



MarkVision Enterprise

Benutzerhandbuch

Hinweis zur Ausgabe

Januar 2012

Der folgende Abschnitt gilt nicht für Länder, in denen diese Bestimmungen mit dem dort geltenden Recht unvereinbar sind: LEXMARK INTERNATIONAL, INC., STELLT DIESE VERÖFFENTLICHUNG OHNE MANGELGEWÄHR ZUR VERFÜGUNG UND ÜBERNIMMT KEINERLEI GARANTIE, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, DER GESETZLICHEN GARANTIE FÜR MARKTGÄNGIGKEIT EINES PRODUKTS ODER SEINER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. In einigen Staaten ist der Ausschluss von ausdrücklichen oder stillschweigenden Garantien bei bestimmten Rechtsgeschäften nicht zulässig. Deshalb besitzt diese Aussage für Sie möglicherweise keine Gültigkeit.

Diese Publikation kann technische Ungenauigkeiten oder typografische Fehler enthalten. Die hierin enthaltenen Informationen werden regelmäßig geändert; diese Änderungen werden in höheren Versionen aufgenommen. Verbesserungen oder Änderungen an den beschriebenen Produkten oder Programmen können jederzeit vorgenommen werden.

Die in dieser Softwareokumentation enthaltenen Verweise auf Produkte, Programme und Dienstleistungen besagen nicht, dass der Hersteller beabsichtigt, diese in allen Ländern zugänglich zu machen, in denen diese Softwareokumentation angeboten wird. Kein Verweis auf ein Produkt, Programm oder einen Dienst besagt oder impliziert, dass nur dieses Produkt, Programm oder dieser Dienst verwendet werden darf. Sämtliche Produkte, Programme oder Dienste mit denselben Funktionen, die nicht gegen vorhandenen Beschränkungen bezüglich geistigen Eigentums verstoßen, können stattdessen verwendet werden. Bei Verwendung anderer Produkte, Programme und Dienstleistungen als den ausdrücklich vom Hersteller empfohlenen ist der Benutzer für die Beurteilung und Prüfung der Funktionsfähigkeit selbst zuständig.

Den technischen Support von Lexmark finden Sie unter **support.lexmark.com**.

Unter **www.lexmark.com** erhalten Sie Informationen zu Zubehör und Downloads.

Verfügen Sie über keinen Internetzugang, wenden Sie sich unter folgender Adresse schriftlich an Lexmark:

Lexmark International, Inc.
Bldg 004-2/CSC
740 New Circle Road NW
Lexington, KY 40550
USA

© 2012 Lexmark International, Inc.

Alle Rechte vorbehalten.

Marken

Lexmark, Lexmark mit der Raute und Markvision sind in den USA und/oder anderen Ländern eingetragene Marken von Lexmark International, Inc.

Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

Lizenzhinweise

Alle Lizenzhinweise in Verbindung mit diesem Produkt können im Root-Verzeichnis der Installationssoftware-CD eingesehen werden.

Inhalt

Hinweis zur Ausgabe.....	2
Übersicht.....	7
Was ist Markvision Enterprise?.....	7
Erste Schritte.....	8
Unterstützte Systeme und Software.....	8
Systemvoraussetzungen	8
Unterstützte Datenbankserver	8
Installieren von Markvision.....	8
Aktualisieren auf die neueste Version von Markvision.....	9
Sichern und Wiederherstellen der Firebird-Datenbank.....	9
Zugreifen auf Markvision.....	10
Migrieren aus MarkVision Professional in Markvision Enterprise.....	11
Verwenden von Markvision.....	12
Der Startbildschirm.....	14
Grundlagen zu Anschlüssen und Protokollen.....	15
Verwalten von Beständen.....	18
Suchen nach Geräten.....	18
Erstellen eines Suchprofils	18
Bearbeiten oder Löschen von Suchprofilen	20
Importieren von Geräten aus einer Datei	20
Verwalten von Geräten.....	21
Festlegen des Gerätelebenszyklusstatus	21
Prüfen von Geräten	22
Anzeigen von Geräteeigenschaften	23
Suchen und Organisieren von Geräten im System.....	24
Suchen nach Geräten im System.....	24
Arbeiten mit Lesezeichen.....	27
Erstellen von Lesezeichen	27
Zugriff auf Lesezeichen	27
Löschen von Lesezeichen.....	27
Verwenden von Kategorien und Schlüsselwörtern.....	27
Hinzufügen, Bearbeiten oder Löschen von Kategorien	28
Hinzufügen, Bearbeiten oder Löschen von Schlüsselwörtern	28

Zuordnen von Schlüsselwörtern zu Geräten.....	28
Entfernen zugewiesener Schlüsselwörter aus Geräten	29
Verwalten von Richtlinien.....	30
Erstellen einer Richtlinie.....	30
Erstellen neuer Richtlinien.....	30
Erstellen von Geräte Richtlinien.....	31
Grundlagen zur Sicherheitsrichtlinie.....	32
Grundlagen zu gesicherten Geräten	32
Grundlagen zu Einstellungen für Sicherheitsrichtlinien.....	34
Erstellen einer Sicherheitsrichtlinie	35
Ändern der Kommunikations-Anmeldeinformationen eines eingeschränkten Geräts	40
Bearbeiten oder Löschen von Richtlinien.....	41
Richtlinien zuweisen.....	41
Überprüfen der Übereinstimmung mit Richtlinien.....	41
Durchsetzen von Richtlinien.....	42
Entfernen von Richtlinien.....	42
Verwalten des Service Desks.....	43
Arbeiten mit Richtlinien.....	43
Überprüfen der Übereinstimmung des Geräts mit Richtlinien.....	43
Durchsetzen von Richtlinien	43
Arbeiten mit einem Gerät.....	43
Überprüfen des Gerätestatus	43
Anzeigen von Geräten von einem entfernten Standort aus	44
Anzeigen der eingebetteten Webseite	44
Verwalten von Geräteereignissen.....	45
Erstellen eines Ziels.....	45
Bearbeiten oder Löschen eines Ziels.....	45
Erstellen von Ereignissen.....	46
Bearbeiten oder Löschen von Ereignissen.....	46
Zuordnen von Ereignissen zu einem Gerät.....	47
Entfernen von Ereignissen aus Geräten.....	47
Anzeigen von Ereignisdetails.....	47
Ausführen weiterer Verwaltungsaufgaben.....	48
Herunterladen generischer Dateien.....	48
Konfigurieren der E-Mail-Einstellungen.....	48
Konfigurieren von Systemeinstellungen.....	49

Hinzufügen, Bearbeiten oder Löschen von Benutzern im System.....	49
Aktivieren der LDAP-Serverauthentifizierung.....	50
Generieren von Berichten.....	55
Planen von Tasks.....	56
Anzeigen des Systemprotokolls.....	57
Häufig gestellte Fragen.....	58
Fehlerbehebung.....	59
Benutzer hat das Passwort vergessen.....	59
Die Anwendung kann das Netzwerkgerät nicht finden.....	59
Alle Druckerverbindungen überprüfen.....	59
Sicherstellen, dass der interne Druckserver richtig installiert und aktiviert ist	59
Vergewissern Sie sich, dass der Gerätenamen in der Anwendung mit dem im Druckserver eingestellten Namen übereinstimmt.	60
Stellen Sie sicher, dass der Druckserver im Netzwerk kommuniziert.....	60
Geräteinformationen sind falsch.....	60
Anhang.....	61
Glossar der Sicherheitsbegriffe.....	62
Index.....	63

Übersicht

Was ist Markvision Enterprise?

