisioning-Datei ohne Dateierweiterung ein. Die Provisioning-Datei muss auf den Clients im Verzeichnis <code>/setup/ica/</code> vorhanden sein. Für weitere Informationen, siehe StoreFront / Citrix Store-Provisioning-Dateien.</p> <p>Diese Option schließt die Angabe von Store-URLs (nächste Option) aus.</p>
Stores	<p>Geben Sie die URL eines oder mehrerer Stores ein:</p> <p>► Klicken Sie auf die Schaltfläche Hinzufügen und ändern den automatisch erzeugten Vorgabewert auf Ihren individuellen Wert ab (Doppelklick oder F2).</p> <p>Beispiel: <code>https://CtrXd76.sampletec-01.com/Citrix/Store33/discovery</code></p> <p>Diese Option schließt die Verwendung einer Provisioning-Datei (vorherige Option) aus.</p>
Anmeldung	Die Anmeldung des Benutzers am Store erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).

¹ab Scout Enterprise Management Suite Version 15.5

Option	Beschreibung
Passthrough-Anmeldung	<p>Die Anmeldung des Benutzers am Store erfolgt via Single Sign-On. Die Werte der AD-Benutzeranmeldung werden verwendet.</p> <p>Wenn die AD-Benutzeranmeldung über Smartcard erfolgt, darf bei Verwendung von Citrix Receiver for Linux 13.4 oder höher die Authentifizierungsmethode Domain pass-through am Citrix-Server nicht aktiviert sein.</p>

**Hinweis**

Wenn Sie vordefinierte Anmeldedaten oder Passthrough verwenden möchten, muss das eLux-Paket **Citrix Receiver Extensions** und das hierin enthaltene Feature-Paket **Dialog Extension** auf den Clients installiert sein.

Für weitere Informationen siehe "StoreFront / Authentifizierung" auf Seite 203.

Letzten Benutzer anzeigen	<p>Im StoreFront-Anmeldedialog werden die Anmeldedaten (außer Kennwort) der letzten Anmeldung angezeigt.</p> <p>Diese Option hat keine Auswirkung, wenn Sie unter Anmeldung feste Anmeldedaten zur automatischen Anmeldung eintragen.</p>
Autostart	<p>Geben Sie die Namen der StoreFront-Anwendungen ein, die automatisch gestartet werden sollen. Achten Sie auf die korrekte Schreibweise gemäß Anwendungsnamen in StoreFront. Trennen Sie mehrere Anwendungsnamen durch Semikolon.</p> <p>Beispiel: MyApp1 ; MyApp2</p> <p>Wenn nur eine Ressource im Store definiert ist, setzen Sie alternativ den freien Parameter <code>AutostartUniqueResource=true</code>¹</p>
Dauerbetrieb automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen
Freie Parameter (optional)	Individuelle Parameter für den Anwendungsstart siehe Freie Anwendungsparameter definieren

- Wenn Sie einen Eintrag aus der **Stores**-Liste löschen möchten, markieren Sie den Eintrag und klicken auf **Löschen**.
- Für weitere Einstellungen klicken Sie auf die Schaltfläche **Erweitert** und bearbeiten folgende Felder:

¹ab eLux RP 6.4 (Citrix Workspace app)

Option	Beschreibung
Fenstereigenschaften	Desktops können im Vollbild-Modus oder im Fenster-Modus gestartet werden.
Zeitgesteuertes Abmelden	<p>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.</p> <p>Alternativ kann eine automatische Abmeldung nach dem Beenden der letzten StoreFront-Anwendung konfiguriert werden.</p>
Wiederverbinden von Anwendungen	<p>Legen Sie fest, was beim Wiederverbinden zum StoreFront-Server passieren soll.</p> <p>Nicht wiederverbinden: Die Verbindung zum Desktop bzw. zu den veröffentlichten Anwendungen wird nicht wiederhergestellt (Standard).</p> <p>Nur getrennte Sitzungen: Die Verbindung zu einer getrennten Sitzung wird wiederhergestellt.</p> <p>Aktive und getrennte Sitzungen: Die Verbindung zu einer getrennten oder aktiven Sitzung wird wiederhergestellt.</p>
Manuelles Abmelden	<p>Legen Sie fest, was bei der Abmeldung am StoreFront-Server passieren soll.</p> <p>Nur Server abmelden: Eine Abmeldung erfolgt nur vom StoreFront-Server.</p> <p>Server und Anwendungen abmelden: Eine Abmeldung erfolgt vom StoreFront-Server und vom virtuellen Desktop oder den veröffentlichten Anwendungen.</p> <p>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.</p>



Hinweis

Der Zugriff auf die erweiterten Einstellungen kann über die Objektrechte definiert werden.¹

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

*Nach der Anmeldung an einem StoreFront-Store oder einem Webinterface-Server kann der Benutzer alle verfügbaren Ressourcen mit einem Doppelklick auf das **StoreFront**-Symbol auf dem eLux-Desktop anzeigen.*

¹ab Scout Enterprise Management Suite Version 15.5

7.2.2. StoreFront / Store-Provisioning-Datei

– ab eLux RP 6.3 –

Store-Provisioning-Dateien können im Citrix-Backend erstellt werden und enthalten alle relevanten Verbindungsinformationen. Die Verwendung einer Provisioning-Datei erlaubt das automatische Wechseln von den Citrix StoreFront-Verbindungsdaten auf die Citrix Access Gateway-Verbindungsdaten, wenn StoreFront nicht erreichbar ist (Szenario: Wechseln zwischen Firmen-Büro und Homeoffice).

Um eine Store-Provisioning-Datei unter eLux zu nutzen, beachten Sie folgendes:

- Die `.cr`-Datei muss sich auf den Clients im Verzeichnis `/setup/ica/` befinden. Verwenden Sie zum Übertragen die Funktion **Konfigurierte Dateiübertragung**. Für weitere Informationen siehe [Erweiterte Konfiguration > Dateien](#).
- Für Scout Enterprise Management Suite 15.4 und früher, fügen Sie der StoreFront-Anwendungsdefinition zwei freie Parameter hinzu:

```
UseCrFile=true
CrFile=<filename>.cr
```

Lassen Sie das Feld für die Store-URLs leer.

7.2.3. StoreFront / Authentifizierung

Wenn auf dem Client Smartcard-Pakete installiert sind und die Citrix Workspace app für Linux auf dem Client eine Smartcard-Middleware findet, hat die Smartcard-Anmeldung standardmäßig Vorrang. Um für bestimmte Clients dennoch über Benutzername und Kennwort zu authentifizieren, definieren Sie die Authentifizierungsmethode über einen Parameter:

Authentifizierungsmethode über eLux steuern¹

Die Anmeldung kann unabhängig von installierten Smartcard-Paketen über Benutzername und Kennwort gesteuert werden.

- Definieren Sie mit Hilfe der Scout Enterprise-Funktion [Erweiterte Dateieinträge](#) folgenden Eintrag:

Datei	<code>/setup/sessions.ini</code>
Abschnitt	<code>ICADefaults</code>
Eintrag	<code>StoreFrontLogOnWithPassword</code>
Wert	<code>true false (Default: false)</code>

Verhalten bei Smartcard-Authentifizierung konfigurieren

Wenn Sie die Smartcard-Authentifizierung für StoreFront nutzen, können Sie das Verhalten beim Ziehen der Smartcard konfigurieren.

¹ab eLux RP 5.7 und eLux RP 6.2



Hinweis

Die entsprechende Smartcard-Middleware muss auf den Clients installiert sein. Weiterhin muss die Smartcard-Authentifizierung auf der Citrix-Farm aktiviert sein.

-
- 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)

Weitere Parameter zur Authentifizierung¹

Um weitere Parameter zur Authentifizierung zu definieren, verwenden Sie die Konfigurationsdatei /setup/ica/AuthManConfig.xml.template. Diese Datei wird bei der Installation auf die Clients übertragen. Mit Hilfe der Funktionen **Diagnose** und **Konfigurierte Dateiübertragung** können Sie die Datei holen, bearbeiten und wieder auf die relevanten Clients übertragen. Für weitere Informationen siehe [Erweiterte Konfiguration > Dateien](#).

Damit die Funktion am Client aktiv wird, ist ein Neustart für die Übertragung auf den Client und weiterer Neustart für das Aktivieren der neuen Parameter notwendig.

¹ab eLux RP 6.8

7.2.4. 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 Workspace app for Linux**¹ 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 den Anwendungstyp **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie <i>Benutzerdefiniert</i> .
Parameter (erforderlich)	Geben Sie folgenden Programmnamen zum Aufruf ein: <code>selfservice</code>

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`) für eLux RP 5-Clients. Ab eLux RP 6.2 können Sie die **Citrix Self-Service-Benutzeroberfläche im Kiosk-Modus** verwenden.

¹früher Citrix Receiver for Linux

7.2.5. 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

– Vorgehensweise für eLux RP 5 / ab eLux RP 6.2 siehe [Citrix Self-Service-Benutzeroberfläche im Kiosk-Modus](#) –



Hinweis

Das eLux-Paket **Citrix Workspace app for Linux** oder **Citrix Receiver for Linux 13.x** muss installiert sein.

Das eLux-Paket **Citrix Extensions 2.x**² oder höher und das hierin enthaltene Feature-Paket **Self-service wrapper** müssen installiert sein.

Für Anpassungen am Citrix-Dialog-Design müssen weitere Feature-Pakete auf den Clients installiert sein:

Dialog Extension und **Self-service dialog themes**

Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

-
1. Fügen Sie eine [neue Anwendung hinzu](#) und wählen Sie den Anwendungstyp **Lokal**.
 2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie <code>Benutzerdefiniert</code> .
Parameter (erforderlich)	Geben Sie folgenden Programmnamen zum Aufruf ein: <code>ucselfservice</code>

¹ab eLux RP 5.6 CR

²früher Citrix Receiver Extensions

Option	Beschreibung
Freie Parameter	<p>Definieren Sie die StoreFront-URL für alle Stores, die Sie zur Verfügung stellen möchten, in folgendem Format als Freie Anwendungsparameter:</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre>StoreUrl1=<URL to store1> StoreUrl2=<URL to store2> StoreUrl3=<URL to store3></pre> </div> <p>Alternativ können Sie dem Benutzer eine Auswahl vordefinierter Stores zur Verfügung stellen.¹ Für weitere Informationen siehe Self-Service-Benutzeroberfläche mit MultiStore-Option.</p>

3. Definieren Sie optional weitere Parameter und Werte für Fenstereigenschaften und Verbindungsoptionen. Für weitere Informationen siehe [Parameter für die Self-Service-Erweiterung \(ucselfservice\)](#).
4. Bestätigen Sie mit **Übernehmen** und **OK**.
5. Wenn Sie das Design der Citrix-Dialoge für alle Citrix-Verbindungen ändern möchten, verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole. Für weitere Informationen siehe [Parameter für die Self-Service-Erweiterung \(ucselfservice\)](#).

7.2.6. Self-Service-Benutzeroberfläche mit MultiStore-Option

Hierbei handelt es sich um eine erweiterte Citrix Self-Service-Benutzeroberfläche mit der zusätzlichen Option, mehrere Stores für die Benutzer vorzukonfigurieren. Der Benutzer kann dann den gewünschten Store beim Verbindungsaufbau aus einer Dropdown-Liste auswählen.²

Citrix Self-Service mit erweiterter Funktionalität und MultiStore-Option definieren

– Vorgehensweise für eLux RP 5 / ab eLux RP 6.2 siehe [Citrix Self-Service-Benutzeroberfläche im Kiosk-Modus](#) –

¹ab eLux RP 5.5.1000 LTSR CU

²ab eLux RP 5.5.1000 LTSR CU



Hinweis

Das eLux-Paket **Citrix Workspace app for Linux** oder **Citrix Receiver for Linux 13.x** muss installiert sein.

Das eLux-Paket **Citrix Extensions 2.x**¹ oder höher und das hierin enthaltene Feature-Paket **Self-service wrapper** müssen installiert sein.

Für Anpassungen am Citrix-Dialog-Design müssen weitere Feature-Pakete auf den Clients installiert sein:

Dialog Extension und **Self-service dialog themes**

Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Fügen Sie eine **neue Anwendung hinzu** und wählen Sie den Anwendungstyp **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: <code>ucselfservice</code>
Freie Parameter	Konfigurieren Sie den Zugriff auf die Stores, die Sie dem Benutzer zur Auswahl anbieten möchten. Verwenden Sie dazu die Funktion Freie Anwendungsparameter : <div><pre>Stores=<Anzahl der Store-Einträge> Store1=<Store-Anzeigename>,<Store-URL> Store2=<Store-Anzeigename>,<Store-URL> ... Domains=<Anzahl der Domänen-Einträge> Domain1=<Domänen-Anzeigename>,<Domäne> Domain2=<Domänen-Anzeigename>,<Domäne> ... ShowLastUser=<0 1></pre></div> <p>Hinweis: Sie können beliebig viele Stores und Domänen im angegebenen Format vordefinieren.</p>

¹früher Citrix Receiver Extensions

3. Definieren Sie optional weitere Parameter und Werte für Fenstereigenschaften und Verbindungsoptionen. Für weitere Informationen siehe [Parameter für die Self-Service-Erweiterung \(ucselfservice\)](#).
4. Bestätigen Sie mit **Übernehmen** und **OK**.
5. Wenn Sie das Design der Citrix-Dialoge für alle Citrix-Verbindungen ändern möchten, verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole. Für weitere Informationen siehe [Parameter für die Self-Service-Erweiterung \(ucselfservice\)](#).

7.2.7. Parameter für die Self-Service-Erweiterung (ucselfservice)

Parameter für Fenstereigenschaften und Verbindungsoptionen

- Definieren Sie in den Anwendungseigenschaften folgende Optionen als freie Parameter (Vorgehensweise für eLux RP 5):

Parameter	Beschreibung	Herkunft
<code>SharedUserMode=true false</code>	Im Shared User Mode wird ein Systemkonto für mehrere Benutzer verwendet. Beim Abmelden oder Schließen der Benutzeroberfläche werden die Benutzerdaten entfernt.	Citrix
<code>FullscreenMode=0 1 2</code>	0 kein Vollbildmodus 1 Vollbildmodus 2 maximiert und ohne Rahmen, Taskleiste bleibt sichtbar Kann für die Verwendung von seamless applications sinnvoll sein Default: 0 (kein Vollbildmodus)	Citrix
<code>SelfSelection=true false</code>	Wird zur Deaktivierung des Suchfeldes und der Self-Selection-Leiste verwendet Das Deaktivieren verhindert, dass Benutzer weitere Anwendungen abonnieren können. Default: false	Citrix
<code>StoreGateway=<store gateway></code>	Angabe eines Gateways, falls erforderlich	Citrix

Parameter	Beschreibung	Herkunft
ReconnectOnLogon=true false	Legt fest, ob die SelfService-Oberfläche versucht, direkt nach der Anmeldung an einem Store alle Sitzungen für diesen Store wiederzuverbinden	Citrix
ReconnectOnLaunchOrRefresh=true false	Legt fest, ob die SelfService-Oberfläche 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=0 1	1 Logoff-Timer wird mit der Anmeldung gestartet 0 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

Für weitere Informationen siehe [Freie Anwendungsparameter definieren](#).



Achtung

Die dem Benutzer zur Verfügung gestellten Stores können Sie entweder fest vorgeben oder dem Benutzer über ein Pre-Login eine Auswahl vorgeben.¹ Für weitere Informationen siehe

- Self-Service-Benutzeroberfläche mit Erweiterungen oder
- Self-Service-Benutzeroberfläche mit MultiStore-Option

Parameter für das Design der Citrix-Dialoge

- Wenn Sie das Design der Citrix-Dialoge für alle Citrix-Verbindungen ändern möchten, verwenden Sie die Funktion **Erweiterte Dateieinträge** der Scout Enterprise-Konsole und setzen folgende Einträge:

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.

7.2.8. Benutzerdefiniertes Design für Citrix Workspace app

– ab eLux RP 6.4 –



Hinweis

Das eLux-Paket **Citrix Workspace app for Linux** Version 18.08 oder neuer muss installiert sein.

¹ab eLux RP 5.5.1000 LTSR CU

Um das Layout Ihrer Citrix-Sitzung an Ihr Corporate Design anzupassen, übertragen Sie die relevanten Layout-Dateien auf die Clients in die Citrix-Verzeichnisstruktur. Die Dateien werden dann mit den Citrix-Layout-Dateien gemergt.

Zum Übertragen der Dateien verwenden Sie die Funktion **Konfigurierte Dateiübertragung**. Für weitere Informationen siehe [Erweiterte Konfiguration > Dateien](#).

Als Ziel verwenden Sie die vorhandenen Citrix-Verzeichnisse. Beispiel:

Standard	/setup/ica/site_custom
Bei Verwendung des Shared User Mode	/setup/ica/site_custom/sum_screen

Die Citrix-Verzeichnisstruktur muss der originalen Struktur entsprechen. Die Original-Struktur finden Sie unter /opt/Citrix/ICAClient/site_orig.

7.2.9. 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 den Anwendungstyp **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: <code>https://<Servername>/Citrix/StoreWeb</code> <code>https://<Servername>/Citrix/XenApp</code>

-
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.

7.2.10. 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

`//Inetpub/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 den Anwendungstyp **PNAgent**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Server	<p>Geben Sie die Adresse der Konfigurationsdatei am Webinterface-Server an (URL).</p> <p>Wenn das Standardverzeichnis und Port 80 genutzt werden, genügt die Angabe des Servers.</p> <p>Beispiele:</p> <p><code>https://CtrXd.sampletec-01.de/Citrix/PNAgent/config.xml</code></p> <p><code>https://192.168.10.11:81</code></p>
Anmeldung	Die Anmeldung des Benutzers am Webinterface erfolgt automatisch über die angegebenen Anmeldedaten (Benutzer, Kennwort, Domäne).

Option	Beschreibung
Passthrough-Anmeldung	<p>Die Anmeldung des Benutzers am Webinterface erfolgt via Single Sign-On. Die Werte der AD-Benutzeranmeldung werden verwendet.</p> <p>Hinweis: Die Authentifizierung über Kerberos wird für Citrix Receiver for Linux 13.x und neuere Versionen nicht mehr unterstützt.</p>
Autostart Anwendung/Verzeichnis	<p>Geben Sie die Namen der Anwendungen an, die automatisch gestartet werden sollen.</p> <p>Alternativ können Sie einen Autostart-Ordner angeben, der veröffentlichte Anwendungen enthält. Der Ordner muss am Citrix Webinterface-Server angelegt sein.</p>
Letzten Benutzer anzeigen	<p>Im PNAgent-Anmeldedialog werden die Benutzerdaten (außer Kennwort) der letzten Anmeldung angezeigt.</p> <p>Diese Option hat keine Auswirkung, wenn Sie Benutzerdaten zur automatischen Anmeldung eintragen.</p>
Abbrechen erlauben	Erlaubt dem Benutzer, den PNAgent-Anmeldedialog zu schließen
Dauerbetrieb automatisch starten Desktop-Symbol	Siehe Anwendung hinzufügen
Freie Parameter (optional)	<p>Individuelle Parameter für den Anwendungsstart</p> <p>Beispiel: <code>PNATimeout=60</code> führt dazu, dass die Citrix Workspace App¹ 60 Sekunden lang versucht, die veröffentlichten Anwendungen und Desktops zu enumerieren.</p> <p>Um Dual-Monitorbetrieb einzurichten, können Sie auch die Freien Parameter verwenden, siehe unten.</p> <p>Für weitere Informationen siehe Freie Anwendungsparameter definieren</p>

- 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.

¹früher Citrix Receiver

Option	Beschreibung
Zeitgesteuertes Abmelden	<p>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.</p> <p>Alternativ kann eine automatische Abmeldung nach dem Beenden der letzten PNAgent-Anwendung konfiguriert werden.</p>
Wiederverbinden von Anwendungen	<p>Legen Sie fest, was beim Wiederverbinden zum Webinterface-Server passieren soll.</p> <p>Nicht wiederverbinden: Die Verbindung zum Desktop oder zu den veröffentlichten Anwendungen wird nicht wiederhergestellt (Standard).</p> <p>Nur getrennte Sitzungen: Die Verbindung zu einer getrennten Sitzung wird wiederhergestellt.</p> <p>Aktive und getrennte Sitzungen: Die Verbindung zu einer getrennten oder zu einer aktiven Sitzung wird wiederhergestellt.</p>
Manuelles Abmelden	<p>Legen Sie fest, was nach einem Abmelden am Webinterface-Server passieren soll.</p> <p>Nur Server abmelden: Eine Abmeldung erfolgt nur vom Webinterface-Server.</p> <p>Server und Anwendungen abmelden: Eine Abmeldung erfolgt vom Webinterface-Server und vom virtuellen Desktop bzw. den veröffentlichten Anwendungen</p> <p>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.</p>



Hinweis

Der Zugriff auf die erweiterten Einstellungen kann über die Objektrechte definiert werden.¹

- 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:

¹ab Scout Enterprise Management Suite Version 15.5

\$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.sampletec-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	<code>/setup/sessions.ini</code>
Abschnitt	<code>ICADefaults</code>
Eintrag	<code>Xinerama</code>
Wert	<code>-1 0 1</code>

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

7.2.11. ICA-Anwendung definieren



Hinweis

Der Zugriff über den Anwendungstyp **ICA** ist veraltet und wird nur bis XenApp 6.x von Citrix unterstützt.

Der Typ **ICA** wird unter eLux RP 6 in der lokalen Anwendungsdefinition nicht mehr unterstützt.

1. Fügen Sie eine [neue Anwendung hinzu](#) und wählen Sie den Anwendungstyp **ICA**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die 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.

Option	Beschreibung
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 und neuere Versionen nicht mehr unterstützt.
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	Öffnet den Citrix-Konfigurations-Dialog (<code>wfcmgr</code>) Bearbeiten Sie die gewünschten Optionen.
Erweitert (eLux)	Die Konfiguration für die Citrix Workspace-App ¹ wird in der Datei <code>/setup/ica/wfclient.ini</code> 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.

¹früher Citrix Receiver

7.2.12. Citrix Software-StandardEinstellungen

Für Citrix-Anwendungen können Sie in der Scout Enterprise-Konsole Citrix Workspace App¹-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](#).



Hinweis

Um Parameter in bestimmten Konfigurationsdateien zu setzen, verwenden Sie die Funktion [Erweiterte Dateieinträge](#). Konfigurationen, die Sie über die **Erweiterten Dateieinträge** setzen, haben Priorität gegenüber den Software-Standardeinstellungen.

Einige Citrix-Standardeinstellungen werden im folgenden beschrieben. Weitere Informationen entnehmen Sie bitte der Dokumentation von Citrix.

Register Allgemein

Option	Beschreibung
TW2StopwatchMinimum	<p>Bildlaufgeschwindigkeit für Remote Anwendungen (beispielsweise für Adobe Acrobat Reader, Excel)</p> <p>Je höher der Wert, desto langsamer die Geschwindigkeit beim Scrollen</p> <p>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.</p> <p>Standardwert = 25</p>

¹früher Citrix Receiver

Option	Beschreibung
ClientName – Vorlage	Definition des Client-Namens in der Citrix-Sitzung Hinweis: Sie können die Program Neighborhood-Variablen <code>\$ICANAME</code> und <code>\$ICADOMAIN</code> 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 <code>/media/usbdisk</code> oder <code>/media/cdrom</code> .
Attribute E / R / W	bezeichnen die Art des Zugriffsrechts: <ul style="list-style-type: none"> • E = aktivieren (enable) • R = lesen (read) • W = schreiben (write)
Laufwerkszuordnung erlauben	Nur bei eingeschalteter Option werden die definierten Laufwerkszuordnungen durchgeführt.
Dynamische Zuordnung aktivieren	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 Gerätenamen des COM-Anschlusses am Thin Client bekannt sein.

Der COM-Port-Gerätenamen beginnt immer mit `/dev`. Groß- und Kleinschreibung ist bei den Gerätenamen relevant.

Beispiele:

Port-Gerätenamen	COM Port
<code>/dev/ttyS0</code>	COM1
<code>/dev/ttyS1</code>	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`

7.2.13. 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 Desktop-Anwendung angezeigt.¹

Citrix Connection Center konfigurieren



Hinweis

Wenn Sie **Citrix Receiver for Linux** einsetzen, muss das eLux-Paket **Citrix Receiver Extensions** und das hierin enthaltene Feature-Paket **Connection Center** auf den Clients installiert sein. Wenn Sie die neuere **Citrix Workspace app** einsetzen, muss das hierin enthaltene Feature-Paket **Utilities and tools** 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 den Anwendungstyp **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie <code>Citrix Connection Center</code> .

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

¹früher als Systray-Icon in der Systemleiste

7.2.14. Protokollierung für Citrix Workspace app

Für die Citrix Workspace app können Sie die Protokollierung über einen Konfigurationsparameter aktivieren und einstellen.

Protokollierung konfigurieren

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Geräte die **Erweiterte Konfiguration > Erweiterte Dateieinträge**.
2. Definieren Sie folgenden Eintrag:

Datei	/setup/ica/module.ini		
Abschnitt	WFClient		
Eintrag	SyslogThreshold		
Wert	0 3 7	0 Keine Protokollierung (Standard) 3 Nur Fehler werden protokolliert 7 Protokolleinträge für alle Ebenen werden erzeugt	

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

Sobald die neue Konfiguration aktiv ist, werden die Protokolle nach `/var/log/messages` geschrieben.

7.3. Zusätzliche Software für Citrix-Umgebungen

Zum Installieren zusätzlicher Software sind folgende Schritte notwendig:

1. Downloaden Sie das angegebene Software-Paket von unserem Portal www.mylux.com für die gewünschte eLux-Version.
2. In Scout Enterprise ELIAS importieren Sie das Paket in Ihren Container. Für weitere Informationen siehe [Pakete in einen Container importieren](#) im **ELIAS**-Handbuch oder [Software-Pakete importieren](#) im **ELIAS 18**-Handbuch.
3. In Scout Enterprise ELIAS fügen Sie das Paket Ihrer Imagedatei (IDF) hinzu und speichern die modifizierte Imagedatei. Für weitere Informationen siehe [IDF erstellen](#) im **ELIAS**-Handbuch oder [Image erstellen](#) im **ELIAS 18**-Handbuch.
4. Führen Sie für die relevanten Clients ein Firmware-Update auf die modifizierte Imagedatei durch.
Das Software-Paket wird auf den Clients installiert.
5. Konfigurieren Sie die Software in der Backend-Umgebung.

7.3.1. Avaya Equinox

Softphone-Anwendung für den Zugriff auf Unified Communications (UC) und Over the Top (OTT)-Dienste

Paketname: **Avaya Equinox VDI Client**

7.3.2. Cisco JVDI

Jabber Softphone for VDI (JVDI)¹ 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 JVDI-Software routet alle Audio- und Video-Streams direkt von einem Thin Client zum anderen oder zu einem Telefon - ohne über den HVD zu gehen.

Paketnamen: **Cisco JVDI Client** und **Utilities for Cisco JVDI Client**

- Folgen Sie dem Cisco Deployment and Installation Workflow auf der Cisco-Webseite, um die JVDI-Systemumgebung zu konfigurieren.

7.3.3. deviceTRUST

Dynamische Kontext-Erkennung, ermöglicht den Benutzern, von jedem Ort und von jedem Gerät auf ihren Arbeitsbereich zuzugreifen unter Einhaltung aller IT-Richtlinien

Paketname: **deviceTRUST Contextualizing IT**

¹früher VXME

7.3.4. DriveLock

DriveLock bietet Endpoint-Security für USB-Schnittstellen am Thin Client.

Paketname: **DriveLock**

7.3.5. Grundig Citrix Extensions

Digitale Diktierlösung von Grundig Business Systems

Paketname: **Grundig Citrix Extensions**

7.3.6. HDX RealTime Media Engine

Die HDX RealTime Media Engine (RTME) ermöglicht eine bessere Audio- und Videoqualität bei VOIP und Videochat.

Paketname: **Citrix HDX RTME**

- Konfigurieren Sie Microsoft Lync oder Skype for Business in der Backend-Umgebung.

7.3.7. JabraXpress Device Updater

Der JabraXpress Device Updater wird auf dem Thin Client des Endbenutzers installiert. Er verwaltet und steuert Firmware-Versionen und Geräte-Einstellungen für die Jabra-Geräte.

Eine ausführliche Beschreibung zur Verwendung des JabraXpress Device Updater finden Sie in der Dokumentation für JabraXpress für Linux:

<https://jabraxpress.jabra.com/Downloadables/Linux/UserGuide.pdf>

Paketname: **JabraXpress Device Updater**

7.3.8. Olympus Dictation

Digitale Diktierlösung von Olympus

Paketname: **Olympus Dictation Drivers**

7.3.9. Philips Speech

Digitale Diktierlösung von Philips Speech Processing Solutions

Paketname: **Philips Speech Drivers**

7.3.10. SecMaker

– ab eLux RP 6.5 –

SecMaker Net iD Enterprise ist eine Middleware für Smartcards, die SSL 3.0/TLS 1.0 (Client-Identifizierung), PKCS #7 (Digitale Signaturen) und PKCS #10 (Zertifikatanforderungen) unterstützt. Die Verwendung von SecMaker Net iD 6.x auf dem Client erfordert eine gesonderte Lizenz.

Paketname: **SecMaker NetID**

- ▶ Verwenden Sie die Scout Enterprise-Funktion **Dateien**, um die Lizenzdatei in das Zielverzeichnis `/setup/iid/netidlicense.lic` am Client zu übertragen.

Für weitere Informationen siehe [Dateien](#).



Hinweis

Die Lizenzvereinbarung (EULA) ist auf dem eLux-Client verfügbar unter `/etc/iid/SecMaker License and Support Conditions 20150202.pdf`.

7.3.11. Zoom

Videokonferenzen für Unternehmen mit Echtzeit-Messaging und Content-Sharing

Paketname: **Zoom Client for Linux**

Zoom Client für Linux ist eine lokale Anwendung auf eLux, die Peer-to-Peer-Verbindungen zwischen verbundenen Geräten ermöglicht.

Paketname: **Zoom Citrix Plugin**

Mit dem Zoom Citrix-Plugin kann ZoomVDI in einer virtuellen Desktop-Infrastruktur mit einer Citrix-Lösung verwendet werden. Peer-to-Peer-Verbindungen werden in diesem Szenario nicht unterstützt.

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 Optionen zur Konfiguration 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 den Anwendungstyp **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	<p>Erlaubt die Definition aller Parameter, die eLuxRDP zulässt, im Format:</p> <pre>FreeRDPParams=<Parameter> <Parameter> <Parameter>...</pre> <p>Trennen Sie mehrere Parameter durch Leerzeichen.</p> <p>Beispiele:</p> <pre>FreeRDPParams=/microphone:sys:pulse +fonts /cert-ignore</pre> <p>Eine Liste der Parameter erhalten Sie durch Eingabe des Kommandos <code>eluxrdp</code> in einer Shell.</p> <p>Für weitere Informationen siehe Freie Anwendungsparameter definieren.</p>
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 den Anwendungstyp **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 Beispiele: <code>c:\Programme\Microsoft Office\Office\EXCEL.EXE</code> <code>%SystemRoot%\system32\notepad.exe</code>
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 Anwendungs-Einstellungen / RDP und VMware

Die unten beschriebenen Einstellungen beziehen sich auf folgende Anwendungen:

- RDP-Anwendungen
- VMware-Anwendungen

Wenn Sie ein anderes Protokoll als RDP wählen, sind nicht alle Optionen verfügbar.

Erweiterte Anwendungs-Einstellungen öffnen



Hinweis

Der Zugriff auf die erweiterten Einstellungen kann über die Objektrechte eingeschränkt werden.¹

- ▶ Scout Enterprise: Klicken Sie in den Anwendungseigenschaften einer RDP- oder VMware-Anwendung auf die Schaltfläche **Erweitert**.
- ▶ eLux RP 6: Öffnen Sie in den Anwendungseigenschaften einer RDP- oder VMware-Anwendung unterhalb von **Eigenschaften** das relevante Register.

Register Anzeige

Option	Beschreibung
Fenstergröße	Vollbild oder eine bestimmte Auflösung
Vollbild auf Monitor	Wenn Sie die Fenstergröße <code>vollbild</code> gewählt haben, können Sie wählen, ob auf alle oder einen bestimmten Monitor ausgegeben werden soll. Es werden bis zu acht Monitore unterstützt. ²
Farben	Farbtiefe der Sitzung (8-32 Bit)



Hinweis

Wenn mehrere Bildschirme angeschlossen sind und wenn Sie auf einen einzelnen Monitor auszugeben möchten, muss in der Geräte-Konfiguration 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 5.2 oder höher unterstützen.

¹ab Scout Enterprise Management Suite Version 15.5

²ab Scout Enterprise Management Suite Version 15.0



Hinweis

– für Terminalserver, die die RDP-Protokollversion 5.2 oder höher unterstützen –
Die Einstellungen werden nur dann wirksam, wenn im Register **Erweitert** das **Protokoll** nicht auf RDP V4 gesetzt ist.

Option	Beschreibung
Laufwerke	<p>Wählen Sie Laufwerk, Mountpoint und den Laufwerksbuchstaben, der in der RDP/VMware-Sitzung dargestellt werden soll.</p> <p>Die Mountpoints entsprechen dem lokalen Zugriffspfad auf die Ressource und werden von eLux zur Verfügung gestellt.</p> <p>Für USB-Sticks lauten die Mountpoints <code>/media/usbdisk</code> <code>/media/usbdisk0</code> usw.</p> <p>Für weitere Informationen siehe Mountpoints.</p>
Drucker	<p>Bis zu vier Druckerdefinitionen für eine Sitzung können automatisch erstellt werden. Die Drucker müssen im Register Drucker der eLux-Geräte-Konfiguration 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 Als Standard setzen in der eLux-Drucker-Konfiguration.</p>
Sound	<p>Mit der Option Lokal abspielen wird der Ton lokal am Client wiedergegeben. Remote abspielen bewirkt die Wiedergabe am entfernten Server.</p>
Anschlüsse	<p>Macht die definierten Schnittstellen von der Sitzung aus zugänglich.</p>
Kartenleser	<p>Smartcards können zur Anmeldung auf Basis eines Zertifikats verwendet werden.</p>

Register Erweitert

Option	Beschreibung
Protokoll (nur RDP)	<p>Ermöglicht die Einstellung auf die RDP-Protokollversion 4 oder 5</p> <p>Standardmäßig wird das Protokoll automatisch erkannt.</p>
Tastatursprache	<p>Definiert das Tastaturlayout innerhalb einer Sitzung</p> <p>Die Standardeinstellung <code>Auto</code> entspricht der Einstellung der Tastatursprache in der eLux-Geräte-Konfiguration.</p>



Achtung

Wenn Sie eine bestimmte Tastatursprache einstellen, muss diese identisch mit der Tastatursprache sein, die in der eLux-Geräte-Konfiguration im **Tastatur**-Dialog eingetragen ist.

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 <code>Standard</code> , <code>Modem</code> , <code>Breitband</code> , <code>LAN</code> .

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



Hinweis

Am eLux RP 6-Client steht dieser Anwendungstyp nicht zur Verfügung, dafür jedoch der Anwendungstyp **VMware Horizon**.

Als **virtuellen Desktop** können Sie einen Virtual Desktop Broker für Citrix-Verbindungen oder VMware-Verbindungen definieren.¹

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 den Anwendungstyp **Virtueller Desktop**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
VD Broker	Wählen Sie die Virtual Desktop-Anwendung aus der Liste.
Server	Geben Sie die IP-Adresse (oder Name) des Servers ein.
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.
Protokoll (nur VMware Horizon)	Wählen Sie zwischen folgenden Werten: RDP PCoIP VMware Blast ²

3. Um weitere Einstellungen für XenDesktop oder VMware Horizon zu setzen, klicken Sie auf die Schaltfläche **Erweitert**. Für weitere Informationen siehe je nach gewähltem Broker
 - **Erweiterte Anwendungs-Einstellungen / RDP und VMware** (für VMware Horizon) oder
 - **Erweiterte XenDesktop-Einstellungen**
4. Bestätigen Sie mit **Übernehmen** und **OK**.

¹Ab Scout Enterprise 15.8 wird nur noch VMware Horizon unterstützt.

²ab Scout Enterprise Management Suite Version 15.2

7.5.2. VMware Horizon



Hinweis

Dieser Anwendungstyp steht nur am eLux RP 6-Client zur Verfügung. Am eLux RP 5-Client und in der Scout Enterprise-Konsole wählen Sie den Anwendungstyp **Virtueller Desktop** und als VD-Broker **VMware View**.

Anwendungstyp VMware	...
Name VMware A1 *	
VD-Broker VMware Horizon	
Server	
Passthrough-Anmeldung	<input type="checkbox"/>
Benutzer	
Kennwort	
Domäne	
Verwende SSL	<input type="checkbox"/>
Letzten Benutzer anzeigen	<input checked="" type="checkbox"/>
Protokoll RDP	...
Automatisch starten	<input type="checkbox"/>
Desktop-Symbol	<input type="checkbox"/>

Die Abbildung bezieht sich auf eLux RP 6.

Option	Beschreibung
Name	Name für die Anwendung

Option	Beschreibung
VD-Broker	VMware Horizon
Server	Geben Sie die IP-Adresse (oder den Namen) des Servers ein.
Passthrough-Anmeldung	Die Werte der AD-Benutzeranmeldung werden verwendet.
Benutzer, Kennwort, Domäne	Die Anmeldung des Benutzers am Server erfolgt automatisch über die angegebenen Anmeldedaten.
Verwende SSL	Erzwingt die Verbindung über HTTPS Beachten Sie, dass die entsprechenden Zertifikate am Client vorhanden sein müssen.
Letzten Benutzer anzeigen	Im Anmeldedialog werden die Anmeldedaten (außer Kennwort) der letzten Anmeldung angezeigt.
Protokoll	Wählen Sie zwischen folgenden Werten: RDP PCoIP VMware Blast ¹
Automatisch starten	Die Verbindung wird automatisch gestartet.
Desktop-Symbol	Für die Anwendung wird eine Verknüpfung auf dem Desktop angelegt.

Für Informationen zu den Erweiterten Einstellungen siehe [Erweiterte Anwendungs-Einstellungen](#).

Die Konfiguration für VMware Horizon kann über die Anwendungseigenschaften in der Scout Enterprise-Konsole oder lokal am Client erfolgen. Wenn Sie darüber hinaus weitere Parameter setzen möchten, die nicht in der Oberfläche berücksichtigt werden, können Sie eine Konfigurationsdatei verwenden:

- ▶ Erstellen Sie mit Hilfe der VMware-Dokumentation² die Datei `view-userpreferences`. Übertragen Sie die Datei mit der Scout Enterprise-Funktion [Konfigurierte Dateiübertragung](#) auf die Clients nach `/setup/elux/.vmware/view-userpreferences`



Hinweis

Die Konfiguration über die Oberfläche in Scout Enterprise oder eLux hat Priorität gegenüber der Konfigurationsdatei und überschreibt ggf. Werte der Konfigurationsdatei.

¹ab Scout Enterprise Management Suite Version 15.2

²Installationshandbuch für VMware Horizon Client für Linux

7.6. Browser

Unterstützte Browser sind Mozilla Firefox und Google Chromium.

Daneben ist der Builtin-Browser als einfacher Browser verfügbar.¹ Der Builtin-Browser basiert auf der WebKit2-Engine, die im Paket **Desktop environment**² enthalten ist. Standardmäßig wird der Builtin-Browser ohne Adress- und Navigationsleiste ausgeführt. Diese und weitere Funktionen können für den Kiosk-Modus konfiguriert werden.



Hinweis

Wenn Sie Chromium einsetzen, empfehlen wir mindestens 2 GB RAM für die Thin Clients.

Ab eLux RP 6 wird das Java Browser-Plugin nicht mehr unterstützt.

7.6.1. Browser-Anwendung definieren

1. Fügen Sie eine **neue Anwendung hinzu** und wählen Sie den Anwendungstyp **Browser**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für den Browser, wird in der Scout Enterprise-Konsole angezeigt
Browsertyp	Wählen Sie Firefox , Chromium oder Builtin-Browser . ³
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

¹ab Scout Enterprise Management Suite 15.4 und eLux RP 6.5

²früher MATE Desktop

³ab Scout Enterprise Management Suite 15.4 und eLux RP 6.5

Option	Beschreibung
Proxy-Einstellung	<ul style="list-style-type: none"> Kein Proxy: Keinen Proxy-Server verwenden Manuell (Proxy:Port): Proxy-Server und Portnummer manuell festlegen Auto (URL): Proxy-Konfigurationsdatei verwenden System-Proxy verwenden (Standard):¹ Proxy-Einstellung, die 'systemweit' in der Geräte-Konfiguration Netzwerk > Erweitert pro Netzwerk-Profil definiert wird <p>Beachten Sie, dass die Einstellung hinter System-Proxy auch Kein Proxy sein kann.</p> <p>Für weitere Informationen siehe Proxy-Konfiguration.</p>

**Hinweis**

Für den Builtin-Browser muss die Einstellung auf System-Proxy verwenden bleiben.

Dauerbetrieb Siehe [Anwendung hinzufügen](#)
 Automatisch starten
 Desktop-Symbol

Freie Parameter (optional) Individuelle Parameter für den Anwendungsstart
 siehe [Freie Anwendungsparameter](#)

- Um den Kiosk-Modus für Firefox einzuschalten, siehe [Kiosk-Modus für Firefox](#).
- 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](#)

¹ab Scout Enterprise Management Suite 15.5

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 ¹ Ab eLux RP 6.5 und Firefox 60.5 können die Zertifikate auch in /setup/cacerts/browser liegen.
Google Chromium	/setup/cacerts/browser

Für weitere Informationen siehe [Konfigurierte Dateiübertragung](#).

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 [Konfigurierte Dateiübertragung](#).