Markvision™ Enterprise (MVE) ist ein webfähiges Dienstprogramm zur Geräteverwaltung für IT-Mitarbeiter. MVE dient als Client-Server-Anwendung. Der Server erkennt Geräte im Netzwerk, kommuniziert mit ihnen und liefert dem Client Informationen zu diesen Geräten. Der Client zeigt Informationen zu den Geräten an und stellt eine Benutzeroberfläche zur Verwaltung dieser Geräte bereit. Jeder Markvision-Server kann Tausende von Geräten verwalten.

Integrierte Sicherheitsvorrichtungen verhindern unberechtigten Zugriff auf die Anwendung, und nur autorisierte Benutzer können mithilfe des Clients auf die Verwaltungsoptionen zugreifen.

Mit Markvision können Sie Ihren gesamten aus Druckern und Druckservern bestehenden Druckerpool überwachen und verwalten. In der *Information Technology Infrastructure Library* (ITIL) werden Drucker und Druckserver auch als *Konfigurationselemente* (Configuration Items, CIs) bezeichnet. In diesem Dokument werden CIs, Drucker oder Druckserver meistens als Geräte bezeichnet.

Erste Schritte

Unterstützte Systeme und Software

Eine vollständige Liste der unterstützten Betriebssysteme und Webbrowser finden Sie in den *Versionshinweisen*.

Systemvoraussetzungen

RAM

- Erforderlich: 1 GB
- Empfohlen: 2 GB+

Prozessorgeschwindigkeit

- Erforderlich: 1 physisch 2 GHz oder höher (Hyper-Threaded/Dual Core)
- Empfohlen: 1+ physisch 3+ GHz (Hyper-Threaded/Dual Core+)

Festplattenspeicher des Computers

- Mindestens 60 GB Speicherplatz

Bildschirmauflösung

- Mindestens 1024 x 768 Pixel (nur bei MVE-Clients)

Unterstützte Datenbankserver

- Firebird
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Hinweise:

- Die Anwendung unterstützt ausschließlich die 32-Bit-Versionen und verfügt über eine vorkonfigurierte Firebird-Datenbank.
- Der Datenbankserver, auf dem MVE installiert ist, darf nur über eine *Netzwerkschnittstellenkarte* verfügen.

Installieren von Markvision

Mit Markvision können Sie Firebird oder Microsoft SQL Server als Backend-Datenbank verwenden.

Wenn Sie Microsoft SQL Server verwenden, gehen Sie vor der Installation von Markvision wie folgt vor:

- Aktivieren Sie die Authentifizierung des Mischmodus und die automatische Ausführung.
- Richten Sie die Netzwerkbibliotheken so ein, dass sie einen statischen Port und TCP/IP-Anschlüsse verwenden.
- Richten Sie ein Benutzerkonto ein, mit dem Markvision das Datenbankschema und eventuelle Datenbankverbindungen erstellt.

- Richten Sie die folgenden Datenbanken ein:
 - FRAMEWORK
 - MONITOR
 - QUARTZ

Hinweis: Stellen Sie sicher, dass Ihr eingerichtetes Konto entweder der Eigentümer dieser Datenbanken ist oder über die entsprechenden Berechtigungen verfügt, ein Schema zu erstellen und DML-Operationen (*Data Manipulation Language*) auszuführen.

- 1 Entpacken Sie die Installationsdateien in einen Pfad, der *keine* Leerzeichen enthält.
- 2 Starten Sie **setup.exe**, und befolgen Sie die Anweisungen auf dem Computerbildschirm.

Aktualisieren auf die neueste Version von Markvision

Die Aktualisierung auf die neue Version kann nur von der unmittelbaren Vorgängerversion ausgeführt werden.

- 1 Sichern Sie Ihre Datenbank.


Hinweise:

- Bei Verwendung einer Firebird-Datenbank finden Sie weitere Informationen unter "Sichern der Firebird-Datenbank" auf Seite 9.
 - Bei Verwendung von MS SQL Server wenden Sie sich an Ihren MS SQL-Administrator.
- 2 Dekomprimieren Sie die Installationsdateien in einen temporären Speicherort und achten Sie darauf, dass der Pfad *keine* Leerzeichen enthält.
 - 3 Starten Sie **setup.exe** und folgen Sie den Anweisungen auf dem Computerbildschirm.

Sichern und Wiederherstellen der Firebird-Datenbank

Sichern der Firebird-Datenbank

Hinweis: Bei Verwendung von MS SQL Server als Datenbank wenden Sie sich an Ihren MS SQL-Administrator.

- 1 Beenden Sie den Markvision Enterprise-Dienst.
 - a Klicken Sie auf  oder auf **Start > Einstellungen**.
 - b Wählen Sie **Systemsteuerung** und klicken Sie dann ggf. auf **System & Sicherheit**.
 - c Doppelklicken Sie auf **Verwaltung**.
 - d Doppelklicken Sie ggf. auf **Komponentendienste**.
 - e Doppelklicken Sie auf **Dienste**.
 - f Wählen Sie im Bereich "Dienste" **Markvision Enterprise** und klicken Sie dann auf **Beenden**.
- 2 Suchen Sie den Installationsordner von Markvision Enterprise und wechseln Sie dann zu "firebird\data".
Beispiel: `C:\Programme\Lexmark\Markvision Enterprise\firebird\data`

- 3 Kopieren Sie folgende Datenbanken in ein sicheres Repository.
 - FRAMEWORK.FDB
 - MONITOR.FDB
 - QUARTZ.FDB
- 4 Starten Sie den Markvision Enterprise-Dienst erneut.
 - a Wiederholen Sie die Schritte **1a** bis **1e**.
 - b Wählen Sie im Bereich "Dienste" **Markvision Enterprise** und klicken Sie dann auf **Neu starten**.

Wiederherstellen der Firebird-Datenbank

- 1 Vergewissern Sie sich, dass die Sicherung der Firebird-Datenbank abgeschlossen ist.
- 2 Beenden Sie den Markvision Enterprise-Dienst.

Weitere Informationen finden Sie in Schritt 1 unter "Sichern der Firebird-Datenbank" auf Seite 9.
- 3 Suchen Sie den Installationsordner von Markvision Enterprise und wechseln Sie dann zu "firebird\data".

Beispiel: **C:\Programme\Lexmark\Markvision Enterprise\firebird\data**
- 4 Ersetzen Sie die folgenden Datenbanken durch die nach Abschluss des Sicherungsprozesses gespeicherten Datenbanken.
 - FRAMEWORK.FDB
 - MONITOR.FDB
 - QUARTZ.FDB
- 5 Starten Sie den Markvision Enterprise-Dienst erneut.