7.6.3. Voreinstellungen Firefox

Firefox-spezifische Voreinstellungen, die über die Konfigurationsmöglichkeiten der Anwendungsdefinition hinausgehen, können Sie mit Hilfe der Konfigurationsdatei /setup/firefox/user.ini am Client festlegen.²

Zusätzlich unterstützt Firefox ab der Version 60 ESR Unternehmensrichtlinien, die über .json-Dateien Plattform-unabhängig eingesetzt werden können.³ Ab eLux RP 6.5 wird Firefox mit aktivierten Unternehmensrichtlinien installiert, die standardmäßig den Zugriff auf about:config und weitere Konfigurationsmöglichkeiten sperren.

¹bis eLux RP 6.4

²ab Firefox Version 38.5.2.1

³Diese Methode schließt die Steuerung durch Windows-Gruppenrichtlinien aus.

Voreinstellungen für Firefox (about:config) mit `user.ini` definieren

Zur Verfügung stehen alle Optionen, die im Firefox-Konfigurationseditor (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.

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 Geräte-Konfiguration > Erweiterte Dateieinträge**.
3. Definieren Sie folgenden Eintrag:

Datei	<code>/setup/firefox/user.ini</code>
Abschnitt	<i><Einstellungsname, wie im Konfigurationseditor angegeben – Zeichenfolge links vom letzten Punkt></i>
Eintrag	<i><Einstellungsname, wie im Konfigurationseditor angegeben – Zeichenfolge rechts vom letzten Punkt></i>
Wert	<i><gewünschter Wert></i>

Beispiel:

Sie möchten den Wert für die Option **`browser.tabs.closeWindowWithLastTab`** auf den Wert `false` setzen.

Datei	<code>/setup/firefox/user.ini</code>
Abschnitt	<code>browser.tabs</code>
Eintrag	<code>closeWindowWithLastTab</code>
Wert	<code>false</code>

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

Voreinstellungen für Firefox mit `.json`-Dateien definieren (Richtlinien)

– ab eLux RP 6.5 und Firefox-Version 60 ESR –

Zur Verfügung stehen alle Optionen, die im [README des Mozilla GitHub Repository](#) beschrieben sind.¹

Eine oder mehrere Optionen werden in einer `.json`-Datei mit Hilfe der Scout Enterprise-Funktion **Konfigurierte Dateiübertragung** zum Client übertragen.

¹Beachten Sie, dass der aktuelle Firefox-Stand von demjenigen der eingesetzten eLux-Version abweichen kann.



Hinweis

Standardmäßig ist der Zugriff auf die Firefox-Konfiguration gesperrt.

1. Erstellen Sie eine `.json`-Datei mit beliebigem Namen. Fügen Sie eine oder mehrere Firefox-Optionen durch Komma getrennt ein.

Beispiel:

```
{  
  "BlockAboutConfig": false,  
  "DisableBuiltinPDFViewer": true  
}
```

2. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Geräte-Konfiguration > Dateien**.

Geben Sie die `.json`-Datei als Quelldatei an. Definieren Sie die Zieldatei im Verzeichnis `/setup/firefox/policies/`.

Beispiel: `/setup/firefox/policies/custom_A.json`

Für weitere Informationen siehe [Erweiterte Konfiguration > Dateien](#).

Die Dateien werden beim nächsten Client-Start übertragen und ausgewertet.



Hinweis

In das Client-Verzeichnis `/setup/firefox/policies/` können mehrere `.json`-Dateien übertragen werden. Die Dateien werden in alphabetischer Reihenfolge zusammengeführt: Bei gleichen Optionen haben Werte aus Dateien mit absteigendem Namen Priorität (B überschreibt A).

7.6.4. Voreinstellungen Builtin-Browser

Der Builtin-Browser überträgt bei jedem Seitenaufruf einen "User Agent"-String, der durch die WebKit2-Engine vordefiniert ist. Er enthält Informationen wie Mozilla-Kompatibilität und Betriebssystem.

Um stattdessen eigene Informationen zu übertragen, definieren Sie einen Erweiterten Dateieintrag:¹

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Geräte-Konfiguration > Erweiterte Dateieinträge**.
2. Definieren Sie folgenden Eintrag:

Datei	/setup/sessions.ini
Abschnitt	[BuiltinBrowserDefaults]
Eintrag	UserAgentString
Wert	<individuelle Zeichenfolge>

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

¹ab eLux RP 6.8.2

7.6.5. 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).

Beispiel: `/smb/share`


Für weitere Informationen siehe [Netzlaufwerk definieren](#).

Speicherort für Browser-Dateien festlegen



Hinweis

Die folgenden Informationen beziehen sich auf die Scout Enterprise Management Suite Version 15.0 und höher. Informationen zu älteren Versionen finden Sie im Archiv der Download-Seite [PDF-Downloads](#).

1. Öffnen Sie in der Baumstruktur für die relevante Ebene das Kontextmenü der  **Anwendungen** und wählen Sie den Eintrag **Software-Standardeinstellungen....**
Für weitere Informationen siehe [Standardeinstellungen für Anwendungen setzen](#).
2. Wählen Sie im Listefeld den gewünschten Browser und klicken Sie auf **Bearbeiten**.
3. Geben Sie im Feld **Browser-Homeverzeichnis** ein als Laufwerk definiertes Freigabeverzeichnis aus der **Geräte-Konfiguration > Laufwerke** ein. Der Name muss demjenigen aus der Liste entsprechen.
Beispiel: `/smb/share`
4. Bestätigen Sie mit **OK**.

Der Browser legt die Einstellungsdaten im angegebenen Windows-Verzeichnis ab.

7.6.6. Kiosk-Modus für Firefox

– für Firefox bis zur Version ESR 52.8 ¹ –



Hinweis

Ab eLux RP 6.5 können Sie den Builtin-Browser im Kiosk-Modus verwenden. Für weitere Informationen siehe [Builtin-Browser im Kiosk-Modus](#).

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.

¹in eLux RP 6.4 enthalten

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 den Anwendungstyp **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

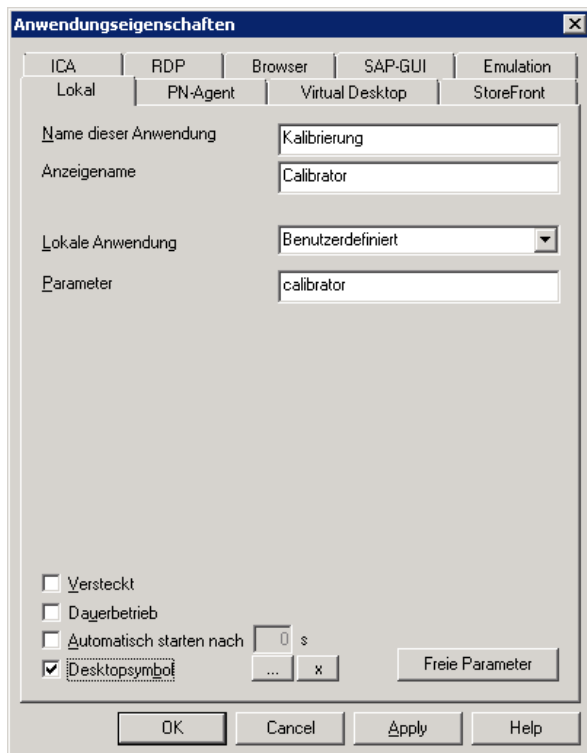
3. Bestätigen Sie mit **Übernehmen** und **OK**.

7.7.2. Benutzerdefinierte Anwendung definieren

1. Fügen Sie eine **neue Anwendung hinzu** und wählen Sie den Anwendungstyp **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Name für die Anwendung
Lokale Anwendung	Wählen Sie Benutzerdefiniert .
Parameter (erforderlich)	<p>Geben Sie den Programmnamen zum Aufruf der Anwendung ein. Wenn gewünscht, geben Sie zusätzlich Parameter ein, mit denen die Anwendung gestartet werden soll.</p> <p>Beispiel:</p> <p><code>calibrator</code> ruft die Anwendung Calibrator auf.</p> <p><code>squid</code> ruft die Anwendung Squid auf.</p> <p><code>squid /tmp/mycache</code> ruft Squid mit einem bestimmten Cache-Verzeichnis auf.</p>
Versteckt	<p>Die Anwendung wird am Client nicht im Register Anwendungen angezeigt.</p> <p>Aktivieren Sie entweder die Option Automatisch starten oder die Option Dauerbetrieb.</p>
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. Zoom für Linux definieren

Der native Zoom-Client für Linux ist eine Videokonferenz- und Webkonferenz-Lösung mit sehr guten Video-, Audio- und Screen-Sharing-Möglichkeiten.

Die Konfiguration der Video- und Audio-Geräte erfolgt über die Oberfläche der Anwendung.

1. Fügen Sie eine neue Anwendung hinzu und wählen Sie in den **Anwendungs-Eigenschaften** den Anwendungstyp **Lokal**.
2. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Name	Frei wählbarer Name
Anwendung	Benutzerdefiniert
Parameter	zoom

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

7.7.4. Ekiga SIP Softphone definieren

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** den Anwendungstyp **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:¹

Emulation	Beschreibung
PowerTerm InterConnect	<p>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.</p> <p>Das PowerTerm InterConnect (powerterm)-Paket muss installiert sein. Die Software ist lizenzpflichtig und ist bei unseren Vertriebspartnern erhältlich.</p>
eterm	<p>eterm ist eine Terminalemulationssuite, die folgende Emulationen enthält: Siemens 97801 (7 & 8 Bit), ANSI, AT386, BA-80, VT320.</p> <p>Das Eterm 97801 terminal emulation (eterm)-Paket muss installiert sein.</p> <p>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.</p>
Virtual Network Computing	<p>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.</p> <p>Der Dialog Emulationen dient zur Konfiguration des VNC Viewers, der als Open Source Komponente kostenlos in die eLux Software integriert ist.</p> <p>Das VNC client-Paket des eLux-Pakets X Org muss installiert sein. Für weitere Informationen siehe Spiegelung im Scout Enterprise-Handbuch.</p>
X11	<p>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.</p> <p>Der X11-Server von The XFree86 Project, Inc. (http://www.xfree86.org) ist im Xorg-Paket enthalten und ist Teil des BaseOS.</p>

Für weitere Informationen zur Konfiguration siehe [PowerTerm InterConnect konfigurieren](#) und [X11-Anwendung konfigurieren](#) im Scout Enterprise-Handbuch.

¹Der Anwendungstyp `Emulation` steht in der Scout Enterprise-Konsole und lokal am eLux RP 5-Client zur Anwendungsdefinition zur Verfügung, aber nicht am eLux RP 6-Client. eLux RP 6-Clients können über die Scout Enterprise-Konsole definierte Emulationen nutzen.

7.8.1. X11-Anwendung definieren

1. Fügen Sie eine **neue Anwendung hinzu** und wählen Sie den Anwendungstyp **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



Hinweis

Das **PowerTerm** Software-Paket muss auf dem Client installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

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 den Anwendungstyp **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.										
Parameter	<p>Optionale Aufruf-Parameter für die PowerTerm-Anwendung:</p> <table> <tr> <td><code>-fullscreen</code></td><td>Vollbild</td></tr> <tr> <td><code>-maximize</code></td><td>Maximiertes Fenster</td></tr> <tr> <td><code>-no-menu-bar</code></td><td>keine Menüleiste</td></tr> <tr> <td><code>-no-tool-bar</code></td><td>keine Toolbar</td></tr> <tr> <td><code>[myName].pts</code></td><td>Name einer individuellen PowerTerm-Konfigurationsdatei des Clients</td></tr> </table> <p>Beispiel 1: <code>-fullscreen -no-menu-bar -no-tool-bar</code></p> <p>Beispiel 2: <code>-fullscreen ptconfig001.pts</code></p>	<code>-fullscreen</code>	Vollbild	<code>-maximize</code>	Maximiertes Fenster	<code>-no-menu-bar</code>	keine Menüleiste	<code>-no-tool-bar</code>	keine Toolbar	<code>[myName].pts</code>	Name einer individuellen PowerTerm-Konfigurationsdatei des Clients
<code>-fullscreen</code>	Vollbild										
<code>-maximize</code>	Maximiertes Fenster										
<code>-no-menu-bar</code>	keine Menüleiste										
<code>-no-tool-bar</code>	keine Toolbar										
<code>[myName].pts</code>	Name einer individuellen PowerTerm-Konfigurationsdatei des Clients										
Terminal-konfigurationsdatei	Wählen Sie die zu übertragende <code>.pts</code> -Datei des Referenz-Clients aus dem Dateisystem.										
Kommunikations-datei	Wählen Sie die zu übertragende <code>.ptc</code> -Datei des Referenz-Clients aus dem Dateisystem.										
Tastaturdatei	Wählen Sie die zu übertragende <code>.ptk</code> -Datei des Referenz-Clients aus dem Dateisystem.										
Power PAD-Datei	Wählen Sie die zu übertragende <code>.ptp</code> -Datei des Referenz-Clients aus dem Dateisystem.										
Schaltfläche x	<p>Löschen Sie ggf. eine ausgewählte Konfigurationsdatei aus der Scout Enterprise-Datenbank.</p> <p>Zum Löschen der Datei am Client ist der Grundzustand (Factory Reset) des Clients erforderlich.</p>										

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.mylux.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 den Anwendungstyp **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**.

Zwei Optionen zur Konfiguration stehen zur Verfügung:

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 <code>/setup/sapgui/platin.ini</code> . Für weitere Informationen zur Dateiübertragung siehe Konfigurierte Dateiübertragung .



Hinweis

Weitere Informationen zur lokalen Konfiguration der SAPGUI und zur SAP-Konfigurationsdatei finden Sie in der SAP-Dokumentation.

7.10. Anwendungen im Kiosk-Modus

Bestimmte Anwendungen können so konfiguriert werden, dass sie vom Benutzer nur im Kiosk-Modus bedient werden können.

¹ab Scout Enterprise Management Suite Version 14.7

Im Kiosk-Modus wird die Anwendung als Fullscreen-Fenster geöffnet. Der Benutzer kann keine weiteren Fenster öffnen und die Anwendung nicht beenden. Die Verbindungs-Einstellungen und die Ressourcen, auf die die Benutzer am Backend zugreifen dürfen wie beispielsweise Citrix-Stores, werden über eine Konfigurationsdatei vordefiniert. Die Definition von Anwendungen für den Benutzer wird damit obsolet.

Der Client startet nach dem Systemstart die über Konfigurationsdateien festgelegte Anwendung im Kiosk-Modus, so dass sich der Benutzer direkt in der vorgesehenen Arbeitsumgebung befindet und nicht ausbrechen kann.

Der Kiosk-Modus wird ab eLux RP 6.2 für die Citrix Self-Service-Benutzeroberfläche mit Erweiterungen unterstützt. Ab eLux RP 6.5 kann der Builtin Browser im Kiosk-Modus ausgeführt werden.¹

7.10.1. Citrix Self-Service-Benutzeroberfläche im Kiosk-Modus

– ab eLux RP 6.2 –

Die Citrix Self-Service-Benutzeroberfläche mit Erweiterungen wird ab eLux RP 6.2 nicht mehr als benutzerdefinierte Anwendung `ucselfservice` mit freien Parametern konfiguriert. Die Definition einer Anwendung entfällt, stattdessen konfigurieren Sie den Kiosk-Modus. Alle relevanten Parameter werden in der Konfigurationsdatei `kioskmode.ini` definiert. Erweiterte Funktionalität und MultiStore-Option sind ebenfalls konfigurierbar.

Citrix Self-Service im Kiosk-Modus definieren



Hinweis

Das eLux-Paket **Citrix Workspace app for Linux** oder **Citrix Receiver for Linux 13.x** muss installiert sein.

Das eLux-Paket **Citrix Extensions 2.x²** oder höher und das hierin enthaltene Feature-Paket **Self-service wrapper** müssen installiert sein.

Für Anpassungen am Citrix-Dialog-Design müssen weitere Feature-Pakete auf den Clients installiert sein:

Dialog Extension und **Self-service dialog themes**

Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Geräte-Konfiguration > Erweiterte Dateieinträge** und definieren Sie folgenden Eintrag:

Datei	/setup/terminal.ini
Abschnitt	Layout

¹Für ältere Versionen verwenden Sie Firefox im Kiosk-Modus.

²früher Citrix Receiver Extensions

Eintrag	KioskMode
Wert	1

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

Dieser Parameter aktiviert den Kiosk-Modus für die Self-Service-Oberfläche mit Erweiterungen.

- Erstellen Sie die Textdatei `kioskmode.ini` und darin den Abschnitt `[Parameters]`. Fügen Sie die gewünschten Parameter ein:¹

Parameter	Beschreibung
<code>ReconnectOnLogon=true false</code>	Legt fest, ob die SelfService-Oberfläche versucht, direkt nach der Anmeldung an einem Store alle Sitzungen für diesen Store wiederzuverbinden (Citrix SelfService-Option)
<code>ReconnectOnLaunchOrRefresh=true false</code>	Legt fest, ob die SelfService-Oberfläche versucht, alle Sitzungen wiederzuverbinden, sobald eine Anwendung gestartet oder der Store aktualisiert wird (Citrix SelfService-Option)
<code>SharedUserMode=true false</code>	Wenn der Shared User Mode aktiviert ist, verwendet die SelfService-Oberfläche ein Systemkonto für mehrere Benutzer. Die Benutzerdaten werden beim Schließen oder Abmelden gelöscht. (Citrix SelfService-Option) Wir empfehlen, diesen Parameter nicht mit <code>Prelogin=true</code> zu verwenden.
<code>SelfSelection=true false</code>	Wird zur Deaktivierung des Suchfeldes und der Self-Selection-Leiste (alte Oberfläche) verwendet Das Deaktivieren verhindert, dass Benutzer weitere Anwendungen abonnieren können.
<code>LogoffMode=0 1 2 3</code>	0 Keine automatische Abmeldung 1 Abmelden-Timer wird mit der Anmeldung gestartet 2 Abmelden-Timer wird nach Beenden der letzten Citrix-Anwendung/Desktop gestartet 3 Abmelden-Timer wird mit dem Öffnen der ersten Citrix-Anwendung/Desktop gestartet
<code>LogoffDelay=<seconds></code>	Verzögerung in Sekunden beim Starten des Abmelden-Timers

¹Default-Werte sind **fett** dargestellt

Parameter	Beschreibung
LogoffInfoTimeout=<seconds>	Zeigt während der Abmeldung eine Meldung für n Sekunden
ShowLastUser=true false	Zeigt im Benutzer -Feld den zuletzt angemeldeten Benutzer
PreLogin=true false	Legt fest, ob bei der Anmeldung eine Dropdown-Liste mit vorkonfigurierten Stores angezeigt wird (MultiStore). Wir empfehlen, diesen Parameter nicht zusammen mit SharedUserMode=true zu verwenden.
PreLoginTitle	Dialogtitel für die Store-Auswahl (MultiStore)
PassThroughMode=0 1	0 Keine Passthrough-Anmeldedaten 1 Active Directory
Domain<1-N>=<Domänen-Anzeigenname,Domäne>	Jeder Eintrag enthält eine Domäne.

3. Um den Zugriff auf die Stores zu definieren, fügen Sie in der Datei `kioskmode.ini` einen oder mehreren Abschnitte `[Store<1-N>]` oder `[Environment_Store<1-N>]` ein.

Wenn Sie Stores mit `[Environment_Store<N>]` definieren, kann der Benutzer über die Schaltfläche **Store** in der Taskleiste zwischen den Stores wechseln. Die Stores werden in Gruppen (Environment) angezeigt.

`[Store<1-N>]`

Parameter	Beschreibung
Url=<Store-URL>	URL des Citrix-Stores
FriendlyName=<Anzeigename>	Anzeigename für den Citrix-Store
Default=true false	Legt fest, ob dieser Store als Standard angezeigt wird
AutostartResources=<App/Desktop1;App/Desktop2;...>	Liste der Citrix-Anwendungen/Desktops, die automatisch nach der Anmeldung gestartet werden sollen Zur Zeit nur verfügbar mit <code>PreLogin=true</code>

`[Environment_Store<N>]`

Parameter	Beschreibung
Url=<Store-URL>	URL des Citrix-Stores
FriendlyName=<Anzeigename>	Anzeigename für den Citrix-Store
Default=true false	Legt fest, ob dieser Store als Standard angezeigt wird

Parameter	Beschreibung
Environment=<Gruppenname>	Gibt die Gruppe an, nach der die Stores gruppiert werden (frei definierbare Zeichenfolge)
AutostartResources=<App/Desktop1;App/desktop2;...>	Liste der Citrix-Anwendungen/Desktops, die automatisch nach der Anmeldung gestartet werden sollen Zur Zeit nur verfügbar mit PreLogin=true

4. Um das Design der Citrix-Dialoge für alle Citrix-Verbindungen anzupassen, fügen Sie in der Datei `kioskmode.ini` einen Abschnitt [Theme] ein:

Parameter	Beschreibung
ThemeName=<Name des Themes>	Name des Citrix-Themes Default: <code>ucselfservice</code>
Decorated=true false	Legt fest, ob die Fenster mit Fenster-Dekoration angezeigt werden
ColorHover=<RGB-Farbcode>	Hintergrundfarbe für Listenelemente beim Zeigen mit der Maus (Citrix list selection widgets) Default: <code>#e6f1f7</code>
ColorUnselected=<RGB-Farbcode>	Hintergrundfarbe für nicht ausgewählte Listenelemente (Citrix list selection widgets) Default: <code>#ffffff</code>
ColorSelected=<RGB-Farbcode>	Hintergrundfarbe für ausgewählte Listenelemente (Citrix list selection widgets) Default: <code>#cce3f0</code>

5. Übertragen Sie die Datei `kioskmode.ini` auf die Clients nach `/setup/kioskmode.ini`. Verwenden Sie dazu die Funktion **Konfigurierte Dateiübertragung**. Für weitere Informationen siehe [Konfigurierte Dateiübertragung](#).

Der `terminal.ini`-Eintrag zusammen mit der Datei `kioskmode.ini` auf dem Client bewirken, dass der Client nach dem Starten die Citrix Self-Service-Oberfläche im Kiosk-Modus öffnet. Dem Benutzer stehen die konfigurierten Stores zur Verfügung. Neben der Self-Service-Oberfläche können keine anderen Anwendungen gestartet werden.



Hinweis

Wenn mehrere Stores definiert sind, kann der Benutzer zwischen den Stores wechseln, indem er bei gedrückter UMSCHALT-Taste auf die Schaltfläche **Store** in der Taskleiste klickt.

Beispiel für kioskmode.ini

```
[Parameters]
ReconnectOnLogon=true
ReconnectOnLaunchOrRefresh=true
SharedUserMode=true
SelfSelection=false
ShowLastUser=true
LogoffMode=3
LogoffDelay=10

[Store1]
Url=https://xd7a/int.sampletec-01.com/Citrix/Store/discovery
FriendlyName=XenApp A

[Environment_Store1]
Url=https://xd7b./int.sampletec-01.com/Citrix/Store/discovery
FriendlyName=XenApp B
Default=true
Environment=PROD

[Environment_Store2]
Url=https://xd7c./int.sampletec-01.com/Citrix/Store/discovery
FriendlyName=XenApp C
Default=false
Environment=INT

[Theme]
ThemeName=ucselfservice
Decorated=false
ColorHover=#b0b0b0
ColorUnselected=#a0a0a0
ColorSelected=#c0c0c0
```

7.10.2. Builtin-Browser im Kiosk-Modus

– ab eLux RP 6.5 –

Im Kiosk-Modus wird der Browser als Fullscreen-Anwendung geöffnet. Der Benutzer kann keine weiteren Fenster öffnen und den Browser nicht beenden. Beachten Sie, dass der Builtin-Browser, wenn er als Anwendung definiert wird, nicht im Kiosk-Modus ausgeführt wird, obwohl Adress- und Navigationsleiste nicht angezeigt werden.



Hinweis

Firefox kann bis zur Version ESR 52.8 ¹ im Kiosk-Modus ausgeführt werden. Die Firefox-Version ESR 60² unterstützt den Kiosk-Modus nicht mehr. Für weitere Informationen siehe [Kiosk-Modus für Firefox](#).

Builtin-Browser im Kiosk-Modus definieren

1. Öffnen Sie in der Scout Enterprise-Konsole für die relevanten Clients die **Erweiterte Geräte-Konfiguration** > **Erweiterte Dateieinträge** und definieren Sie folgenden Eintrag:

Datei	/setup/terminal.ini
Abschnitt	Layout
Eintrag	KioskMode
Wert	2

Für weitere Informationen siehe [Erweiterte Dateieinträge](#).

Dieser Parameter aktiviert den Kiosk-Modus für die Browser-Anwendung.

2. Erstellen Sie die Textdatei `kioskmode.ini` und darin den Abschnitt `[Browser1]`.
3. Fügen Sie darunter die gewünschten Parameter ein:³

Parameter	Beschreibung
Url=<URL of startup page>	Webseite (URL), die unmittelbar nach dem Starten des Browsers öffnet (Anfangsseite)
Homepage=<URL of homepage>	Webseite (URL), die beim Klicken auf Home öffnet
SaveFirstLink=true false	Wenn Sie true setzen, wird die erste URL, die nach der Startseite geladen wird, als neue Startseite gespeichert.

¹im eLux RP 6.4-Container enthalten

²im eLux RP 6.5-Container enthalten

³Default-Werte sind **fett** dargestellt

Parameter	Beschreibung
Navbar=true false	Legt fest, ob die Navigationsleiste angezeigt wird
NavbarPrint=true false	Legt fest, ob auf der Navigationsleiste die Drucken -Schaltfläche angezeigt wird
NavbarForward=true false	Legt fest, ob auf der Navigationsleiste die Vorwärts -Schaltfläche angezeigt wird
NavbarBackward=true false	Legt fest, ob auf der Navigationsleiste die Zurück -Schaltfläche angezeigt wird
NavbarHome=true false	Legt fest, ob auf der Navigationsleiste die Home -Schaltfläche angezeigt wird
NavbarUrl=true false	Legt fest, ob die Adressleiste angezeigt wird
NavbarRefresh=true false	Legt fest, ob auf der Navigationsleiste die Aktualisieren -Schaltfläche angezeigt wird

- Übertragen Sie die Datei `kioskmode.ini` auf die Clients nach `/setup/kioskmode.ini`. Verwenden Sie dazu die Funktion **Konfigurierte Dateiübertragung**. Für weitere Informationen siehe [Konfigurierte Dateiübertragung](#).

Der `terminal.ini`-Eintrag zusammen mit der Datei `kioskmode.ini` auf dem Client bewirken, dass nach dem Systemstart der Builtin-Browser im Kiosk-Modus öffnet. Dem Benutzer stehen die konfigurierten Funktionen zur Verfügung. Neben dem Browser können keine anderen Anwendungen gestartet werden.



Hinweis

Für die korrekte Verwendung des Kiosk-Modus empfehlen wir, die Benutzerrechte für den Client einzuschränken.

Unterschiedliche Webseiten für Geräte/OUs definieren

– ab eLux RP 6.7 –

Wenn Ihre Geräte mit unterschiedlichen Seiten starten sollen oder unterschiedliche Startseiten (Home) haben sollen, können Sie die Webseiten über Umgebungsvariablen parametrisieren. Führen Sie dazu oben beschriebene Schritte mit den folgenden Abweichungen durch:

- Fügen Sie in der `kioskmode.ini` im Abschnitt `[Browser1]` für den ersten und/oder zweiten Wert eine Variable ein. Beispiel:

```
Url=$URL1
```

```
Homepage=$URL2
```

- Definieren Sie die in der `kioskmode.ini` verwendeten Variablen als Umgebungsvariablen für die relevanten Geräte (Erweiterte Geräte-Konfiguration). Beispiel:

```
URL1=https://www.unicon-software.com
```

URL2=`https://www.unicon-software.com/myeluxcom/`

Für weitere Informationen siehe [Umgebungsvariablen](#).

7.11. Problembehandlung Anwendungsdefinition

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.
Probleme mit Zertifikaten in Kombination mit VMware-Server	Es liegt ein Server-Problem vor: Der VMware-Server verwendet nach der Installation ein Self-signed-Zertifikat. Wenn der Client richtig konfiguriert ist, akzeptiert er dieses Zertifikat nicht. Grund: Für Serverzertifikate muss der FQDN (fully qualified domain name) eingetragen sein.	Erstellen Sie in der Windows-CA ein Serverzertifikat mit FQDN. In der MMC verwenden Sie das Snap-In Certificates (Local Computer) . Der Schlüssel muss exportierbar sein. Der Anzeigename des Servers muss vdm lauten. Im Zertifikatspeicher Local Computer/Personal darf nur ein Zertifikat mit diesem Namen existieren.

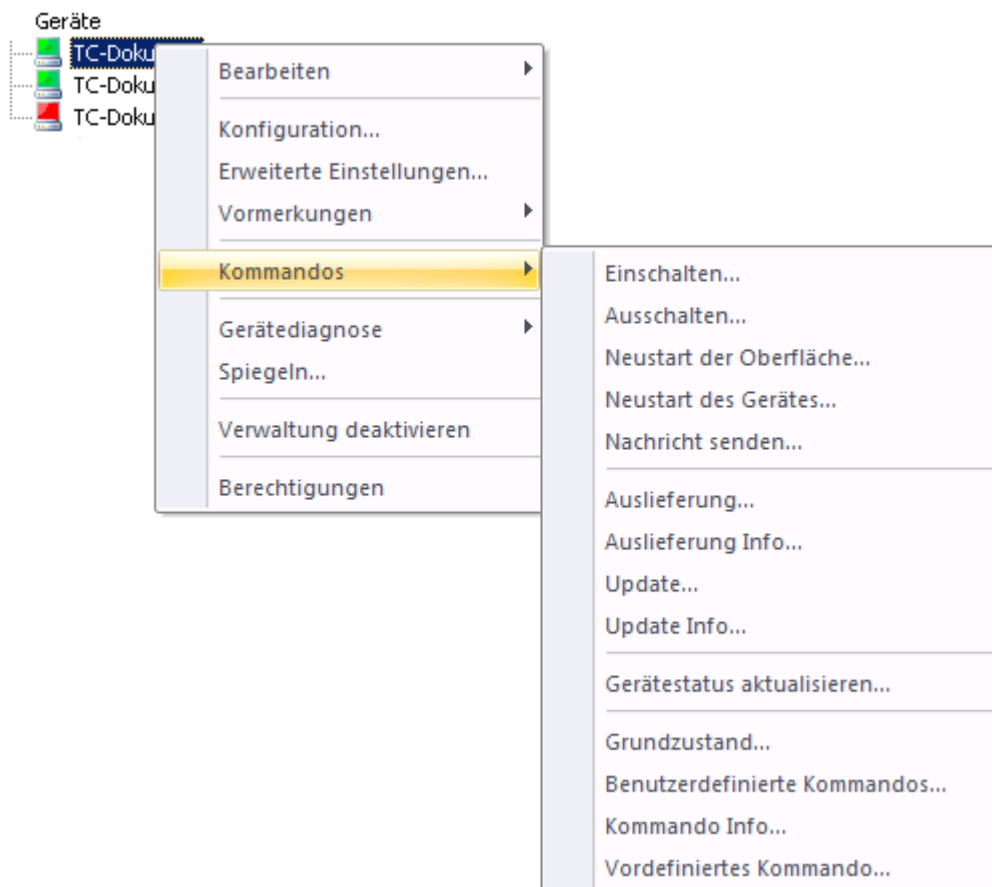
Fehler / Problem	Ursache	Lösung
COM-Port-Redirection mit RDP funktioniert nicht	Kommunikationsfehler (z.B. hohe Latenzen im Netzwerk) zwischen Ihrem seriellen Endgerät und dem virtuellen Desktop erlauben keine serielle Kommunikation.	<p>Schalten Sie den permissive mode für die RDP-Anwendung ein. Dieser Schalter bewirkt, dass Kommunikationsfehler auf Warnungen heruntergestuft werden, und die Kommunikation wird in Bezug auf Timeouts toleranter.</p> <p>Setzen Sie in Ihrer RDP-Anwendungsdefinition einen Freien Parameter mit der Option permissive.</p> <p>Beispiel:</p> <pre>FreeRDPParams=/serial:COM1,/dev/ttyS0,Serial,permissive</pre> <p>Für weitere Informationen siehe Freie Anwendungsparameter definieren.</p>

8. 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.



8.1. 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 der Oberfläche	Startet die eLux-Oberfläche neu
Neustart des Gerätes...	Startet das Gerät/die Geräte 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. Für weitere Informationen siehe Kommando Grundzustand .
Benutzerdefiniertes Kommando...	Eingabe eines benutzerdefiniertes Kommandos, das an das Gerät/die Geräte gesendet wird Beispiele: Lizenz-Lease aktualisieren, BIOS-Update durchführen



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 .
eLux Command Scheduler unterbrechen	Wenn vom Administrator wiederkehrende Kommandos definiert wurden, die lokal am Gerät durch den eLux Command Scheduler eingeplant werden (Cron-jobs), wird die Ausführung dieser Kommandos bis zum nächsten Neustart des Gerätes ausgesetzt.
Konfigurationslauf... (nicht für einzelne Geräte)	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

8.2. Kommando ausführen

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.

DE.DE_KA.DE_KA_2.TC-MMI-S920

Kommando: Neustart des Geräts

☒ Benutzer informieren für 60 sek.
☐ Benutzer kann Kommando abbrechen

☒ Sofort
☐ Einmalig Datum: Freitag ,06.09.2019 Zeit: 19:00
☐ Wiederholend Monatstag: 1, 2, 3, 4 Zeit: 11:48

Bei mehreren Geräten nach jedem Kommando 0 ms warten

Ausführen Abbrechen

Der **Kommando**-Dialog öffnet. Je nach ausgewähltem Kommando können die Optionen variieren.

3. Um den Inhalt der Fenstertitelzeile vollständig anzuzeigen, bewegen Sie den Mauszeiger auf die Fenstertitelzeile.

In der Titelleiste wird das betroffene Gerät oder die betroffene OU angezeigt.

4. Bearbeiten Sie folgende Felder:

Option	Beschreibung
Kommando	Erlaubt den Wechsel zu einem anderen Kommando
Benutzer informieren	Der Benutzer wird vor der Kommando-Ausführung durch eine Benachrichtigung informiert. Geben Sie die Zeitspanne in Sekunden für die Anzeige der Benachrichtigung an. Danach wird das Kommando ausgeführt. Wenn 0, wird die Benachrichtigung so lange angezeigt, bis der Benutzer die Ausführung des Kommandos via Schaltfläche bestätigt.
Benutzer darf abbrechen	Der Benutzer darf die Ausführung des Kommandos via Schaltfläche verhindern.
Mit Systemrechten ausführen	Manche Kommandos erfordern Systemrechte, die vor der Ausführung überprüft werden.
Sofort/Einmalig/Wiederholend	Zeitpunkt der Ausführung, periodische Wiederholung
Bei mehreren Geräten warten	Verzögerung nach der Ausführung, wenn mehrere Geräte betroffen sind
Untergruppen einbeziehen	Untergeordnete OUs einbeziehen, wenn vorhanden

5. Bestätigen Sie mit **Ausführen**.

Das Kommando wird zum definierten Zeitpunkt ausgeführt. Je nach Kommando wird eine Meldung angezeigt, die Sie bestätigen müssen.

8.3. Kommando einplanen

Die Durchführung der meisten Kommandos kann für einen definierten Zeitpunkt eingeplant statt sofort ausgeführt werden. Viele Kommandos können auch monatlich oder wöchentlich wiederkehrend eingeplant werden, beispielsweise das Einspielen eines Firmware-Updates.

- Öffnen Sie für das relevante Gerät, die OU oder die Dynamische Gerätegruppe das Kontextmenü und wählen Sie **Kommandos**.
- Wählen Sie aus dem Untermenü das gewünschte Kommando.
- Wählen Sie als Zeitpunkt der Ausführung **Einmalig** oder **Wiederholend**.
Wählen Sie dann das Datum oder für wiederholende Ausführung den Tag im Monat oder in der Woche.
Wählen Sie schließlich die Uhrzeit.
- Bearbeiten Sie die weiteren Optionen des **Kommando**-Dialoges
- Bestätigen Sie mit **Ausführen**.

Das Kommando wird zum definierten Zeitpunkt ausgeführt. Alle eingeplanten Kommandos (einmalig und wiederholend) können unter **Ansicht > Zeitplanung** angezeigt, geändert und gelöscht werden.

8.4. Kommando-Ergebnisse und Update-Informationen

Rückmeldungen über durchgeführte Update-, Auslieferungs- und benutzerdefinierte Kommandos erhalten Sie

- für das jeweilige Gerät im **Eigenschaften**-Fenster und im Dialog **Update-Info/Kommando-Info**
- für alle Geräte im Fenster **Kommandoverlauf**.


Alle Vorgänge werden aufgezeichnet, auch wenn das Kommando abgebrochen wurde oder gar nicht ausgeführt wurde, da beispielsweise bei einem Update-Kommando das entsprechende Image aktuell war. Vollständig durchgeführte Kommandos werden grün gekennzeichnet. Für weitere Informationen siehe [Kommandoverlauf](#).

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. Um das Eigenschaften-Fenster anzuzeigen, wählen Sie **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 Imagedefinitions-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

¹Ab Scout Enterprise Management Suite Version 14.8

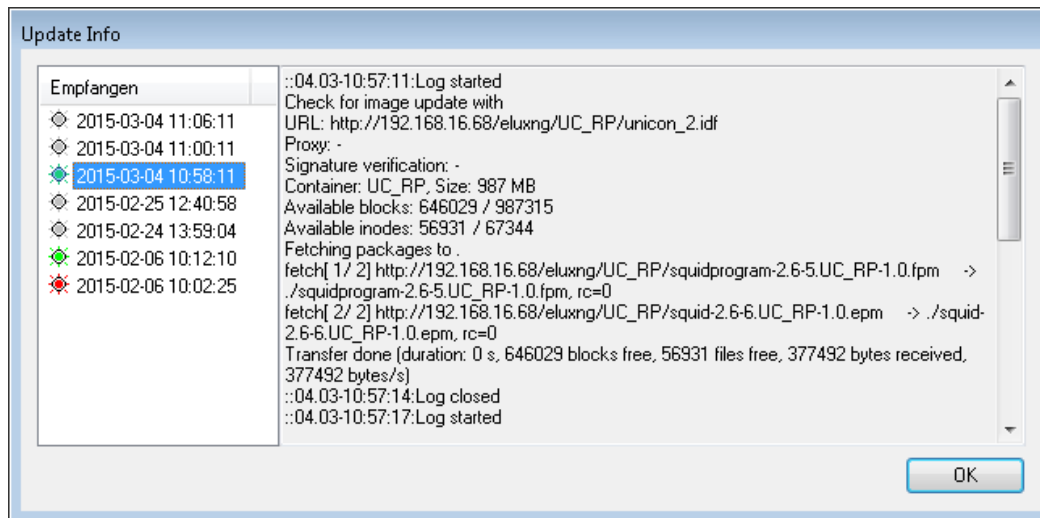


Hinweis

Die Eigenschaften **Update-Provider** und **Update-Größe** werden nur bei einem Update, aber nicht bei der Migration auf eine höhere Hauptversion und nicht beim Downgrade ausgewertet.

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 worden sein, da die Image-Datei aktuell war. Für ein markiertes Update-Kommando werden rechts alle Protokoll-Informationen 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](#).

8.5. 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	<p>Klicken Sie auf eine Spaltenüberschrift.</p> <p><i>Der erste Klick sortiert die Jobs aufsteigend nach dem ausgewähltem Wert; der zweite Klick sortiert absteigend.</i></p> <p><i>Klick auf die F5-Taste stellt die Standardsortierung wieder her.</i></p>

Auf einen markierten Job können Sie folgende Funktionen anwenden:

Funktion	Aktion
Details anzeigen	<p>Klicken Sie auf Details....</p> <p><i>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.</i></p>
Objekt in der Baumansicht der Scout Enterprise-Konsole suchen	<p>Klicken Sie mit der rechten Maustaste auf einen Objektnamen und wählen Sie In Baumansicht suchen.</p> <p><i>Der erste Treffer wird in der Baumansicht markiert.</i></p>
Laufenden Job beenden	<p>Markieren Sie einen Job mit Status Läuft und klicken Sie auf Beenden.</p> <p><i>Eine Beenden-Anforderung für das Kommando wird an den Scout Enterprise-Server gesendet. Die Übermittlung des Kommandos an die Geräte wird dadurch gestoppt.</i></p>

8.6. Kommando Grundzustand

Das Kommando **Grundzustand** setzt die relevanten Geräte zurück auf den Grundzustand. Standardmäßig werden die lokale Geräte-Konfiguration und lokale Anwendungsdefinitionen gelöscht.

Folgende Daten bleiben standardmäßig erhalten:

- Verbindung zum Scout Enterprise-Server mit Server-Adresse und OU-ID
- Lizenzinformationen
- Das installierte Image mit allen Software-Paketen (Firmware)

Nachdem das Gerät das Kommando **Grundzustand** erhält, wird die aktuelle Konfiguration am Gerät zurückgesetzt und das Gerät wird neu gestartet. Das Gerät verbindet sich zum Scout Enterprise-Server und erhält von diesem die Konfiguration der OU, der es zugeordnet ist.