Weitere Informationen finden Sie in Schritt 4 unter "Sichern der Firebird-Datenbank" auf Seite 9.

Zugreifen auf Markvision

- 1 Öffnen Sie einen Webbrowser und geben Sie dann im Feld "URL" **http://MVE_SERVER:9788/mve/** ein.

Hinweis: Ersetzen Sie **MVE_SERVER** durch den Hostnamen oder die IP-Adresse des Computers, auf dem Markvision gehostet wird.
- 2 Geben Sie im Feld "Benutzer" **admin** ein.
- 3 Geben Sie im Feld "Kennwort" **Administrator1** ein und klicken Sie dann auf **Anmelden**.

Hinweis: Um das Kennwort zu ändern, klicken Sie in der oberen rechten Ecke des Startbildschirms auf **Kennwort ändern**.

Wenn Markvision mehr als 30 Minuten nicht genutzt wurde, wird der Benutzer automatisch abgemeldet. Sie müssen sich erneut anmelden, um auf Markvision zuzugreifen.

Migrieren aus MarkVision Professional in Markvision Enterprise


Hinweis: Markvision Enterprise (MVE) unterstützt nur die Migration von Daten aus MarkVision Professional (MVP) v11.2.1.

Exportieren von Daten aus MVP

Mit der MVP-Server-Webseite

- 1 Öffnen Sie einen Web-Browser, und geben Sie in das Feld "URL" Folgendes ein: `http://MVP_SERVER:9180/~MvServer`.

Hinweis: Ersetzen Sie `MVP_SERVER` durch die IP-Adresse oder den Hostnamen des MVP-Servers.

- 2 Klicken Sie in der MarkVision-Server-Webseite auf **Data Dir**.
- 3 Geben Sie bei Aufforderung den Benutzernamen und das Passwort ein.
- 4 Klicken Sie auf der Seite "Datenverzeichnis herunterladen" auf , um die MVP-Daten als ZIP-Datei herunterzuladen.
- 5 Speichern Sie die ZIP-Datei.

Mit dem Dateisystem

- 1 Navigieren Sie in System das den MVP-Server ausführt, auf das Verzeichnis, in dem der MVP-Server installiert ist.
- 2 Komprimieren Sie den Datenordner in eine ZIP-Datei.

Importieren von Daten in MVE

- 1 Melden Sie sich bei Markvision Enterprise an.
- 2 Klicken Sie im Dialogfeld "Daten aus MarkVision Professional importieren" auf **Ja** und dann auf **Durchsuchen**.

Hinweise:

- Wenn Sie auf **Ja** klicken, wird das Dialogfeld bei der nächsten Anmeldung in MVE nicht angezeigt.
- Wenn Sie auf **Nein** klicken und das Dialogfeld nicht mehr angezeigt werden soll, wählen Sie **Diese Meldung nicht mehr anzeigen** aus.

- 3 Navigieren Sie zu der Position, an der Ihre ZIP-Datei gespeichert wurde, und klicken Sie dann auf **Öffnen**.
- 4 Wählen Sie im Bereich "Zu importierende Daten" den zu importierenden Datentyp.

Daten	Einzelheiten
Anwender	<ul style="list-style-type: none"> • In MarkVision Professional erhalten Benutzer für bestimmte Funktionen Rechte. • In Markvision Enterprise werden Benutzern Rollen mit verschiedenen Funktionen zugewiesen. • Alle aus MVP importierten Benutzer werden automatisch allen Rollen zugewiesen, außer ROLE_ADMIN. • Wenn das Passwort eines MVP-Benutzers nicht den MVE-Passwortkriterien entspricht, wird die Zeichenfolge Administrator1 an das aktuelle Benutzerpasswort angehängt.

Daten	Einzelheiten
Geräte	<ul style="list-style-type: none"> • MVE importiert nur allgemeine Geräteinformationen aus MVP, einschließlich Modellname, Seriennummer, MAC-Adresse und IP-Adresse. • Wenn bereits ein Drucker in MVE vorhanden ist, wird dieser Drucker während des Imports ignoriert. • Während des Imports verwirft MVE Drucker, die mit den externen Netzwerkadaptern (ENAs) verbunden sind, da MVE derzeit ENAs nicht unterstützt. • Die importierten Geräte werden automatisch auf den Lebenszyklus-Status Verwaltet (normal) gesetzt. • MVP verwaltet Drucker und Druckserver. MVE verwaltet nur Drucker. Daher werden zwei Einträge in MVP zu einem einzelnen Eintrag in MVE.
Suchprofile	<ul style="list-style-type: none"> • Beim Import von MVP-Profilen in das MVE-System werden nur die folgenden Details importiert: <ul style="list-style-type: none"> – SNMP-Gemeinschaftsname – Erneute Versuche – Zeitübers. – Adresse ausschließen – Adresse einschließen • In MVP enthält jeder Eintrag zu "Einschließen/Ausschließen" das Set "Gemeinschaftsnamen Lesen/Schreiben". Ein Profil mit mehreren Einträgen zu "Einschließen/Ausschließen" kann auch mehrere eindeutige Sets "Gemeinschaftsnamen Lesen/Schreiben" enthalten. In MVE gehört das Set "Gemeinschaftsnamen Lesen/Schreiben" zum Profil selbst. Jedes Profil kann nur ein Set "Gemeinschaftsnamen Lesen/Schreiben" enthalten. Daher wird ein Suchprofil in MVP (enthält mehrere eindeutige Sets "Gemeinschaftsnamen Lesen/Schreiben") beim Import in MVE in mehrere Suchprofile aufgeteilt (jedes einzelne enthält ein Set "Gemeinschaftsnamen Lesen/Schreiben"). Die Anzahl der Profile in MVE entspricht der Anzahl der eindeutigen Sets "Gemeinschaftsnamen Lesen/Schreiben" im ursprünglichen MVP-Profil. • Bei "Zeitübers." wandelt MVE die MVP-Zeitüberschreitung in Millisekunden um, indem der MVP-Wert (in Sekunden) mit 1000 multipliziert wird. • Die Option "Automatisch verwalten" wird während des Imports auf Falsch gesetzt.

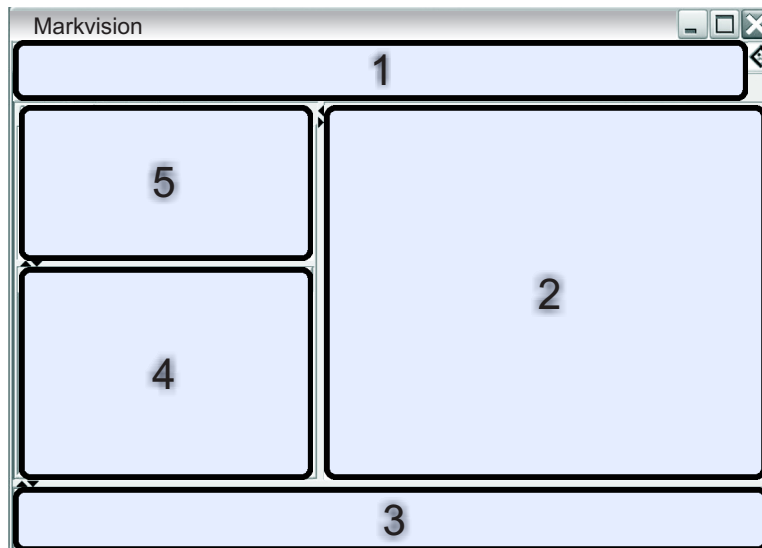
5 Klicken Sie auf **Importieren**.

Verwenden von Markvision

Die Eigenschaften und Funktionen von Markvision werden in vier Servicebereiche eingeteilt. Dadurch wird die Anwendung erleichtert, da die Schnittstelle nur mit den Eigenschaften und Funktionen bestückt ist, die für die aktuelle Task erforderlich sind. Auf jeden Servicebereich kann über eine Registerkarte auf dem Startbildschirm zugegriffen werden, und er entspricht jeweils einer Lebenszyklusstufe in der Information Technology Infrastructure Library (ITIL) Version 3. Die ITIL-Richtlinie genießt für die Sammlung von Best Practices für die Verwaltung von IT-Ressourcen innerhalb einer Organisation weltweite Anerkennung.

Verwenden Sie diese Registerkarte	Um
Bestand	<p>Suchen, Identifizieren, Organisieren und Nachverfolgen der physischen Bestände (Drucker und Multifunktionsgeräte), die zum Druckerpool gehören. Hier können Sie Informationen über die Einsatzmöglichkeiten der Poolmodelle, zu den integrierten Optionen und zum Lebenszyklus erfassen und verwalten.</p> <p>In ITIL ist dies dem Bereich "Serviceübergang" zugeordnet.</p> <p>Wenn zu Ihrem Verantwortungsbereich die Verwaltung von IT-Beständen gehört, gehen Sie auf "Verwalten von Beständen" auf Seite 18.</p>
Richtlinien	<p>Definieren und verwalten der Softwarekonfiguration des Druckerpools. Hier können Sie eine definierte Richtlinie zuweisen, mit der die entsprechenden Konfigurationseinstellungen der einzelnen Modelle bestimmt werden. Sie können überwachen, ob der Druckerpool den Richtlinien entspricht, und diese Richtlinien bei Bedarf durchsetzen.</p> <p>In ITIL ist dies dem Bereich "Serviceübergang" zugeordnet.</p> <p>Wenn zu Ihrem Verantwortungsbereich die Verwaltung und Wartung von Verwaltungsprogrammen zur Konfiguration gehört, gehen Sie auf "Verwalten von Richtlinien" auf Seite 30.</p>
Service Desk	<p>Direkt mit einem einzelnen Gerät im Druckerpool kommunizieren. Hier können Sie das Gerät von einem entfernten Standort aus über den eingebetteten Web-Server verwalten, die Richtlinienübereinstimmung prüfen, Richtlinien durchsetzen und Konfigurationseinstellungen anpassen.</p> <p>In ITIL ist dies dem Bereich "Servicebetrieb" zugeordnet.</p> <p>Wenn zu Ihrem Verantwortungsbereich die Verwaltung oder Administration des IT-Support-Kundendienstes gehört, gehen Sie auf "Verwalten des Service Desks" auf Seite 43.</p>
Event Manager	<p>Erstellen Sie ein automatisches Ereignis, wenn ein Gerät eine Warnung an das Netzwerk sendet. Sie können eine E-Mail senden oder andere festgeschriebene Aktionen durchführen, um angegebene Mitarbeiter zu informieren.</p> <p>In ITIL ist dies dem Bereich "Servicebetrieb" zugeordnet.</p> <p>Wenn zu Ihrem Verantwortungsbereich die Verwaltung von Problemen oder die Handhabung von Vorfällen gehört, gehen Sie auf "Verwalten von Geräteereignissen" auf Seite 45.</p>

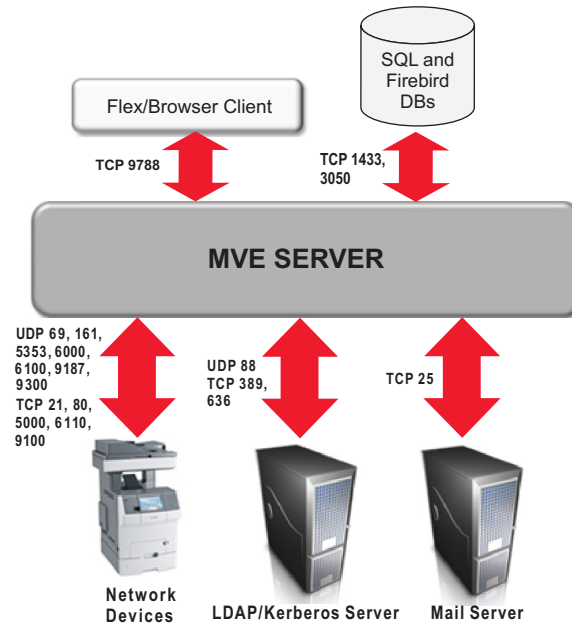
Der Startbildschirm



Verwenden Sie diesen Bereich		Um
1	Kopfzeile	Zugriff auf die vier Servicebereich-Registerkarten und Ausführen anderer administrativer Aufgaben.
2	Suchergebnisse:	Anzeige der vollständigen, seitennummerierten Liste mit Geräten, die der aktuell gewählten Lesezeichen-Suche entsprechen.
3	Task-Informationen	Anzeige des Status der letzten Aktivität.
4	Zusammenfassung Suchergebnisse	Anzeige einer kategorisierten Zusammenfassung der aktuell ausgewählten Lesezeichensuche.
5	Lesezeichen und erweiterte Suche	Verwaltung und Auswahl der Lesezeichen und Verfeinerung der Suchabfragen.

Grundlagen zu Anschlüssen und Protokollen

Wie in der folgenden Übersicht dargestellt, setzt Markvision unterschiedliche Anschlüsse und Protokolle für verschiedene Netzwerkkommunikationstypen ein.



Hinweis: Die Anschlüsse sind bidirektional und müssen geöffnet oder aktiv sein, damit Markvision ordnungsgemäß ausgeführt werden kann. Stellen Sie sicher, dass alle Geräteanschlüsse, je nach Gerät, entweder auf **Sicher/Nicht sicher** oder **Aktiviert** festgelegt wurden.

Kommunikation zwischen Server und Gerät

In der folgenden Tabelle sehen Sie die während der Kommunikation zwischen Markvision-Server und Netzwerkgeräten verwendeten Anschlüsse und Protokolle.