Das Kommando kann mit folgenden zusätzlichen Optionen gestartet werden:

Option	Beschreibung
Lokale Konfiguration bei-behalten (nicht-gesperrte Felder) ¹	Benutzerdefinierte Werte der lokalen Geräte-Konfiguration in erlaubten Feldern bleiben erhalten. Dies bezieht sich nur auf Felder, die der Benutzer bearbeiten darf. Für weitere Informationen siehe Lokale Konfiguration schützen .
Scout Enterprise-Server-Adresse am Client löschen	Folgende Daten werden zusätzlich zu den Konfigurationsdaten gelöscht: <ul style="list-style-type: none">• Adresse der Scout Enterprise-Server-Maschine• Zertifikate in <code>/setup/cacerts</code>• WLAN-Konfiguration• 802.1X-Konfiguration• in TPM 2.0-Modul gespeicherte private Schlüssel eines SCEP Client-Zertifikates²• Eine über TPM 2.0 verschlüsselte Setup-Partition wird entschlüsselt.³

¹ab Scout Enterprise 15.7 und eLux RP 6.7

²ab eLux RP 6.7

³ab eLux RP 6.7

Option	Beschreibung
Am Client gespeicherte Lizenzen löschen ¹	<p>Lokal gespeicherte Lizenzen (eLux RP 5)² oder die Lizenz-Lease (eLux RP 6) werden zusätzlich zur Konfiguration und oben gelisteten Daten gelöscht. Diese Option kann beispielsweise für den Abverkauf des Gerätes verwendet werden.</p> <p>Danach wird das Gerät heruntergefahren und bleibt ausgeschaltet.</p> <p>Das Kommando Grundzustand mit dieser Option entspricht dem lokalen Zurücksetzen des Clients über die Schaltfläche Grundzustand im erweiterten Command panel in eLux.³ Für weitere Informationen siehe Client auf Grundzustand zurücksetzen im eLux RP-Handbuch.</p>



Hinweis

Das Kommando **Grundzustand** wirkt sich auf die Setup-Partition des Thin Clients aus. Die System-Partition mit installierter Firmware ist vom Grundzustand nicht betroffen und wird ausschließlich über das Kommando **Update** mit der Option **Systempartition vor dem Update formatieren** verändert.

8.7. Vordefinierte Kommandos erstellen

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. Eine andere Anwendung ist das Script zur Erneuerung der Lease-Gültigkeit von eLux RP 6-Clients.

Diese Kommandos sind anschließend über den Kommando-Dialog verfügbar und können von berechtigten Administratoren angewendet werden.

1. Wählen Sie im Scout Enterprise-Menü **Optionen > Erweiterte Optionen > Vordefinierte Kommandos**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

¹bis Scout Enterprise Management Suite Version 14.9 und eLux RP 5

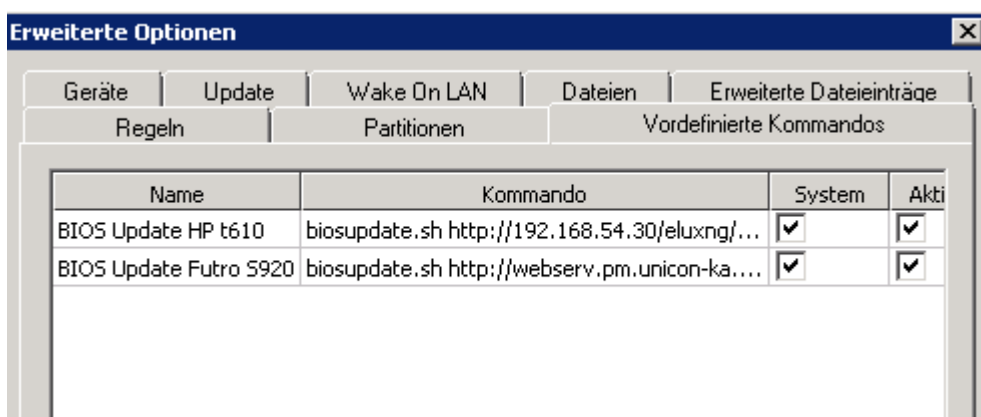
²Ab eLux RP 6 werden keine Lizenzen lokal am Client gespeichert.

³Für eLux RP 5: Die Schaltfläche **Grundzustand** befindet sich in der Systemsteuerung im Register **Firmware**.

3. Bearbeiten Sie folgende Optionen für Ihrem neuen Eintrag:

Option	Beschreibung
Name	Der Kommandoname wird den Administratoren im Kommando-Dialog angezeigt; das eigentliche Kommando wird nicht angezeigt.
Kommando	<p>Syntax für das auszuführende Kommando</p> <p>Damit ein Administrator beim Ausführen eines vordefinierten Kommandos individuelle Werte setzen kann, können Sie Variablen verwenden.¹ Die Werte für jede Variable werden vom Administrator abgefragt, sobald er das vordefinierte Kommando im Kommando-Dialog auswählt.</p> <p>Beispiel: <code>ls -__PARAMS__ __FILES__</code></p> <p>Korrekte Schreibweise für Variablen: Zwei Unterstriche gefolgt vom Variablennamen gefolgt von zwei Unterstrichen</p> <p>Der Variablenname darf Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten.</p>
System	Für das Ausführen des Kommandos sind Systemrechte erforderlich.
Aktiviert	Das Kommando wird im Listenfeld für vordefinierte Kommandos angezeigt.

4. 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.

Für die berechtigten Administratoren wird statt dem Befehl der Name des Kommandos angezeigt

- im **Kommando**-Dialog
- im Eigenschaften-Fenster des Gerätes unter **Kommandozeile**²

¹ab Scout Enterprise Management Suite 15.9

²ab Scout Enterprise Management Suite 15.7

- in der **Kommando-Info** (Historie für das relevante Geräte)¹

8.8. Vorlagen für Standard-Kommandos definieren

Für Standard-Kommandos wie **Neustart** oder **Update** können Sie Kommando-Vorlagen definieren.²

1. Wählen Sie im Scout Enterprise-Menü **Optionen > Erweiterte Optionen > Vordefinierte Kommandos**.
2. Aktivieren Sie unter **Kommando-Vorlagen** die Option **Vorlage für Kommando** und wählen Sie im Listenfeld das gewünschte Kommando.
3. Um Voreinstellungen verpflichtend zu definieren, aktivieren Sie die Option **Vorlage ist nicht veränderbar**.

Wenn eine Vorlage veränderbar ist, können die ausführenden Administratoren die angegebenen Standard-Werte überschreiben.

4. Legen Sie die Werte für die gewünschten Voreinstellungen des ausgewählten Kommandos fest.

Kommando-Vorlagen

☐ Vorlage für Kommando Grundzustand ▼ verwenden

☐ Vorlage ist nicht veränderbar

☐ Benutzer informieren für sek.

☐ Kommando kann vom Benutzer abgebrochen werden

☐ Scout-Server-Adresse am Client löschen

☐ Am Client gespeicherte Lizenzen löschen

In einer Vorlage können Sie neben Kommando-spezifischen Optionen folgende allgemeine Optionen vorbelegen:

Benutzer informieren für x Sekunden

Kommando darf vom Benutzer abgebrochen werden



Hinweis

Voreinstellungen für Standard-Kommandos sind nur in der Scout Enterprise-Konsole und nicht in Scout Enterprise-Dashboard verfügbar.

¹ab Scout Enterprise Management Suite 15.7

²ab Scout Enterprise Management Suite 15.2

8.9. eLux Command Scheduler

– ab eLux RP 6.8 und Scout Enterprise 15.8 –

Wiederkehrende Kommandos können so definiert werden, dass sie lokal am Gerät durch den eLux Command Scheduler eingeplant und ausgeführt werden. Diese Kommandos werden wie Cronjobs zu festgelegten Zeiten vom Gerät initiiert im Gegensatz zu den Server-seitig initiierten Scout Enterprise-Kommandos. Der Zeitpunkt der Ausführung richtet sich entsprechend nach der Zeitzone, in der sich das Gerät befindet.

Zur Definition muss der Administrator eine `.ini`-Datei zu den Clients schicken, die alle Kommando-Definitionen enthält. Folgende Kommandos kann der eLux Command Scheduler verarbeiten:

- Firmware-Update einspielen
- Geräte-Konfiguration synchronisieren
- Gerät neu starten

Wiederkehrende Kommandos für den eLux Command Scheduler definieren

1. Erstellen Sie eine Textdatei mit Namen `scheduler.ini`
2. Erstellen Sie für jede Kommando-Definition einen Abschnitt `[Job<N>]`
3. Definieren Sie für jeden Abschnitt folgende Parameter:

Parameter	Beschreibung
<code>Id=<Eindeutige Zeichenfolge></code>	Zeichenfolge zur eindeutigen Identifizierung des Kommandos
<code>Type=1 2 3</code>	Kommandotyp
	1 Update
	2 Konfiguration synchronisieren
	3 Neustart

Parameter	Beschreibung
Schedule=<Zeitpunkt der Ausführung>	<p>Das Format richtet sich nach den systemd calendar events. Syntax für einen Zeitstempel: Tue 2020-01-21 11:12:13</p> <p>Jede Minute *-*-* *:*:00 Stündlich *-*-* *:00:00 Täglich *-*-* 00:00:00 Monatlich *-*-*01 00:00:00 Wöchentlich Mon *-*-* 00:00:00</p> <p>Beispiele:</p> <p>*-*-* 4:00:00 Täglich um 4:00 Uhr Mon..Fri *-*-* 22:30 Täglich werktags um 22:30 Uhr -*-*1,5 11:12 Jeden ersten und fünften des Monats um 11:12. Uhr Sun 2020-*-* 17:15 Jeden Sonntag des Jahres 2020 um 17:15 Uhr</p> <p>Für weitere Informationen siehe https://www.freedesktop.org/software/systemd/man/systemd.time.html</p>
SpreadFactor=<Verzögerung>	<p>Zeitspanne, innerhalb der zufällige Verzögerungen generiert werden, um die gleichzeitige Ausführung auf vielen Geräten zu verhindern</p> <p>Beispiele: 10m, 1h, 30s Bei Ausführungs-Zeitpunkt 18:00 Uhr und SpreadFactor=10m wird für die Ausführung des Kommandos pro Gerät ein zufällig generierter Zeit-Wert, der maximal bei 10 Minuten liegen kann, auf die Uhrzeit 18:00 Uhr addiert. Das Kommando wird also zwischen 18:00 Uhr und 18:10 Uhr ausgeführt.</p> <p>Default: 0</p>
Persistent=true false	<p>Versäumte Kommando-Ausführungen werden nach dem nächsten Gerätstart sofort nachgeholt. Wenn mehrere Wiederholungen desselben Kommandos eingeplant waren, wird das Kommando einmalig nachgeholt.</p>
WakeSystem=true false	<p>Bei true wird das System zur Ausführung des Kommandos aus dem Standby-Modus (Suspend) geweckt.</p>

Beispiel:

```
[Job1]
Id=001
Type=2
Schedule=Mon..Fri *-*-* 22:30
SpreadFactor=0
Persistent=false
WakeSystem=true
```

[Job2]

...

- Übertragen Sie die Datei mit Hilfe der Funktion **Konfigurierte Dateiübertragung** auf die Geräte nach `/setup/scheduler/scheduler.ini`
Für weitere Informationen siehe [Erweiterte Konfiguration > Dateien](#) im **Scout Enterprise-Handbuch**.

Beim nächsten Konfigurationstransfer wird die Datei übertragen. Die in der `.ini` Datei definierten Kommandos werden dem eLux Command Scheduler übergeben. Nach einem weiteren Neustart werden die Kommandos auf dem Gerät eingeplant und ausgeführt.

Informationen über den Status eines Kommandos und über die nächste Ausführung erhalten Sie mit
`systemctl status <jobId>.service` und
`systemctl status <jobId>.timer`

Verschieben-Option für die Benutzer

Ähnlich wie bei Scout Enterprise-Kommandos können Sie auch für die Kommando-Definitionen des eLux Command Schedulers definieren, ob die Benutzer vor der Kommando-Ausführung informiert werden, diese abbrechen oder verschieben dürfen.

- Verwenden Sie dazu in der Textdatei `scheduler.ini` innerhalb einer Kommando-Definition `Job<N>` folgende Parameter:

Parameter	Beschreibung
<code>InformUser=true false</code>	Der Benutzer wird vor der Kommando-Ausführung durch eine Benachrichtigung informiert.
<code>Timeout=<0-N></code>	Zeitspanne in Sekunden für die Anzeige der Benachrichtigung Danach wird das Kommando ausgeführt. Wenn 0, wird die Benachrichtigung so lange angezeigt, bis der Benutzer die Ausführung des Kommandos via Schaltfläche bestätigt.
<code>AllowUserCancel=true false</code>	Der Benutzer darf die Ausführung des Kommandos via Schaltfläche verhindern.
<code>NumberOfDeferments=<0-N></code>	Anzahl der erlaubten Verschiebungen Standardmäßig darf der Benutzer nicht verschieben.
<code>DefermentTimes=N1,N2...</code>	Komma-separierte Liste mit Integer-Werten (Minuten) für die Verzögerung Diese Werte werden dem Benutzer als mögliche Zeitintervalle zum Verschieben angeboten (Verzögerungen bis zur nächsten Erinnerung).

eLux Command Scheduler unterbrechen

Die regelmäßige Ausführung von definierten Kommandos durch den eLux Command Scheduler kann aus der Scout Enterprise-Konsole heraus vorübergehend ausgesetzt werden. Dazu schickt der Administrator ein Kommando an die relevanten Geräte, das den eLux Command Scheduler bis zum nächsten Neustart der Geräte anhält. Nach dem nächsten Gerätestart verarbeitet der eLux Command Scheduler die eingeplanten Kommandos wieder nach Plan.

1. Öffnen Sie für das relevante Gerät, die OU oder die Dynamische Gerätegruppe das Kontextmenü und wählen Sie **Kommandos > eLux Command Scheduler unterbrechen**.
2. Bestätigen Sie mit **Ausführen**.

Die Ausführung aller Kommandos, die der eLux Command Scheduler eingeplant hat, wird mit sofortiger Wirkung bis zum nächsten Neustart der Geräte ausgesetzt.



Hinweis

Wenn Kommandos mit `Persistent=true` definiert werden und das Gerät zum Zeitpunkt der geplanten Kommando-Ausführung ausgeschaltet ist, werden diese Kommandos (persistente Jobs) nach dem nächsten Neustart nachträglich gestartet.

9. Fernwartung

Für Wartung, Benutzer-Support und zur Überprüfung bestimmter Funktionalitäten auf den Clients stehen dem Administrator verschiedene Werkzeuge zur Verfügung

9.1. 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 Funktionalität überprüft werden.

9.1.1. Voraussetzungen

- VNC-Viewer
Auf dem Administrationssystem muss ein VNC-Viewer installiert sein. Dieser wird über die Scout Enterprise-Konsole zur Verfügung gestellt.
- VNC-Server
Auf dem Zielgerät muss ein VNC-Server installiert sein. Für eLux-Clients muss das im eLux-Paket **XOrg** enthaltene Feature-Paket **VNC Server extension** installiert sein. Dies kann eine Anpassung der Imagedefinitions-Datei am Webserver mit Hilfe von ELIAS erfordern.
- Konfiguration
Für das Zielgerät muss in **Geräte-Konfiguration > Sicherheit > Spiegelungseinstellungen** die Spiegelung aktiviert und konfiguriert sein. Für weitere Informationen siehe [Spiegelung konfigurieren](#).

9.1.2. 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. Die Meldung bleibt permanent im Vordergrund und erlaubt dem Gespiegelten jederzeit, die Sitzung zu beenden.

Spiegelungssitzung eröffnen



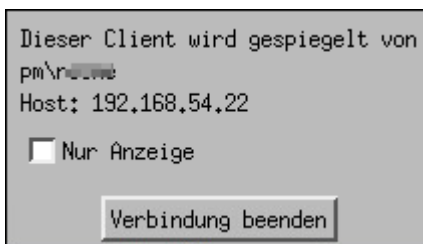
Hinweis

- 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....**
2. Bestätigen Sie den **Spiegeln**-Dialog mit **OK**.
3. Wenn in **Geräte-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. Die Systemmeldung kann verschoben, aber nicht geschlossen werden.



Der Benutzer hat folgende Optionen:

Option	Beschreibung
Nur Anzeige	Der Administrator darf nur lesend auf das gespiegelte Gerät zugreifen. Maus- und Tastatureingaben des Administrators werden nicht in die gespiegelte Sitzung übertragen.
Verbindung beenden	Die Verbindung wird getrennt und die Spiegelung ist beendet.
Beenden und Abmelden (nur wenn konfiguriert)	Die Verbindung wird getrennt und der Benutzer wird abgemeldet. Diese Option ist nur aktiv, wenn in Geräte-Konfiguration > Sicherheit die Option Abmelden bei Verbindungsabbruch eingeschaltet ist.

Die Spiegelungssitzung wird beendet, wenn

- der Administrator das Sitzungsfenster schließt oder die Verbindung über die Schaltfläche der Systemmeldung beendet, oder
- der Benutzer die Verbindung über die Schaltfläche der Systemmeldung beendet.

Wenn in **Geräte-Konfiguration > Sicherheit** konfiguriert, wird die Spiegelungssitzung in der Datei `eluxd.log` protokolliert.¹

9.1.3. Problembehandlung Spiegeln

Fehler / Problem	Ursache	Lösung
Von einem Scout Enterprise-Server mit mehreren Netzwerkkarten schlägt die Verbindung für die Spiegelungssitzung fehl.	Die Spiegelungssitzung wird nicht über die richtige Netzwerkkarte aufgebaut.	Setzen Sie in der Registry den Schlüssel <code>BindIPAddress</code> auf die IP-Adresse der Netzwerkkarte, auf die der Client zugreift: <code>HKEY_CURRENT_USER\Software\Unicon\Scout\Settings\BindIPAddress</code>

¹ab Scout Enterprise 15.4 mit MAC-Adresse

9.2. 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.

Je nach Benutzerrechten ist auch der umgekehrte Weg möglich: Der Benutzer sendet vom Client aus Diagnosedateien oder Screenshots.

Die Funktion **Diagnosedateien anfordern** kann auch eingesetzt werden, um frei zu definierende Dateien vom Client anzufordern.



Hinweis

Um die aktuelle Konfiguration eines Gerätes mit der in der Konsole definierten Geräte-Konfiguration auf Übereinstimmung zu überprüfen (Soll – Ist), verwenden Sie einen Geräte-Report. Für weitere Informationen siehe [Auswertung von Konfigurationsinformationen](#).¹

9.2.1. 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 Gerätes nicht unnötig zu strapazieren.

1. Öffnen Sie für das relevante Gerät das Kontextmenü und wählen Sie **Geräte-Konfiguration....**
Schalten Sie auf dem Register **Allgemein** die Option **Übergeordnete Geräte-Konfiguration verwenden** aus.
Setzen Sie auf dem Register **Diagnose** die Option **Protokollierungsstufe** auf **Ein**.
Bestätigen Sie und führen Sie einen Neustart des Clients durch.
Der Protokollierungs-Parameter am Gerät wird gesetzt.
2. Öffnen Sie das Kontextmenü des Gerätes und wählen Sie **Gerätediagnose > Dateien anfordern....**
*Im Dialog **Diagnosedateien bearbeiten** werden alle definierten Vorlagen angezeigt. Nur ausgewählte Vorlagen (mit Haken) werden berücksichtigt.*

¹Ab Scout Enterprise Management Suite Version 15.0 steht die Kontextmenü-Option **Konfiguration vergleichen (Soll – Ist)** nicht mehr zur Verfügung.

3. Wenn Sie über das notwendige Objektrecht verfügen, 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** `<userprofile>\Documents\UniCon\Scout\Console\Diag` gespeichert.*

5. Klicken Sie auf die Schaltfläche **Explorer**.

Der Datei-Explorer öffnet mit dem Diagnose-Zielverzeichnis.

6. Öffnen Sie in der Scout Enterprise-Konsole das Kontextmenü des Gerätes und wählen Sie **Geräte-Konfiguration...**

Setzen Sie im Register **Diagnose** die Option **Protokollierungsstufe** auf `Aus`.

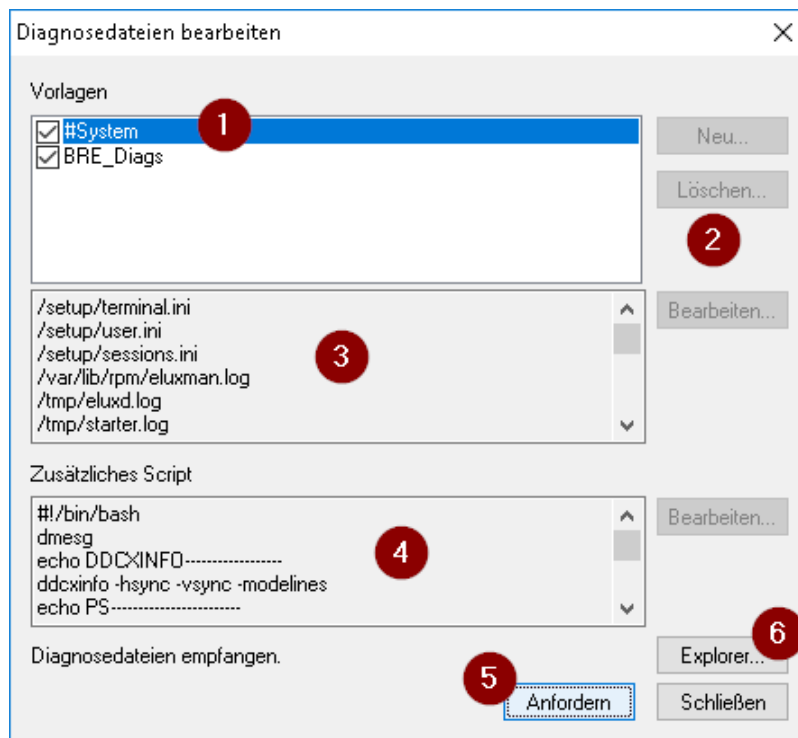
Schalten Sie auf dem Register **Allgemein** die Option **Übergeordnete Geräte-Konfiguration verwenden** ein.