Protokoll	Markvision-Server	Gerät	Verwendungsbereich
NPAP <i>Network Printer Alliance Protocol (Protokoll im NPA-Format)</i>	Flüchtiger UDP-Anschluss (<i>User Datagram Protocol</i>)	UDP 9300	Kommunikation mit Lexmark Netzwerkdruckern
XMLNT <i>XML Network Transport (Objektspeicher)</i>	Flüchtige UDP- und TCP-Anschlüsse (<i>Transmission Control Protocol</i>)	UDP 6000 TCP 5000	Kommunikation mit Lexmark Netzwerkdruckern
LST <i>Lexmark Secure Transport</i>	UDP 6100 Flüchtiger TCP-Anschluss (Quittungsbetrieb)	UDP 6100 TCP 6110 (Quittungsbetrieb)	Verschlüsselte Kommunikation mit Lexmark Netzwerkdruckern
mDNS <i>Multicast Domain Name System</i>	Flüchtiger UDP-Anschluss	UDP 5353	Suche nach bestimmten Lexmark Netzwerkdruckern und Festlegen von Gerätesicherheitsfunktionen

Protokoll	Markvision-Server	Gerät	Verwendungsbereich
SNMP <i>Simple Network Management Protocol</i>	Flüchtiger UDP-Anschluss	UDP 161	Suche nach und Kommunikation mit Lexmark Netzwerkdruckern und Druckern von Drittanbietern
FTP <i>File Transfer Protocol</i>	Flüchtiger TCP-Anschluss	TCP 21	Downloads generischer Dateien
TFTP <i>Trivial File Transfer Protocol</i>	Flüchtiger UDP-Anschluss	UDP 69	Firmware-Aktualisierungen und Downloads generischer Dateien
HTTP <i>Hypertext Transfer Protocol</i>	Flüchtiger TCP-Anschluss	TCP 80	Downloads generischer Dateien
Raw Print-Anschluss	Flüchtiger TCP-Anschluss	TCP 9100	Downloads generischer Dateien

Kommunikation zwischen Gerät und Server

Dies sind der Anschluss und das Protokoll, die während der Kommunikation zwischen Netzwerkgeräten und Markvision-Server verwendet werden.

Protokoll	Gerät	Markvision-Server	Verwendungsbereich
NPAP	UDP 9300	UDP 9187	Generieren und empfangen von Warnungen

Kommunikation zwischen Server und Datenbank

Dies sind die während der Kommunikation zwischen Markvision-Server und Datenbanken verwendeten Anschlüsse.

Markvision-Server	Datenbank	Verwendungsbereich
Flüchtiger TCP-Anschluss	TCP 1433 (SQL Server) Dies ist der Standardanschluss, der vom Benutzer konfiguriert werden kann.	Kommunikation mit einer SQL Server-Datenbank
Flüchtiger TCP-Anschluss	TCP 3050	Kommunikation mit einer Firebird-Datenbank

Kommunikation zwischen Client und Server

Dies sind der Anschluss und das Protokoll, die während der Kommunikation zwischen Flex-/Browserclient und Markvision-Server verwendet werden.

Protokoll	Flex-/Browserclient	Markvision-Server
AMF <i>ActionScript Message Format</i>	TCP-Anschluss	TCP 9788

Meldungen und Warnungen

Dies sind der Anschluss und das Protokoll, die während der Kommunikation zwischen Markvision-Server und einem Mailserver verwendet werden.

Protokoll	Markvision-Server	SMTP-Server	Verwendungsbereich
SMTP <i>Simple Mail Transfer Protocol</i>	Flüchtiger TCP-Anschluss	TCP 25 Dies ist der Standardanschluss, der vom Benutzer konfiguriert werden kann.	Stellt die E-Mail-Funktionen für den Empfang von Gerätewarnungen bereit

Kommunikation zwischen Markvision-Server und LDAP-Server

Dies sind die während der Kommunikation verwendeten Anschlüsse und Protokolle, einschließlich Benutzergruppen und Authentifizierungsfunktionen.

Protokoll	Markvision-Server	LDAP-Server	Verwendungsbereich
LDAP <i>Lightweight Directory Access Protocol</i>	Flüchtiger TCP-Anschluss	TCP 389 oder der Anschluss, für den der LDAP-Server konfiguriert wurde	Authentifizierung von Benutzern von Markvision Enterprise mit einem LDAP-Server
LDAPS <i>Secure Lightweight Directory Access Protocol</i>	Flüchtiger TCP-Anschluss	<i>Transport Layer Security (TLS)</i> oder der Anschluss, für den der LDAP-Server konfiguriert wurde Für TLS-verschlüsselte Verbindungen.	Authentifizierung von Benutzern von Markvision Enterprise mit einem LDAP-Server über einen sicheren Kanal unter Verwendung von TLS
Kerberos	Flüchtiger UDP-Anschluss	UDP 88 Standardanschluss für den Kerberos-Authentifizierungsdienst.	Kerberos-Authentifizierung

Verwalten von Beständen

Suchen nach Geräten

Mit der Anwendung können Sie ein Netzwerk nach Geräten durchsuchen. Wenn Geräte gefunden werden, werden ihre Identifikationsinformationen im System gespeichert. Verwenden Sie Lesezeichen oder Suchläufe, um Geräte im Bereich "Suchergebnisse" anzuzeigen.

Gefundene Geräte werden standardmäßig auf **Neu** festgelegt und nicht vom System verwaltet. Bevor mit dem Gerät eine Aktion ausgeführt werden kann, müssen Sie es auf **Verwaltet** festlegen. Weitere Informationen finden Sie unter "Verwalten von Geräten" auf Seite 21.

Es gibt zwei Möglichkeiten, dem System Geräte hinzuzufügen:


- **Verwenden eines Suchprofils:** Sie können Geräte im Netzwerk mit benutzerdefinierten Parametern suchen.
- **Importieren von Geräten aus einer Datei:** Mithilfe einer Datei im CSV-Format (*durch Kommas getrennte Werte*) können Sie Geräte importieren.

Hinweis: Es kann jeweils nur eines der beiden Verfahren verwendet werden. Wenn Sie beide Verfahren zum Hinzufügen von Geräten zum System ausführen, sind die Geräte doppelt vorhanden.

Unmittelbar nachdem Sie dem System ein Gerät hinzugefügt haben, sollten Sie es prüfen. Durch die Prüfung werden zusätzliche Geräteinformationen bereitgestellt, die zum erfolgreichen Ausführen einiger Tasks erforderlich sind. Weitere Informationen zum Prüfen eines Geräts finden Sie unter "Prüfen von Geräten" auf Seite 22.

Hinweis: Hinweis: Dies gilt *ausschließlich* für uneingeschränkte Geräte. Eingeschränkten Geräten muss zuerst eine Sicherheitsrichtlinie zugewiesen und dann für diese Geräte durchgesetzt werden, bevor eine Prüfung ausgeführt werden kann. Andernfalls tritt ein Prüfungsfehler auf und der Zustand der eingeschränkten Geräte wird auf **(Verwaltet) fehlt** festgelegt. Weitere Informationen zu eingeschränkten Geräten finden Sie unter "Grundlagen zu gesicherten Geräten" auf Seite 32.

Erstellen eines Suchprofils

- 1 Klicken Sie bei Bedarf auf der Registerkarte "Bestand" auf **Suchprofil**, damit der Bereich "Suchprofile" angezeigt wird.
- 2 Klicken Sie auf **+** und geben Sie dann den Namen des neuen Suchprofils ein.
- 3 Wählen Sie auf der Registerkarte "Adressen" die Option **Einschließen** oder **Ausschließen**.
- 4 So importieren Sie eine Liste einzuschließender oder auszuschließender Elemente aus einer Datei:
 - a Klicken Sie auf .
 - b Navigieren Sie zu dem Ordner, in dem die Datei gespeichert ist.
 - c Wählen Sie die Datei aus und klicken Sie anschließend auf **Öffnen**.

Hinweis: In der Datei kann jedes beliebige Muster, das im Textfeld über "Adresse/Bereich" eingegeben werden kann, enthalten sein. Um Beispiele für gültige Muster anzuzeigen, bewegen Sie die Maus über das Textfeld.

- 5 Geben Sie neben **+** die IP-Adresse, den vollqualifizierten DNS-Hostnamen, Teilnetze mit Platzhalterzeichen oder gewünschte Adressbereiche ein und klicken Sie dann auf **+**.

Hinweise:

- Es kann jeweils nur ein Eintrag eingegeben werden. Um Beispiele für gültige Einträge anzuzeigen, bewegen Sie die Maus über das Textfeld oberhalb von "Adresse/Bereich".
- Verwenden Sie bei der Eingabe von Adressbereichen *keine* Platzhalterzeichen.
- Um einen Eintrag zu löschen, wählen Sie diesen aus und klicken dann auf **—**.

6 Klicken Sie auf die Registerkarte **SNMP**, und wählen Sie dann **Version 1, 2c** oder **Version 3** aus.

Hinweis: Wenn Sie die verwendete SNMP-Version nicht genau kennen, informieren Sie sich bei Ihrem Systemadministrator.

7 Wenn Sie unter Schritt 6 **Version 1, 2c** ausgewählt haben, richten Sie im Bereich "Gemeinschaftsnamen" das Verschlüsselungsprofil ein.

Wenn Sie **Version 3** ausgewählt haben, richten Sie im Bereich "Sicherheit" das Sicherheitsprofil ein.

Hinweis: Wenn Sie nicht genau wissen, wie das Sicherheitsprofil für die SNMP-Version 3 konfiguriert wird, informieren Sie sich bei Ihrem Systemadministrator.

8 Klicken Sie auf die Registerkarte **Allgemein** und verfahren Sie im Bereich "Leistung" wie folgt:

- Geben Sie im Feld "Zeitlimit" an, wie lange (in Millisekunden) auf eine Geräteantwort gewartet wird.
- Geben Sie im Feld "Wiederholungen" an, wie häufig das System bei einer fehlgeschlagenen Kommunikation versucht, erneut mit einem Gerät zu kommunizieren.

9 Wählen Sie aus, ob gesicherte Geräte in die Suche einbezogen werden sollen.

Hinweise:


- Wenn Sie über kein gesichertes Gerät verfügen, wählen Sie diese Option *nicht* aus. Andernfalls kommt es zu Leistungseinbußen und die Gerätesuche dauert wesentlich länger.
- Für gesicherte Geräte gilt mindestens eine der folgenden Bedingungen: (a) die Kommunikationsanschlüsse sind deaktiviert und (b) eine Authentifizierung ist erforderlich, um Informationen vom Gerät abzurufen.

10 Wählen Sie aus, ob die gefundenen Geräte vom Suchprofil automatisch verwaltet werden sollen.



Hinweis: Wenn Sie diese Option auswählen, wird für alle gefundenen Geräte automatisch der Lebenszyklusstatus **Verwaltet** festgelegt.

11 Klicken Sie auf **Speichern >Schließen**.

Hinweise:

- Wenn Sie auf  klicken, wird das Suchprofil ausgeführt und *nicht* gespeichert.
- Mit einem neuen Suchprofil werden nur die für die zuverlässige Erkennung eines Geräts erforderlichen Informationen erfasst. Um sämtliche Informationen eines Geräts zu erfassen, legen Sie den Gerätestatus auf **Verwaltet** fest und führen dann eine Geräteprüfung durch.
- Um sicherzustellen, dass die Geräteinformationen aktuell sind, kann eine regelmäßige Suche eingerichtet werden. Weitere Informationen finden Sie unter "Planen von Tasks" auf Seite 56.

Bearbeiten oder Löschen von Suchprofilen

- 1 Klicken Sie bei Bedarf auf der Registerkarte "Assets" auf **Suchprofil**, damit der Bereich "Suchprofile" angezeigt wird.
- 2 Wählen Sie ein Profil aus, und klicken Sie anschließend auf  , um das Suchprofil zu bearbeiten oder auf  , um es zu löschen.
- 3 Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Importieren von Geräten aus einer Datei

Verwenden sie eine CSV-Datei mit durch Kommas getrennten Werten, um Geräte zu importieren.

Hinweis: Zur Vorbereitung einer Bereitstellung ermöglicht Markvision das Hinzufügen von Geräten, bereits *bevor* diese im Netzwerk verfügbar sind.

- 1 Klicken Sie auf der Registerkarte "Bestand" auf **Importieren** und dann auf **Durchsuchen**.
- 2 Wechseln Sie zu dem Ordner, in dem die CSV-Datei gespeichert ist.
Hinweis: Stellen Sie sicher, dass jede Zeile der CSV-Datei ein einzelnes Gerät darstellt.
- 3 Wählen Sie die CSV-Datei aus und klicken Sie anschließend auf **Öffnen**.
- 4 Wählen Sie im Abschnitt "Mögliche Spalten" die Spalten aus, die den Werten in der CSV-Datei entsprechen.
- 5 Wenn Sie das SNMP V3-Protokoll für die Kommunikation mit dem Gerät verwenden, *müssen* die folgenden Spalten ausgewählt werden:
 - **SNMP V3 Lese/Schreib-Benutzer**
 - **SNMP V3 Lese/Schreib-Kennwort**
 - **SNMP V3 Mindest-Authentifizierungsstufe**
 - **SNMP V3 Authentifizierungs-Hash**
 - **SNMP V3 Datenschutz-Algorithmus**

Hinweis: Stellen Sie unter Verwendung der in Schritt 3 ausgewählten CSV-Datei sicher, dass für die folgenden Parameter einer der darunter angegebenen Werte festgelegt ist:

- Mindest-Authentifizierungsstufe
 - **NO_AUTHENTICATION_NO_PRIVACY**
 - **AUTHENTICATION_NO_PRIVACY**
 - **AUTHENTICATION_PRIVACY**
- Authentifizierungs-Hash
 - **MD5**
 - **SHA1**
- Datenschutz-Algorithmus
 - **DES**
 - **AES_128**

- AES_192
- AES_256

Hinweis: Die Werte in der CSV-Datei müssen genau den angegebenen Werten entsprechen. Andernfalls wird das Gerät von MVE nicht gefunden.