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.



Legende

- 1 Vordefinierte Vorlage
#System

Diese Vorlage ist immer aktiv und kann weder gelöscht noch bearbeitet werden.
- 2 Mit dem Objektrecht **Diagnosevorlagen bearbeiten** kann der Administrator weitere Vorlagen erstellen, bearbeiten und löschen.
- 3 Protokoll- und Konfigurationsdateien, die durch die ausgewählte Vorlage definiert sind und vom Gerät angefordert werden
- 4 Zusätzliche Befehle, die durch die ausgewählte Vorlage definiert sind und auf dem Gerät ausgeführt werden
- 5 Die definierten Dateien werden vom Gerät angefordert und die definierten Befehle werden ausgeführt.
- 6 Sobald die angeforderten Dateien vorhanden sind, öffnen Sie den Explorer mit dem Diagnose-Zielverzeichnis.

9.2.2. 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 berechtigte Administratoren eigene Vorlagen definieren und bearbeiten, die sowohl Dateien als auch Script enthalten können. Die Vorlagen sind global verfügbar.

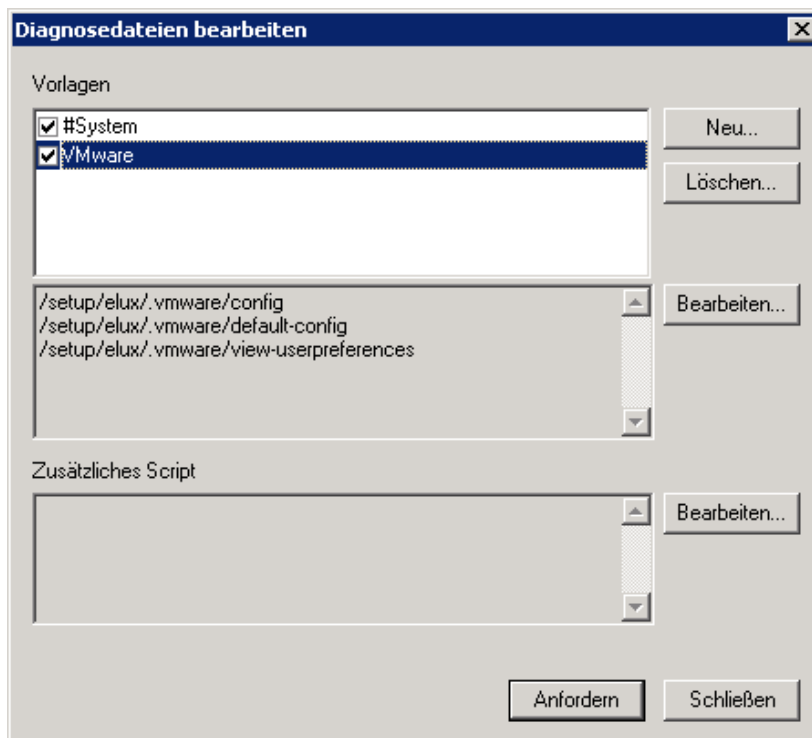
Vorlage für Gerätediagnose definieren



Voraussetzung

Objektrecht **Diagnosevorlagen bearbeiten** (standardmäßig nicht aktiv)¹

1. Öffnen Sie das Kontextmenü eines Gerätes und wählen Sie **Gerätediagnose > Dateien anfordern**.
*Im Dialog **Diagnosedateien bearbeiten** 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 Dateiliste.
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...**.
Geben Sie im Textfenster den auszuführenden Code ein und bestätigen Sie mit **Speichern**.

¹ab Scout Enterprise 15.8



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 [Geräte-Konfiguration > Register Diagnose](#).

10. 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 Imagedefinitions-Datei 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 Software-Pakete übertragen und automatisch installiert. Alternativ können die beiden Aktionen entkoppelt werden 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 eingeplant (einmalig oder periodisch) werden.
- Die Geräte können so konfiguriert werden, dass sie automatisch beim Ein- oder Ausschalten auf eine neue Image-Version prüfen und ggf. updaten.

Die Option **Auf neue Version prüfen** ist Teil der **Geräte-Konfiguration > Firmware** und kann auf einzelne Geräte, OUs und alle Geräte angewendet werden.

- Das Setzen einer **Update-Vormerkung** führt zum Ausführen eines Firmware-Updates beim nächsten Einschalten der Clients.

Wenn konfiguriert, kann der Benutzer die Durchführung des Updates verschieben.

Updates werden nur dann ausgeführt, wenn die relevante Imagedefinitions-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

Recovery-Installation

Wenn Sie Geräte komplett in den Auslieferungszustand zurücksetzen möchten, können Sie eine Recovery-Installation durchführen. Wenn kritische Feature-Pakete des BaseOS aktualisiert 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 Lizenzinformationen) und installiert die eLux-Software. Für weitere Informationen siehe [Recovery-Verfahren](#) in der **Recovery**-Kurzanleitung.

10.1. Voraussetzungen

Sie benötigen folgende Komponenten, um ein Firmware-Update durchzuführen:

- Webserver (zum Beispiel IIS), der die eLux Software-Pakete und Imagedefinitions-Dateien (`.idf`) via HTTP/HTTPS oder FTP/FTPS zur Verfügung stellt, mit aktivierter Webserver-Rolle
- Software-Container mit eLux-Software-Paketen auf dem Webserver
- Scout Enterprise ELIAS (eLux Image Administration Service) zur Erstellung und Änderung von Imagedefinitions-Dateien im Software-Container auf dem Webserver
- Scout Enterprise-Konsole zur Konfiguration des Firmware-Updates für die Clients

Scout Enterprise-Server, Scout Enterprise-Konsole und Scout Enterprise ELIAS sind Bestandteil der Scout Enterprise Management Suite.

Das aktuelle Software-Bundle `eLuxversion_AllPackages.zip` und optional weitere Software-Pakete werden im eLux-Container installiert.

Für weitere Informationen zur Installation der Scout Enterprise Management Suite und des eLux-Containers siehe die Kurzanleitung [Installation](#).

10.2. 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 Imagedefinitions-Datei führt zum Firmware-Update der mit diesem IDF konfigurierten Clients.

1. Wenn die relevante Software nicht im Container enthalten ist, laden Sie die Pakete von unserem Portal herunter und importieren sie in Scout Enterprise ELIAS in Ihren Container. Für weitere Informationen siehe [Pakete in einen Container importieren](#) im **ELIAS**-Handbuch oder [Software-Pakete importieren](#) im **ELIAS 18**-Handbuch.
2. In Scout Enterprise ELIAS fügen Sie Ihrer IDF-Datei die relevanten Software-Pakete hinzu und speichern die modifizierte IDF-Datei. Für weitere Informationen siehe [IDF erstellen](#) im **ELIAS**-Handbuch oder [Image erstellen](#) im **ELIAS 18**-Handbuch.
3. Öffnen Sie für die relevanten Geräte den Dialog **Geräte-Konfiguration**.
Wenn Sie das Update für alle Clients durchführen möchten, öffnen Sie den Dialog **Optionen > Basis-Geräte-Konfiguration**.
4. Überprüfen Sie im Register **Firmware** die korrekte Konfiguration für das Firmware-Update 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 Imagedefinitions-Datei und eLux-Software-Paketen relevant ist.*
Der angegebene Name für die Imagedefinitions-Datei muss mit dem Namen der in ELIAS aktualisierten Imagedefinitions-Datei übereinstimmen.
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 in diesem Fall vom Client initiiert wird, werden die lokal am Client gespeicherten Firmware-Parameter verwendet.
6. Bestätigen Sie mit **OK**.

Für weitere Informationen zur Konfiguration des Firmware-Updates siehe [Geräte-Konfiguration/Firmware](#).

Das Firmware-Update ist für die relevanten Clients konfiguriert.



Hinweis

Sobald eine aktualisierte Imagedefinitions-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](#).

10.3. 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. Um den Benutzer vor dem Update zu informieren, 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 **Benutzer kann Kommando abbrechen** 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 die System-Partition der Client-Flashspeicher vor dem Beschreiben zu formatieren, aktivieren Sie die Option **System-Partition 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. Während der Update-Vorgang läuft, wird der Status *Update läuft* angezeigt und durch zusätzliche Informationen über die aktuelle Phase mit Zeitstempel ergänzt.¹ Beispiel:*

Update läuft (Transfer gestartet – 2018-08-20 11:34:23)

Update läuft (Transfer beendet – 2018-08-20 11:35:45)

Update läuft (Installation gestartet – 2018-08-20 11:35:48)

Update läuft (Installation beendet – 2018-08-20 11:37:56)

Für weitere Informationen siehe [Kommando-Ergebnisse und Update-Informationen](#).

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.

¹ab Scout Enterprise 15.3



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.

10.4. Update über Vormerkung ausführen

Über eine Update-Vormerkung können Sie einmalig eine Update-Anforderung an bestimmte Clients senden. Bei der nächsten Verbindung zum Client wird die Anforderung ausgewertet und ein Update auf das in der Scout Enterprise-Konsole in der Firmware-Konfiguration konfigurierte Image ausgeführt.


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-Update veranlassen...**
*Der Dialog **Firmware-Update vormerken** wird angezeigt.*
3. Legen Sie fest, ob und wie lang der Benutzer informiert werden soll, und ob der Benutzer das Kommando abbrechen darf.
Für weitere Informationen siehe [Update über Kommando ausführen](#).
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 **Update-Vormerkung** der Status *Aktiviert* angezeigt.*



Hinweis

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

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-Anforderung¹ und die Update-Vormerkung wird automatisch gelöscht.

*Je nach Konfiguration in der Vormerkung und in **Geräte-Konfiguration > 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](#).*

¹Beachten Sie, dass ein Update nur dann ausgeführt wird, wenn die relevante Imagedefinitions-Datei verändert wurde.

Der Update-Status wird für jedes einzelne Gerät im **Eigenschaften**-Fenster angezeigt. Für weitere Informationen siehe [Update-Protokoll](#). Wenn ein Update nicht ausgeführt werden konnte, wird kein Versuch unternommen, den Vorgang zu wiederholen.

Bei Geräten ohne Update-Partition¹ 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 **Update-Vormerkung** auswerten.

Update-Vormerkung für ein oder mehrere Geräte löschen

Update-Vormerkungen können gelöscht werden, bevor das Firmware-Update eingespielt wurde:



Verwenden Sie die Kontextmenü-Option **Vormerkungen > Update-Vormerkung löschen**.



Hinweis

Vormerkungen werden immer für alle ausgewählten Geräte gesetzt oder gelöscht, unabhängig davon ob für einzelne Geräte bereits eine Vormerkung vorhanden war.

10.5. Update automatisch bei Systemstart oder Ausschalten

Der Client kann so konfiguriert werden, dass er automatisch beim Systemstart oder beim Herunterfahren prüft, ob ein Firmware-Update verfügbar ist und dieses einspielt.

Ablauf bei automatisch initiiertem Firmware-Update

- Der Client prüft je nach Konfiguration bei jedem Systemstart oder Herunterfahren, ob ein Firmware-Update notwendig ist.

Ein Update ist notwendig, wenn sich die in der Firmware-Konfiguration angegebene Image-definitions-Datei auf dem Web-Server im Vergleich zur lokalen Version geändert hat. Der Client ermittelt das Delta zwischen den Software-Paketen, die durch die Imagedefinitions-Datei (Image) am Web-Server definiert sind, und den installierten Software-Paketen. Wenn ein Delta vorliegt, ist ein Firmware-Update notwendig.
- Wenn ein Firmware-Update notwendig ist, lädt der Client alle im Image definierten Software-Pakete, die sich noch nicht auf seiner Update-Partition befinden, vom Webserver oder Proxy-Server herunter.
- Anschließend wird die Installation gestartet.

¹Flashspeicher unter 4 GB



Hinweis

Da das Update in diesem Fall vom Client initiiert wird, werden die lokal am Client gespeicherten Firmware-Parameter verwendet.

Ausnahme für VPN-Verbindungen

Wenn **Auf neue Version prüfen / Beim Start** konfiguriert ist und die VPN-Verbindung erst nach dem Laden des eLux-Desktops zustande kommt, werden unabhängig von der Notwendigkeit keine Updates installiert.¹ Der Benutzer kann ungestört weiterarbeiten.

Automatische Firmware-Updates beim Systemstart oder Herunterfahren konfigurieren

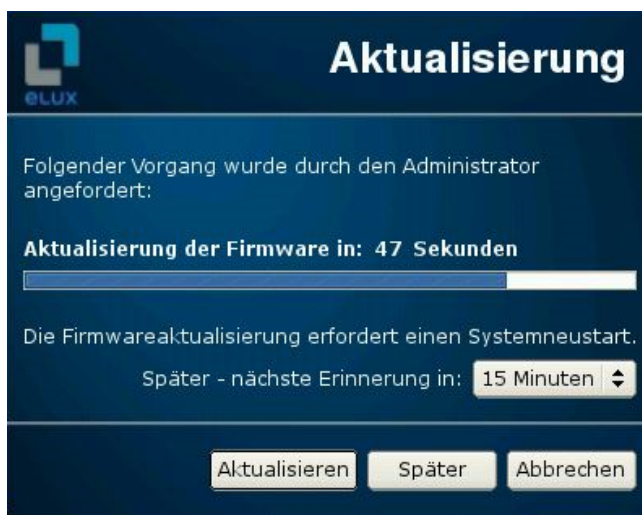
- ▶ Aktivieren Sie für die relevanten Clients in der Geräte-Konfiguration unter **Firmware** die Option **Auf neue Version prüfen**, entweder beim Systemstart oder beim Ausschalten.

Für weitere Informationen siehe [Geräte-Konfiguration/Firmware](#).

Nachdem die Clients die neue Geräte-Konfiguration erhalten haben, wird die Option zur Überprüfung auf neue Firmware-Versionen aktiv.

10.6. 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.



¹ab eLux RP 6.7

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

10.7. 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
Für weitere Informationen zur Update-Partition siehe [eLux-Partitionen](#).

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 **Kommando**-Dialog 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.

- Um zu überprüfen, welche Pakete tatsächlich übertragen worden sind, sehen Sie sich die Diagnosedatei `/var/lib/rpm/eluxman.log` an.

Der Auslieferungs-Status wird für jedes Gerät in der Scout Enterprise-Konsole im **Eigenschaften-**Fenster angezeigt. Während der Auslieferungs-Vorgang läuft, wird der Status `Auslieferung läuft` angezeigt und durch zusätzliche Informationen über die aktuelle Phase mit Zeitstempel ergänzt.¹ Beispiel:

Auslieferung läuft (Transfer gestartet – 2018-08-20 11:34:23)

Auslieferung läuft (Transfer läuft – 2018-08-20 11:35:45)

Auslieferung läuft (Transfer beendet – 2018-08-20 11:35:48)

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.

Bei einem **Update**-Kommando mit **System-Partition formatieren** müssen möglicherweise zusätzliche Pakete heruntergeladen werden, da ein **Delivery**-Befehl nur den Download von Paketen auslöst, die nicht auf der Systempartition installiert und nicht auf der Update-Partition verfügbar sind.

Auswirkungen am Gerät

Wenn der Administrator im **Kommando**-Dialog die Option **Benutzer darf Kommando abbrechen** aktiviert hat, kann der Benutzer die Auslieferung im Popup-Dialog über eine Schaltfläche abbrechen oder starten.

Während der Auslieferung wird am Gerät eine Live-Information auf der Systemleiste angezeigt.

¹ab Scout Enterprise 15.3

10.8. 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 Proxy-Server kommt die freie Software Squid zum Einsatz.



Voraussetzung

Der Proxy-Client muss über eine Hauptspeichergröße von mindestens 1 GB RAM verfügen, 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.



Hinweis

Squid unterstützt ab eLux RP 5.7 und eLux RP 6.2 das `HTTPS`-Protokoll. Um den Update-Prozess sicherer zu machen, können Sie außerdem Signaturen für IDF und Software-Pakete verwenden. 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 **Geräte-Konfiguration > Allgemein** und deaktivieren Sie die Option **Übergeordnete Geräte-Konfiguration verwenden**.

Die Vererbung wird unterbrochen und die Proxy-OU kann unabhängig konfiguriert werden.

3. Wählen Sie in **Geräte-Konfiguration > Firmware**, in der **Proxytyp**-Liste den Eintrag **Statisch (Provider)**.¹

Wenn Sie HTTP verwenden, lassen Sie die Felder **Benutzer** und **Kennwort** leer.

4. Wählen Sie für den Proxy-Client **Geräte-Konfiguration > Netzwerk > LAN** und bearbeiten Sie die LAN-Verbindung.

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 **Geräte-Konfiguration**.

Wenn Sie den Proxy für alle Clients definieren möchten, öffnen Sie den Dialog **Optionen > Basis-Geräte-Konfiguration**.

2. Bearbeiten Sie auf dem Register **Firmware** folgende Felder:

Protokoll	HTTP
Proxytyp ²	Statisch (Consumer)
Provider	<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.

¹ab Scout Enterprise 15.3

²ab Scout Enterprise 15.3

10.9. Dynamischer Proxy-Client

Auch dynamische Proxy-Clients können für die Software-Paket-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.

10.9.1. 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

Der Proxy-Client muss über eine Update-Partition verfügen. Für weitere Informationen zur Update-Partition siehe **eLux-Partitionen**.

10.9.2. Rahmenbedingungen und Rollen

Das Konzept des dynamischen Proxy-Clients basiert auf folgenden Rollen:

Provider



Voraussetzung

Ab Scout Enterprise Management Suite 15.3: Der Client muss in **Geräte-Konfiguration > Firmware > Proxytyp** auf **Dynamisch** konfiguriert sein.

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,

- ▶ wählen Sie ab Scout Enterprise Management Suite 15.3 in **Geräte-Konfiguration > Firmware > Proxytyp** den Eintrag **Keiner**.
- ▶ verwenden Sie bis Scout Enterprise Management Suite 15.2 die Funktion **Erweiterte Datei-**

einträge, um die `terminal.ini`-Datei der Clients zu bearbeiten:

Option	Wert
Datei	<code>/setup/terminal.ini</code>
Abschnitt	<code>DynamicProxy</code>
Eintrag	<code>UseProvider</code>
Wert	<code>false</code>

Für weitere Informationen siehe [Individuelle Dateieinträge festlegen](#).

Consumer



Voraussetzung

Ab Scout Enterprise Management Suite 15.3: Der Client muss in **Geräte-Konfiguration > Firmware > Proxytyp** auf `Dynamisch` konfiguriert sein.

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 Web-server downloaden.

Um bestimmte Geräte von der Consumer-Rolle auszuschließen,

- ▶ wählen Sie ab Scout Enterprise Management Suite 15.3 in **Geräte-Konfiguration > Firmware > Proxytyp** den Eintrag `Keiner`.
- ▶ verwenden Sie bis Scout Enterprise Management Suite 15.2 die Funktion **Erweiterte Dateieinträge**, um die `terminal.ini`-Datei der Clients zu bearbeiten:

Option	Wert
Datei	<code>/setup/terminal.ini</code>
Abschnitt	<code>DynamicProxy</code>
Eintrag	<code>UseConsumer</code>
Wert	<code>false</code>

Für weitere Informationen siehe [Individuelle Dateieinträge festlegen](#).



Hinweis

In der Firmware-Konfiguration dürfen die Felder **Benutzer** und **Kennwort** bei Verwendung von HTTP keinen Eintrag erhalten.

10.9.3. 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.

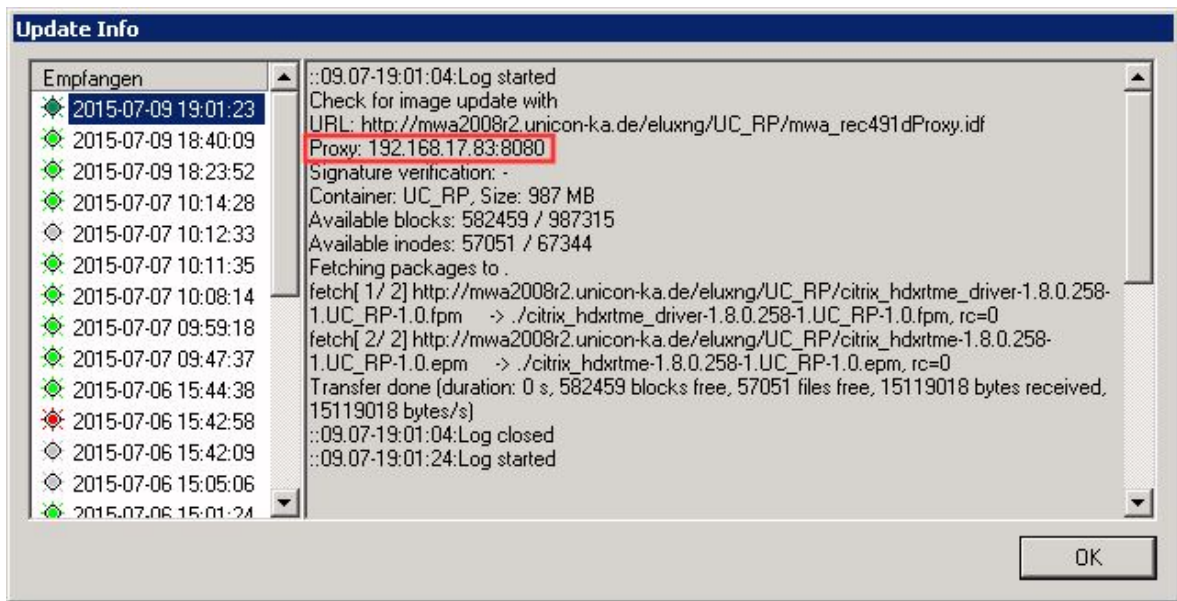
Software-Pakete verteilen und installieren

Die Software-Pakete werden vom Provider zu den Consumern übertragen und die Consumer installieren die Pakete. Dabei gehen Geräte ohne Update-Partition im Rhythmus '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.