- 6 Klicken Sie auf **Hinzufügen**, um die ausgewählten Spalten in den Abschnitt "Spalten der CSV-Datei" zu verschieben.
 - Wenn eine Spalte in der CSV-Datei vom System ignoriert werden soll, wählen Sie **Ignorieren**. Wiederholen Sie diesen Schritt für jede Spalte in der CSV-Datei, die nicht im Abschnitt "Mögliche Spalten" aufgeführt ist.
 - Um die Reihenfolge der ausgewählten Spalten an die CSV-Datei anzupassen, wählen Sie eine Spalte im Abschnitt "Spalten der CSV-Datei" aus und verschieben Sie dann die Überschriften mit den Pfeilen nach oben oder unten.
- 7 Wählen Sie aus, ob die erste Zeile in der CSV-Datei eine Kopfzeile enthält.
- 8 Wählen Sie aus, ob die importierten Geräte automatisch auf den Lebenszyklusstatus **Verwaltet** festgelegt werden sollen.
- 9 Klicken Sie auf **OK**.

Verwalten von Geräten

Einem Gerät können drei verschiedene Lebenszyklus-Status zugewiesen werden:

- **Verwaltet:** Dazu gehören sämtliche Aktivitäten des Geräts, die im System ausgeführt werden können.
 - **Verwaltet (normal):** Das Gerät befindet sich in seinem Dauerzustand.
 - **Verwaltet (geändert):** Es gibt seit der letzten Prüfung Änderungen an der physischen Eigenschaft des Geräts. Wenn bei der nächsten Kommunikation des Systems mit dem Gerät keine weiteren Änderungen an den physischen Eigenschaften vorgenommen werden, wechselt das Gerät in den Status "Verwaltet (normal)" zurück.
 - **Verwaltet (fehlt):** Das System kann mit dem Gerät nicht erfolgreich kommunizieren. Wenn das Systems wieder erfolgreich mit dem Gerät kommunizieren kann und keine Änderungen an den physischen Eigenschaften vorliegen, wechselt das Gerät in den Status "Verwaltet (gefunden)".
 - **Verwaltet (gefunden):** Das Gerät hatte zunächst gefehlt, konnte aber im letzten Versuch erfolgreich die Kommunikation mit dem System aufnehmen. Wenn das Systems das nächste Mal erfolgreich mit dem Gerät kommunizieren kann und keine Änderungen an den physischen Eigenschaften vorliegen, wechselt das Gerät in den Status "Verwaltet (normal)" zurück.
- **Nicht verwaltet:** Dadurch wird das Gerät von sämtlichen im System ausgeführten Aktivitäten ausgeschlossen.
- **Stillgelegt:** Das Gerät befand sich früher im Status "Verwaltet", wurde nun aber aus dem Netzwerk entfernt. Das System behält die Geräteinformationen, geht aber nicht davon aus, das Gerät wieder im Netzwerk zu entdecken. Wenn das Gerät wieder im Netzwerk angezeigt wird, setzt das System seinen Status auf "Neu".

Festlegen des Gerätelebenszyklusstatus

Stellen Sie vor der Ausführung von Aktionen sicher, dass das Gerät auf **Verwaltet** gesetzt ist.

- 1 Wählen Sie auf der Registerkarte "Assets" im Dropdown-Menü "Lesezeichen und Suchläufe" **Neue Drucker** aus.
- 2 Wählen Sie das Kontrollkästchen neben der IP-Adresse des Geräts aus.

Hinweis: Sie können mehrere oder alle Geräte auswählen.
- 3 Wählen Sie aus dem Dropdown-Menü "Status setzen auf" **Verwaltet** aus, und klicken Sie dann auf **Ja**.

Prüfen von Geräten

Bei einer Prüfung werden Informationen jedes einzelnen verwalteten Geräts im Netzwerk erfasst und im System gespeichert. Führen Sie regelmäßige Prüfungen durch, um sicherzustellen, dass die Informationen im System aktuell sind.

- 1 Aktivieren Sie im Bereich "Suchergebnisse" das Kontrollkästchen neben der IP-Adresse eines Geräts.

Hinweise:

- Wenn Sie die IP-Adresse des Geräts nicht kennen, suchen Sie das Gerät in der Spalte "Systemname" oder der Spalte "Hostname".
- Um mehrere Geräte zu prüfen, aktivieren Sie die Kontrollkästchen neben den IP-Adressen der Geräte.
- Um alle Geräte zu prüfen, aktivieren Sie das Kontrollkästchen neben "IP-Adresse".

- 2 Klicken Sie auf **Prüfen**.

Der Status der Prüfung wird im Bereich "Taskinformationen" angezeigt.

- 3 Nach Abschluss der Prüfung klicken Sie im Kopfzeilenbereich auf .

Ergebnisse der letzten Prüfung werden im Dialogfeld "Protokoll" angezeigt.

Nachdem die Geräte geprüft wurden, kann das System durch folgende Instanzen aufgefordert werden, den Zustand eines Geräts auf **Verwaltet (geändert)** festzulegen:

- An folgenden Werten für Geräte-IDs bzw. Gerätefunktionen wurden u. U. Änderungen vorgenommen:
 - Kennzeichnung
 - Hostname
 - Kontaktname
 - Kontaktstandort
 - IP-Adresse
 - Speichergröße
 - Name der Kopieroption
 - Duplexeinheit
- Folgende Optionen für Gerätehardware wurden u. U. hinzugefügt bzw. entfernt:
 - Verbrauchsmaterial
 - Zuführungsoptionen
 - Ausgabeoptionen
 - Anschlüsse
- Folgende Gerätefunktionen oder -anwendungen wurden u. U. hinzugefügt bzw. entfernt:
 - Schriftarten
 - eSF-Anwendungen

Hinweis: Die Durchführung einer Prüfung kann zu einem festgelegten Zeitpunkt oder in regelmäßigen Abständen geplant werden. Weitere Informationen finden Sie unter "Planen von Tasks" auf Seite 56.

Anzeigen von Geräteeigenschaften

Um eine vollständige Liste mit Informationen zum Gerät anzuzeigen, stellen Sie sicher, dass bereits eine Geräteprüfung durchgeführt wurde.

- 1 Wählen Sie auf der Registerkarte "Bestand" im Dropdown-Menü "Lesezeichen und Suchläufe" **Verwaltete Drucker**.
- 2 Wählen Sie im Abschnitt "Alle Drucker" die IP-Adresse des Geräts.
Hinweis: Wenn Sie die IP-Adresse des Geräts nicht kennen, suchen Sie das Gerät in der Spalte "Systemname".
- 3 Dialogfeld mit Geräteeigenschaften:

Option	Informationen
Identifikation	Gerätenetzwerk-ID.
Datum	Liste mit den Geräteereignissen. Dazu gehören das Datum, zu dem das Gerät dem System hinzugefügt wurde, sowie das Suchdatum und letzte Prüfdatum.
Firmware	Firmware-Code-Ebenen für das Gerät.
Einsatzmöglichkeiten	Gerätefunktionen.
Anschlüsse	Am Gerät verfügbare Anschlüsse.
Verbrauchsmaterialien	Verbrauchsmaterialstatus und Details.
Schriftartkassetten	Installierte Schriftartkassetten.
Optionen	Angaben über die Geräteoptionen, beispielsweise zur Gerätefestplatte und dem verbleibenden freien Speicherplatz.
Einzugsoptionen	Einstellungen für verfügbare Papierfächer und andere Gerätezuführungen.
Ausgabeoptionen	Einstellungen für verfügbare Papierausgabefächer.
eSF-Anwendungen	Angaben über die auf dem Gerät installierten eSF-Anwendungen (<i>Embedded Solutions Framework</i>), beispielsweise Versionsnummer und Status.
Gerätestatistik	Spezifische Werte für die einzelnen Geräteeigenschaften.
Änderungsdetails	Angaben zu den am Gerät vorgenommenen Änderungen. Hinweis: Dies gilt <i>nur</i> für Geräte, für die der Zustand Verwaltet (geändert) festgelegt wurde.