10.10. Problembehandlung Firmware-Update

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 Geräte-Kennwort	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**.

11. Kennwörter

Die Eingabe von Kennwörtern kann unter eLux in verschiedenen Situationen für Benutzer oder Administratoren notwendig sein. Beispiele

- AD-Anmeldung zur Benutzer-Authentifizierung nach dem Systemstart
- Anmeldung an Anwendungen
- Geräte-Kennwort zum Entsperren der Geräte-Konfiguration
- Zugriff auf eine Kennwort-geschützte OU
- Definieren eines Spiegelungs-Kennwortes
- Einrichten von Netzwerk-Profilen
- Weitere Funktionen der Geräte-Konfiguration
Beispiel: Netzlaufwerk definieren

Auf Scout Enterprise-Seite wird das Geräte-Kennwort für alle Geräte einer Infrastruktur für weitere Funktionen eingesetzt.

Die Benutzer können unter eLux Kennwörter nach dem Eintippen zur Kontrolle anzeigen:¹

- ▶ Klicken Sie auf das Augen-Symbol neben dem Kennwort-Eingabefeld.

11.1. Lokales Geräte-Kennwort

Das Geräte-Kennwort betrifft die lokalen Geräte. Alle Thin Clients, die von einem Scout Enterprise Server verwaltet werden, erhalten dasselbe Geräte-Kennwort.

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 Geräte-Kennwort 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 Geräte-Konfigurationen durch die lokalen Benutzer zu verhindern.

Für weitere Informationen siehe [Geräte-Kennwort](#) im eLux-Handbuch.

¹ab eLux RP 6.7

11.1.1. 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 > Basis-Geräte-Konfiguration... > 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](#).

11.1.2. Lokales Geräte-Kennwort am Thin Client ändern

eLux RP 5

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**.

eLux RP 6

1. Wählen Sie im Configuration panel **Sicherheit > Geräte-Kennwort**.
2. Geben Sie zunächst das alte Kennwort ein und in die nächsten beiden Felder das neue Kennwort.
3. Bestätigen Sie mit **Anwenden**.



Achtung

Der Client kann ab sofort nicht mehr durch Scout Enterprise verwaltet werden.

11.2. 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 aktivieren und Ihre AD-Konten als Scout Enterprise-Konten anzupassen.

12. Administratorenverwaltung

12.1. 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 angemeldet 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. Danach werden alle Menüoptionen unter **Sicherheit** 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.*

12.2. 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 A- Benutzer zugeordnet sind.

12.3. 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.

12.4. Administratorenrechte

Für alle Scout Enterprise-Administratoren können Sie drei Arten von Zugriffsrechten setzen:

Basisrechte	Haupt-Zugriffsrechte eingeteilt in Funktionsblöcken
Menürechte	Zugriffsrechte auf einzelne Menüfunktionen
Objektrechte	Zugriffsrechte auf OU- oder Geräteebeane für Eigenschaften, Geräte-Konfiguration, Anwendungen und einige weitere Funktionen
Standard-Objektrechte	Standard-Zugriffsrechte für alle OUs oder Geräte, für die keine abweichenden Objektrechte definiert sind

Beachten Sie, dass Sie im Dialog immer erst den relevanten Administrator markieren, für den Sie die Zugriffsrechte bearbeiten möchten. Zur Bearbeitung von Objektrechten, wählen Sie außerdem zuerst die relevante OU oder das Gerät.

In allen **Administratorenrechte**-Dialogen werden für den markierten Administrator die vorhandenen Rechte mit grünem oder roten Symbol angezeigt:

Zugriff erlaubt

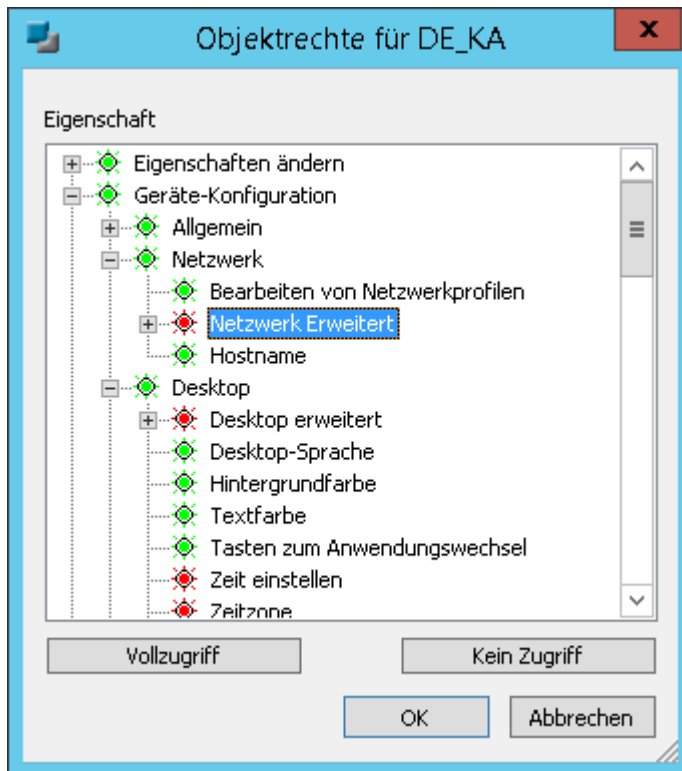


Zugriff verweigert



Um zwischen **Zugriff erlaubt** und **Zugriff verweigert** hin und her zu schalten, doppelklicken Sie auf das Recht oder drücken die Leertaste.

Wenn Sie auf die Schaltflächen **Vollzugriff** oder **Kein Zugriff** klicken, werden alle angezeigten Rechte auf grün bzw. auf rot gesetzt.



Achtung

Für alle Rechte gilt: Wird ein Recht deaktiviert (Zugriff verweigert), hat der Administrator keinen Zugriff mehr darauf. Für den letzten oder einzigen Administrator ist das Deaktivieren der Zugriffsrechte nicht möglich. Damit wird verhindert, dass Sie sich von der Konsole aussperren.

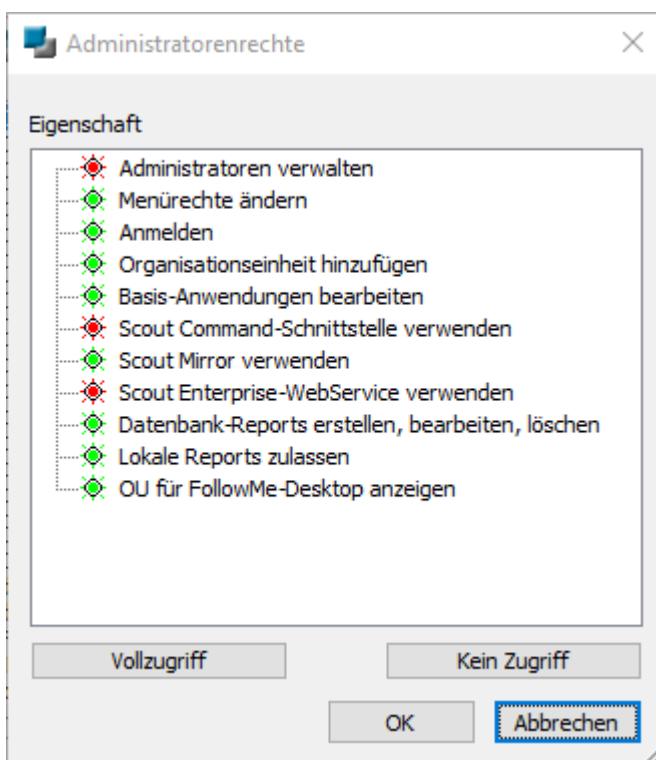
12.4.1. Basisrechte ändern

Administratoren-Basisrechte beziehen sich auf ganze Funktionsblöcke wie die Nutzung des Scout Enterprise-Reportgenerator oder die Konfiguration von FollowMe-Desktop.

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 Rechte durch Doppelklick.
5. Bestätigen Sie mit **OK**.



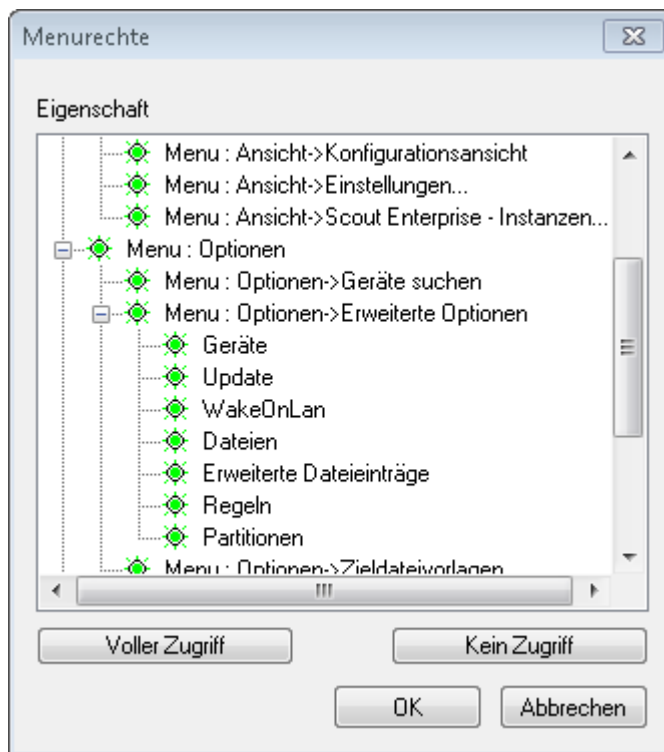
12.4.2. Menürechte ändern

Menürechte beziehen sich auf die Ausführbarkeit von Menüfunktionen. Wenn Sie einem Administrator keinen Zugriff auf eine Menüoption geben, wird der Menüeintrag abgeblendet und der Administrator kann die Funktion nicht ausführen.

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Menürechte....**
2. Markieren Sie einen Administrator .
3. Klicken Sie auf die Schaltfläche **Menürechte....**

*Der Dialog **Menürechte** öffnet.*

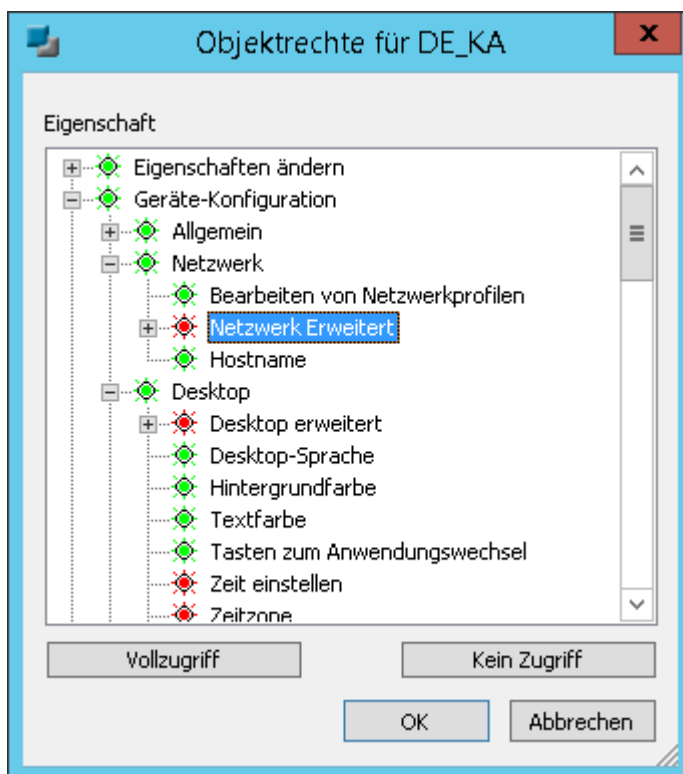
4. Ändern Sie die relevanten Rechte durch Doppelklick.
5. Bestätigen Sie mit **OK**.



12.4.3. Objektrechte ändern

Objektrechte beziehen sich auf eine OU oder ein Gerät. Für ausgewählte OUs oder Geräte können Sie Objektrechte definieren, die von den allgemeinen Standard-Objektrechten abweichen.

1. Markieren Sie in der Baumstruktur eine OU oder ein Gerät.
2. Wählen Sie **Sicherheit > Objektrechte....**
oder:
Wählen Sie den Kontextmenü-Eintrag **Objektrechte**
3. Markieren Sie einen Administrator.
4. Klicken Sie auf die Schaltfläche **Objektrechte bearbeiten...** .
*Der Dialog **Objektrechte für <OU>** öffnet.*
5. Ändern Sie die relevanten Rechte durch Doppelklick oder Leertaste.
6. Bestätigen Sie mit **OK**.



Objektrechte auf Standard zurücksetzen

Objektrechte, die Sie für eine OU oder ein Gerät abweichend definiert haben, können Sie zurücksetzen:

1. Markieren Sie im Dialog **Objektrechte** der OU oder des Gerätes den gewünschten Administrator.
2. Klicken Sie auf die Schaltfläche **Objektrechte löschen**.

12.4.4. Standard-Objektrechte ändern

Standard-Objektrechte gelten auf allen Ebenen. Sie sind gültig für alle OUs oder Geräte, für die keine abweichenden Objektrechte definiert sind.

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 Objektrechte durch Doppelklick.
5. Bestätigen Sie mit **OK**.

12.4.5. 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**.

12.5. Administrator-Aktivitäten anzeigen

Die Aktivitäten aller Administratoren werden je nach eingestellter Monitoring-Stufe in **Sicherheit > Administratoren verwalten** protokolliert. Die Protokollierung mit Monitoring-Stufe 3 ist am ausführlichsten.

Ab Scout Enterprise Management Suite 15.2 können Sie das Protokoll in der Scout Enterprise-Konsole anzeigen und exportieren.¹

1. Wählen Sie in der Scout Enterprise-Konsole **Sicherheit > Administratoren verwalten**.
2. Klicken Sie unter **Monitoring** auf die Schaltfläche **Protokoll anzeigen**.
*Der Dialog **Aktivitäten** öffnet und zeigt die Aktivitäten aller Administratoren je nach eingestellter Monitoring-Stufe.*
3. Um Protokolleinträge in eine Textdatei zu exportieren, markieren Sie die gewünschten Einträge und klicken auf **Markierte Einträge exportieren**.

¹Für ältere Versionen siehe die Scout Enterprise Datenbank-Tabelle `Monitor`

12.6. 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.

12.7. Wartungsfenster

– ab Scout Enterprise 15.7 –

Ein Wartungsfenster ist ein Termin oder Zeitraum, der für Wartungsarbeiten reserviert ist. In der Scout Enterprise-Konsole können berechtigte Administratoren Wartungsfenster definieren, um einen Zeitraum für notwendige IT-Wartungsaufgaben wie das Einspielen von Server-Updates frei zu halten. Während ein Wartungsfenster aktiv ist, können Administratoren ohne die relevante Berechtigung die Scout Enterprise-Konsole nicht verwenden und keine Jobs starten.

Wartungsfenster definieren



Voraussetzung

Menürecht: Menü: Ansicht > Systemdiagnose > Wartungsfenster

1. In der Scout Enterprise-Konsole wählen Sie den Menüeintrag **Ansicht > Systemdiagnose > Wartungsfenster...**
2. Klicken Sie auf **Hinzufügen**.
3. Im Dialog **Wartungsfenster bearbeiten** legen Sie folgende Optionen für Ihr neues Wartungsfenster fest:

Option	Beschreibung
Name	Mit aussagekräftigen Namen unterscheiden Sie mehrere Wartungsfenster.
Ab	Datum und Uhrzeit für den Beginn des ersten Wartungszeitraumes
für	Zeitdauer des Wartungsfensters Geben Sie Anzahl und Einheit (Stunden oder Minuten) an Beispiel: 2 Stunden
Wiederholen	Wiederholt das Wartungsfenster zyklisch, siehe Beispiel unten

4. Bestätigen Sie mit **OK**.

Das Wartungsfenster ist definiert und in der Liste der Wartungsfenster sichtbar.

Für die Dauer eines definierten Wartungsfensters wird für Administratoren, die nicht über das Menürecht `Wartungsfenster` verfügen, die Konsole gesperrt. Die betroffenen Administratoren können nur die Konsole schließen, andere Aktionen sind nicht möglich. Nach Ablauf des Wartungsfensters können sie die Konsole wieder wie gewohnt starten.



Hinweis

Standardmäßig ist das Menürecht `Wartungsfenster` aktiv und Wartungsfenster haben keine Auswirkungen. Sobald Sie das Menürecht für bestimmte Administratoren deaktivieren, können diese während der definierten Wartungsfenster nicht mit der Konsole arbeiten. Administratoren mit aktivem Menürecht `Wartungsfenster` erfahren keinerlei Einschränkungen.

Beispiel für ein zyklisches Wartungsfenster

Für ein Wartungsfenster, beispielsweise definiert von Freitag, 06.09.2019, 20:00 Uhr für 2 Stunden, können Sie folgende Wiederholungs-Optionen setzen:

Jeden Tag	Täglich, beginnend mit dem Startdatum
Jede Woche	Jeden Freitag einer Woche
Jeden Monat	Jeden 6. eines Monats
Jeden ersten Wochentag im Monat	Jeden Freitag der ersten Woche im Monat
Jeden zweiten Wochentag im Monat	Jeden Freitag der zweiten Woche im Monat
Jeden dritten Wochentag im Monat	Jeden Freitag der dritten Woche im Monat
Jeden vierten Wochentag im Monat	Jeden Freitag der vierten Woche im Monat
Jeden letzten Wochentag im Monat	Jeden Freitag der letzten Woche im Monat

13. Scout Enterprise-Statistikservice



Voraussetzung

- eLux RP 5.0 und neuere Versionen
- Scout Enterprise Management Suite 14.5.0 und neuere Versionen

Informationen zu älteren Versionen finden Sie im Archiv der Download-Seite [PDF-Downloads](#).

Der Scout Enterprise-Statistikservice bietet folgende Funktionen:

- 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.

- Verarbeitung dynamischer Geräteinformationen zur statistischen Auswertung

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.

Die Statistik-Daten werden in einer separaten SQL-Datenbank gespeichert.

Die Übermittlung der 'keep alive' messages' und der dynamischen Geräteinformationen erfolgt von den Geräten an den Scout Enterprise-Statistikservice über das HTTPS-Protokoll. Die Verbindung erfordert ein gültiges SSL-Zertifikat. Für weitere Informationen siehe [Zertifikat für Statistikservice](#).



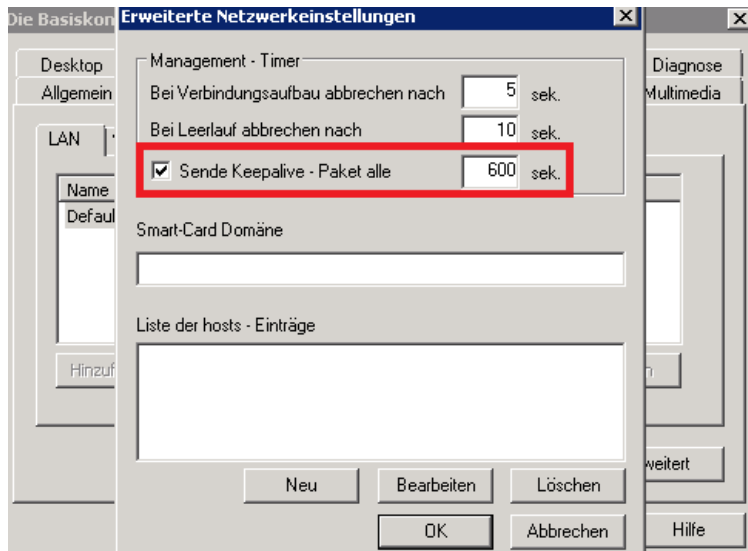
Hinweis

Der Scout Enterprise-Statistikservice ist Teil der Scout Enterprise Management Suite-Installation. Für weitere Informationen siehe [Scout Enterprise Management Suite installieren](#) in der Kurzanleitung **Installation**.

13.1. Definieren der Statusmeldungen (keep alive messages)

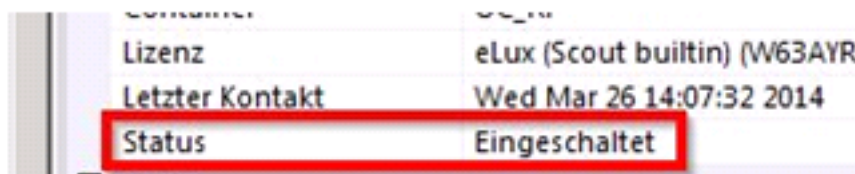
Mit Hilfe des Scout Enterprise-Statistikservice können Sie die automatische Aktualisierung der Statusmeldungen (keep alive messages) konfigurieren.

1. Wählen Sie im Scout Enterprise-Menü **Optionen > Basis-Geräte-Konfiguration > Netzwerk > Erweitert** oder öffnen Sie für das relevante Gerät oder OU den Dialog **Geräte-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:



13.2. 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](#).

13.3. 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.

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

Für weitere Informationen siehe [Scout Enterprise Management Suite installieren](#).

¹Bis Scout Enterprise Management Suite Version 14.9 wird das Dashboard separat installiert.

14. Konsolenkommunikation

Sobald mehrere Scout Enterprise-Konsolen und/oder Scout Enterprise-Dashboards verwendet werden, sind die Funktionen zur Konsolenverwaltung und -kommunikation von Bedeutung. Das web-basierte Scout Enterprise-Dashboard wird wie eine Konsole behandelt und kann beispielsweise wie eine Konsole Nachrichten empfangen.

14.1. Konsole schließen

1. Wählen Sie **Datei > Konsolenverwaltung > Konsole schließen**.
2. Klicken Sie auf **Aktualisieren**, um die aktuelle Liste mit Konsolen anzuzeigen.
3. Um die Liste der geöffneten Konsolen zu filtern, klicken Sie auf **Suchen**.
4. Um den Benutzer vor dem Schließen zu informieren, aktivieren Sie die Option **Benutzer informieren für x Sekunden** und geben Sie die Zeitspanne ein.
5. Um dem Benutzer die Möglichkeit zu geben, den Befehl abubrechen, aktivieren Sie die Option **Kommando kann vom Benutzer abgebrochen werden**.
6. Klicken Sie auf die Schaltfläche **Konsole(n) schließen**.

Das Kommando wird an die ausgewählten 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.

14.2. Nachricht senden

Mit dieser Funktion können Sie Nachrichten an andere Konsoleninstanzen senden. Jede Konsoleninstanz zeigt eine Nachricht nur einmal. Wurde die Konsoleninstanz während 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 dass der Benutzer einen Button auswählt, gilt die Nachricht als angenommen.
6. Wählen Sie **Senden**.
Die Nachricht wird an die ausgewählten Konsolen gesendet.

14.3. 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 durchnummeriert. 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.

14.4. 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.

14.5. 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 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.

15. Import/Export

Die Import- und Export-Funktionen können Sie entweder über die Scout Enterprise-Konsole oder über das SCMD-Interface durchführen.

Beim Export werden Dateien im XML-Dateiformat angelegt. Je nach exportiertem/importiertem Bereich ändert sich die Dateierweiterung.

Datenkategorie für den Export/Import	Dateierweiterung
Konfigurationen von OUs	.oustp
Basis-Geräte-Konfiguration	.oustp
Konfigurationen von Geräten	.devstp
Eigenschaften / Erweiterte Geräte-Konfiguration ¹ von OUs	.oupro
Basis/ Erweiterte Optionen	.oupro
Eigenschaften von Geräten	.devpro
Eigenschaften von Anwendungen	.appro
Geräteliste	.csv
OU-Baum	.outree

15.1. 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**.

15.2. Importieren

Sie können Geräte-Konfigurationen, 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**.

¹früher: Erweiterte Einstellungen

16. Protokollierung und Optimierung

16.1. 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	<code>scout.log</code>	Dient der Fehlersuche Pfad: <code>%USERPROFILE%\Documents\UniCon\Scout\Console</code> In der Scout Enterprise-Konsole öffnen Sie die Datei über Ansicht > Systemdiagnose > Konsolenprotokoll .
Scout Enterprise-Server	<code>eluxd.log</code>	Protokolldatei für den Scout Enterprise-Serverdienst, hilfreich bei Support-Anrufen Standard-Pfad: <code>%PUBLIC%\Documents\UniCon\Scout\Server</code> Ältere Versionen werden umbenannt in <code>elux.log.1...elux.log.3</code> 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	<code>keepAlive.log</code>	Protokolldatei für keep alive-Einträge des Scout Enterprise-Servers Einträge unter Einhaltung eines fest definierten Zeitstempels von 10 Minuten Standard-Pfad: <code>%PUBLIC%\Documents\UniCon\Scout\Server</code>

Für weitere Informationen zu den Dateipfaden siehe [Pfade](#).



Hinweis

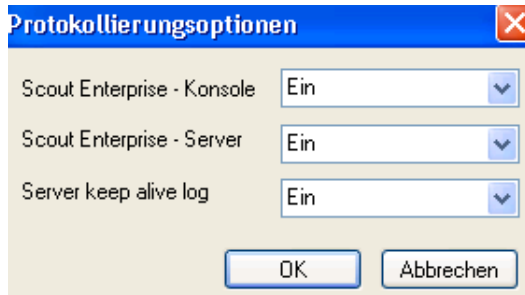
Verwenden Sie **Ansicht > Systemdiagnose > Server-Dateien**, um das `UniCon` Serverdateien-Verzeichnis im Windows-Explorer zu öffnen (wenn Konsole und Server auf der gleichen Maschine installiert sind). Das `UniCon`-Verzeichnis enthält alle Konfigurations- und Protokolldateien in entsprechenden Anwendungs-Unterverzeichnissen.

Folgende weitere Protokolle sind über die Scout Enterprise-Konsole verfügbar und können exportiert werden:

Protokoll	Beschreibung
Lizenzprotokoll	Alle Aktionen im Zusammenhang mit Lizenzen wie Eintragen, Löschen und Exportieren von Lizenzen Ansicht > Systemdiagnose > Lizenzprotokoll
Administrator-Aktivitäten	Alle Administrator-Aktivitäten in Abhängigkeit der eingestellten Monitoring-Stufe Sicherheit > Administratoren verwalten > Protokoll anzeigen Für weitere Informationen siehe Administrator-Aktivitäten anzeigen .

16.1.1. 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.

16.1.2. 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. Setzen Sie folgende Einträge:

Abschnitt	Eintrag	Default	Beschreibung
[ELUXD]	MaxLogFileSizeMB	100	Maximale Größe der Protokolldatei in MB
[ELUXD]	MaxLogFiles	10	Maximale Anzahl der Protokolldateien (<code>eluxd.log</code> 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. Setzen Sie folgenden Eintrag:

Abschnitt	Eintrag	Beispiel	Beschreibung
[ELUXD]	LogFileLocation	c:\log	Lokales Verzeichnis, in das die Protokolldateien <code>eluxd.log</code> und <code>keepAlive.log</code> geschrieben werden

Beim nächsten Starten des Scout Enterprise-Dienstes werden die Protokolldateien im angegebenen Verzeichnis geschrieben. Wenn der Scout Enterprise-Dienst nicht in das Verzeichnis schreiben kann, erzeugt er einen Eintrag in der Windows Ereignisanzeige.

16.2. 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

16.2.1. 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 Thin Client den Verbindungsversuch entsprechend seiner Handshake-Konfiguration, um die Geräte-Konfiguration 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.

Datei	Abschnitt	Eintrag	Wert
/setup/terminal.ini	ScoutHandshake	MaxRetries	8
/setup/terminal.ini	ScoutHandshake	RetryTimer	5
/setup/terminal.ini	ScoutHandshake	WaitUser	60
/setup/terminal.ini	ScoutHandshake	CanCancel	true

/setup/terminal.ini	ScoutHandshake	MaxRetries	8
---------------------	----------------	------------	---

Hinzufügen Ersetzen Löschen

Die Werte in der Abbildung sind Beispielwerte und können entsprechend angepasst werden. Standardmäßig sind keine Handshake-Parameter konfiguriert.

Der Abschnitt `ScoutHandshake` verfügt über folgende konfigurierbare Parameter:

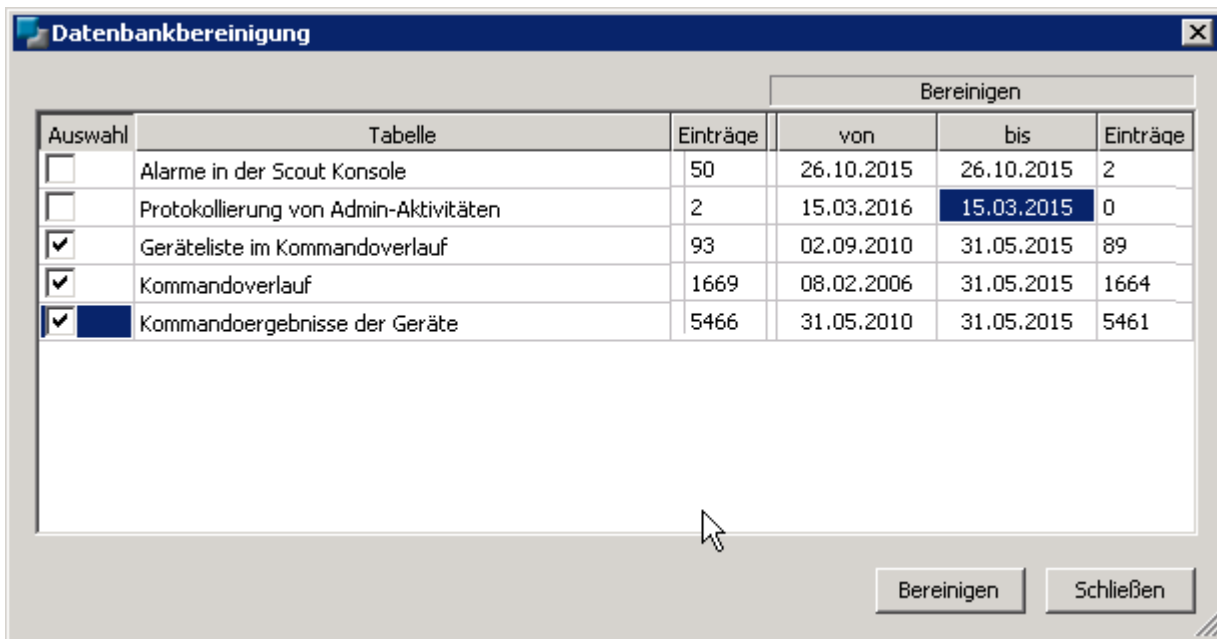
Parameter	Beschreibung
MaxRetries	Anzahl der Verbindungsversuche Der Wert 0 deaktiviert den Handshake.
RetryTimer	Zeit in Sekunden bis zum nächsten Verbindungsversuch Nach jedem Versuch wird die Zeit verdoppelt (+/- Zufallswert). Beispiel: Bei 8 Verbindungsversuchen mit RetryTimer -Startwert 5 Sekunden erfolgt der 8. Versuch nach ca. 22 Minuten.
PermanentRetriesAfterDays	Anzahl der Tage (maximal) ab der letzten erfolgreichen Verbindung bis zum nächsten Verbindungsversuch Stellt sicher, dass nach spätestens n Tagen die Konfigurationsdaten zwischen Gerät und Scout Enterprise-Server verglichen werden Kann mit MaxRetries und RetryTimer kombiniert werden
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 (<code>true</code> <code>false</code>).

16.2.2. 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 löschen¹.

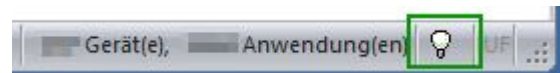
Der Dialog **Datenbankbereinigung** listet fünf verschiedene Tabellen jeweils mit der Gesamt-Anzahl der Einträge und dem Erstelldatum des ersten Eintrages. Der Administrator kann nur die Felder **Auswahl** und **bis** bearbeiten.

¹für LocalDB steht diese Funktion ab Scout Enterprise Management Suite Version 14.9 zur Verfügung



Alarme in der Scout Enterprise-Konsole

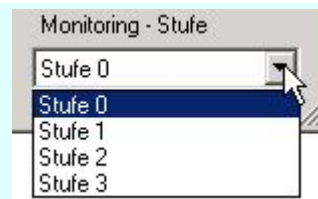
Alarmmeldungen (Fehler, Warnung, Info), die nach Doppelklick auf das Lampensymbol der Scout Enterprise-Konsole angezeigt werden



Protokollierung von Admin-Aktivitäten

Protokolleinträge der durchgeführten Administrator-Aktivitäten in Abhängigkeit der eingestellten Monitoring-Stufe in **Sicherheit > Administratorenverwaltung...**

Für weitere Informationen siehe [Administrator-Aktivitäten anzeigen](#).



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.

17. Anhang

18.1. Programm- und Datei-Verzeichnisse

Programmverzeichnis

Die Scout Enterprise Management Suite wird standardmäßig installiert nach

`%PROGRAMFILES%\Unicon\Scout`¹

Scout Enterprise-Dashboard wird auf dem Webserver (IIS) standardmäßig installiert nach

`<Root-Verzeichnis>\Scout\Dashboard`

Der Verzeichnisname `Dashboard` ist der Anwendungsname, der in der URL angezeigt wird, und kann während der Installation geändert werden.

Der eLux-Container wird auf dem Webserver installiert nach

`<Root-Verzeichnis>\eluxng`

Verzeichnis für Scout Enterprise-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 Hilfe der Scout Enterprise-Menüfunktion **Ansicht > Systemdiagnose > Serverdateien** (nur wenn Konsole und Server auf der gleichen Maschine installiert sind).

Verzeichnis für Benutzer-Dateien

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

`%USERPROFILE%\Documents\Unicon`

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

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

Diagnosedateien, die über Scout Enterprise-Dashboard angefordert werden, werden am Webserver gespeichert unter

`<Root-Verzeichnis>\Scout\Dashboard\Content\Diagnostic`

¹ab Scout Enterprise Management Suite Version 14.0



Hinweis

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

18.2. eLux-Partitionen

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

Alle Partitionen werden während einer Recovery-Installation erstellt.

Partition	Voraussetzungen	Zweck	Wird neu erstellt durch	Sonstiges
System		Reserviert für die Firmware (Software-Pakete)	Scout Enterprise Update -Kommando mit System-Partition vor Update formatieren	Größe 2 GB
Boot	nur UEFI und USB	Boot-Sektion	–	
Setup		Geräte-Konfiguration Lokale Anwendungsdefinitionen	Kommando Grundzustand	Hat keine Auswirkungen auf die System-Partition mit installierter Firmware
Update	4 GB Flash-Speicher	Software-Auslieferung (vor Firmware-Update) via Scout Enterprise-Kommando Signaturprüfung für eLux Software-Pakete Clients mit Update-Partition können als Dynamischer Proxy verwendet werden.	Scout Enterprise Auslieferung -Kommando mit Option Update-Partition vor Auslieferung bereinigen	Die Größe der Update-Partition richtet sich nach dem vorhandenen Speicherplatz. Auf Geräten mit weniger als 4 GB Flash-Speicher wird keine Update-Partition erstellt.

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

18.3. IP-Ports

eLux / notwendige Ports

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
	ICMP	ping muss zur Überprüfung des Gerätestatus der eLux-Geräte unterstützt werden		ein/aus
80	TCP	Firmware-Update via HTTP (und Proxy Port, falls genutzt)		ausgehend
443	TCP	Firmware-Update via HTTPS/TLS		ausgehend
5900	TCP	Spiegelung des eLux Desktop	Spiegelung deaktivieren (Konfig¹ > Sicherheit) oder VNC server-FPM im X.Org-Paket deinstallieren	eingehend
22123	TCP	Scout Enterprise-Server (Scout Enterprise Manager / secure)		ein/aus
22125	TCP	Scout Enterprise-Server (Scout Enterprise Manager / TLS 1.2) ²		ein/aus
22129	TCP	VPN		ausgehend

eLux / optionale Ports

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
	ESP	VPN (Datenphase)	VPN System-Paket deinstallieren	ein/aus
21	TCP	Update via FTP control port (dynamic data port)		ausgehend
22	TCP	SSH-Anwendungen		ausgehend
23	TCP	3270, 5250, 97801 Emulationen und Telnet-Sitzungen		ausgehend

¹Geräte-Konfiguration

²ab Scout Enterprise Management Suite Version 15.1 und eLux RP 6.1

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
53	TCP, UDP	DNS-Server		ausgehend
67	UDP	DHCP-Server	Lokale IP-Adresse konfigurieren (Konfig > Netzwerk)	ausgehend
68	UDP	DHCP Client (oder BootP Client)	Lokale IP-Adresse konfigurieren (Konfig > Netzwerk)	eingehend
69	UDP	TFTP-Server (wird nur während eines PXE-Recovery verwendet)		ausgehend
88	TCP, UDP	AD-Authentifizierung (Kerberos)		Outgoing
111	TCP, UDP	TCP Portmapper – RPC nur zur internen Verwendung Funktioniert mit lockd (random) UDP Portmapper – Treiberzugang auf NFS-Servern Funktioniert mit NFSD-Laufwerkszugriff (Port 2049) und mountd (random)	Network Drive Share-Paket deinstallieren	ein/aus
123	UDP	Windows-Zeitserver (NTP)	Keinen Zeitserver konfigurieren (Konfig > Desktop)	ein/aus
139	TCP, UDP	SMB Laufwerkszuordnung (NetBIOS) und SMB Benutzerauthentifizierung (CIFS)	Pakete Network Drive Share und User authentication modules deinstallieren	ausgehend
161	UDP	SNMP	SNMP Environment-Paket deinstallieren	ein/aus
162	UDP	SNMPTRAP	SNMP Environment-Paket deinstallieren	ausgehend
177	UDP	XCMCP-Protokoll		ausgehend
389	TCP	AD-Authentifizierung mit Benutzervariablen		ausgehend
443	TCP	VPN (Verbindungsaufbau) via HTTPS/TLS	VPN System-Paket deinstallieren	ein/aus

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
464	TCP, UDP	AD-Authentifizierung (Kerberos) / Kennwort setzen		Outgoing
514	TCP	Shell, X11-Anwendungen		ausgehend
515	TCP	Drucken über LPD	Print Environment (CUPS) -Paket deinstallieren	ein/aus
631	TCP, UDP	CUPS (IPP) Druck-Client	Print Environment (CUPS) -Paket deinstallieren	ausgehend
636	TCP	LDAPS-Authentifizierung mit Benutzervariablen		ausgehend
6000	TCP	Remote X11 Anwendungen	Option Konfig > Sicherheit > Remote X11 Clients zulassen deaktivieren	eingehend
7100	TCP	Fontserver Zuordnung in eLux Systemsteuerung möglich (Konfig > Bildschirm > Erweitert)		ausgehend
9100	TCP	Direktdruck auf parallelen Port Zuordnung in eLux Systemsteuerung (Konfig > Drucker)	Option Konfig > Drucker > TCP Direktdruck deaktivieren	eingehend
9101	TCP	Direktdruck auf USB Port Zuordnung in eLux Systemsteuerung (Konfig > Drucker)	Option Konfig > Drucker > TCP Direktdruck deaktivieren	eingehend
20000	UDP	Wake On LAN		ein/aus
22124	TCP	Scout Enterprise Statistics		ausgehend

Scout Enterprise-Server

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
	ICMP	ping muss zur Überprüfung des Gerätestatus der eLux-Geräte unterstützt werden		ein/aus
1433	TCP	MS SQL Server		ausgehend
1434	UDP	MS SQL Server (Browserdienst)		ein/aus

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
22123	TCP	Clients (Scout Enterprise Manager / secure)		ein/aus
22124	TCP	Scout Enterprise Statistics		eingehend
22125	TCP	Clients (Scout Enterprise Manager / TLS 1.2) ¹		ein/aus

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 VNC server-FPM im X.Org-Paket deinstallieren	ausgehend

Scout Enterprise-Dashboard

Das Scout Enterprise-Dashboard kann entweder mit HTTP oder HTTPS installiert werden.

Port	Typ	Beschreibung	Vorgehensweise zum Deaktivieren	Ein/Aus
80	TCP	Dashboard-Service / Webserver über HTTP		eingehend
443	TCP	Dashboard-Service / Webserver über HTTPS/TLS		eingehend
5901	TCP	Spiegelung des eLux Desktop	Spiegelung deaktivieren (Konfig > Sicherheit) oder VNC server-FPM im X.Org-Paket deinstallieren	ausgehend

¹ab Scout Enterprise Management Suite Version 15.1 und eLux RP 6.1

Scout Enterprise Cloud Gateway

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

18.4. SNMP

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

Für eLux RP 5 und eLux RP 6 wird SNMPv3 eingesetzt.



Hinweis

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

18.4.1. SNMP konfigurieren

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

Oder:

Konfigurieren Sie die Datei `terminal.ini` mit der Scout Enterprise-Funktion [Erweiterte Dateieinträge](#). Beispiel:

Datei	<code>/setup/terminal.ini</code>
Abschnitt	SNMPD
Eintrag	<code>rocommunity</code>
Wert	<code>secret</code>

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

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

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

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

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

Hinweise zur Konfiguration von SNMP v3

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



Hinweis

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

18.4.2. SNMPD und SNMP Konfigurations-Befehle

Die nachstehende Liste bezieht sich auf das Software-Paket **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
syservices	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