Suchen und Organisieren von Geräten im System

Suchen nach Geräten im System

Verwenden von Standardlesezeichen

Lesezeichen kennzeichnen eine gespeicherte Suche nach einem Gerät. Bei der Auswahl eines Lesezeichens stimmen die angezeigten Geräte mit den Suchkriterien überein.

Die Standardlesezeichen basieren auf dem Status des Gerätelebenszyklus.

- 1 Wählen Sie im Dropdown-Menü "Lesezeichen und Suchläufe" ein Lesezeichen aus:

Option	Funktion
Verwaltete Drucker	Aktive Geräte im System suchen. Hinweis: Bei der Auswahl dieses Lesezeichens angezeigte Geräte können sich in einem der folgenden Status befinden: <ul style="list-style-type: none"> • Verwaltete (normal) • Verwaltete (geändert) • Verwaltete (fehlt) • Verwaltete (gefunden)
Verwaltete (normale) Drucker	Aktive Geräte im System mit Geräteeigenschaften suchen, die seit der letzten Überwachung nicht geändert wurden.
Verwaltete (geänderte) Drucker	Aktive Geräte im System mit Geräteeigenschaften suchen, die seit der letzten Überwachung geändert wurden.
Verwaltete (fehlende) Drucker	Geräte suchen, mit denen das System keine Kommunikation aufbauen konnte.
Verwaltete (gefundene) Drucker	Geräte suchen, die aus früheren Suchabfragen als fehlend aufgeführt wurden, jetzt aber gefunden wurden.
Neue Drucker	Geräte suchen, die dem System neu hinzugefügt wurden.
Nicht verwaltete Drucker	Geräte suchen, die für im System ausgeführte Aktivitäten als ausgeschlossen gekennzeichnet wurden.
Stillgelegte Drucker	Geräte suchen, die nicht mehr im System aktiv sind.

- 2 Wählen Sie aus dem Bereich "Zusammenfassung Suchergebnisse" ein Kriterium aus, mit dem Sie die in den Lesezeichen gespeicherten Ergebnisse schnell und einfach näher eingrenzen können.

Verwenden der erweiterten Suche

Mit der Funktion "Erweiterte Suche" können Sie schnell komplexe Suchaktionen ausführen, die auf einem oder mehreren Parametern basieren.

- 1 Wählen Sie im Dropdown-Menü "Lesezeichen und Suchläufe" **Erweiterte Suche**.
- 2 Wählen Sie, ob alle Kriterien erfüllt werden müssen oder ob mindestens eines erfüllt werden muss.

3 Um ein neues Suchkriterium hinzuzufügen, klicken Sie auf **+**.

Um Suchkriterien zu gruppieren, klicken Sie auf **[+]** und dann auf **+**, um einzelne Kriterien hinzuzufügen.

Hinweis: Wenn Sie die Suchkriterien gruppieren, behandelt das System alle definierten Kriterien, die gruppiert sind, als ein Kriterium.

4 Wählen Sie aus dem Dropdown-Menü "Parameter" einen Parameter aus:

Option	Funktion
Gerätenummer	Geräte suchen, die über eine zugewiesenes Gerätenummer verfügen.
Unterstützung des Farbdrucks	Geräte nach deren Farbdruckunterstützung suchen.
Verbindung mit Standort	Geräte suchen, die einem bestimmten Standort zugewiesen sind.
Kontaktname	Geräte suchen, die über einen bestimmten Kontaktnamen verfügen.
Unterstützung der Kopierfunktion	Geräte nach ihrer Unterstützung der Kopierfunktion suchen.
Unterstützung der Duplexfunktion	Geräte nach ihrer Unterstützung des beidseitigen Drucks suchen.
Unterstützung der ESF-Funktion	Geräte nach ihrer Fähigkeit suchen, eine eSF-Anwendung (Embedded Solutions Framework) zu verwalten.
eSF-Anwendung (Name)	Geräte nach dem jeweiligen Namen der aktuell installierten eSF-Anwendung suchen.
eSF-Anwendung (Status)	Geräte nach dem aktuellen Status der installierten eSF-Anwendung suchen.
eSF-Anwendung (Version)	Geräte nach der Version der installierten eSF-Anwendung suchen.
Firmware-Version	Geräte nach ihrer Firmware-Version suchen.
Firmware: AIO	Geräte nach dem AIO-Wert ihrer Firmware suchen.
Firmware: Basis	Geräte nach der Basisversion ihrer Firmware suchen.
Firmware: Modul	Geräte nach dem Modul ihrer Firmware suchen.
Firmware: Fax	Geräte nach dem Faxwert ihrer Firmware suchen.
Firmware: Schriftart	Geräte nach dem Schriftartwert ihrer Firmware suchen.
Firmware: Kernel	Geräte nach dem Kernelwert ihrer Firmware suchen.
Firmware: Ladeprogramm	Geräte nach dem Ladeprogrammwert ihrer Firmware suchen.
Firmware: Netzwerk	Geräte nach dem Netzwerkwert ihrer Firmware suchen.
Firmware: Netzwerktreiber	Geräte nach dem Netzwerktreiberwert ihrer Firmware suchen.
Firmware: Bedienfeld	Geräte nach der Bedienfeldversion ihrer Firmware suchen.
Firmware: Scanner	Geräte nach der Scannerversion ihrer Firmware suchen.
Hostname	Geräte nach ihren Hostnamen suchen.
IP-Adresse	Geräte nach ihren IP-Adressen suchen. Hinweis: Sie können in den letzten drei Oktetts der IP-Adresse ein Sternchen (*) als Platzhalterzeichen verwenden, um alle übereinstimmenden IP-Adressen zu suchen. Wenn in einem Oktett ein Sternchen verwendet wird, müssen die darauf folgenden Oktetts ebenfalls ein Sternchen enthalten. <ul style="list-style-type: none"> • Gültige Beispiele: 157.184.32.*, 157.184.*.* und 157.*.*.* • Ungültiges Beispiel: 157.184.*.10.
Schlüsselwort	Geräte nach ihren zugewiesenen Schlüsselwörtern suchen, falls vorhanden.

Option	Funktion
Insgesamt gedruckte Seiten	Geräte nach ihren Werten der insgesamt gedruckten Seiten suchen.
MAC-Adresse	Geräte nach ihren MAC-Adressen suchen.
Wartungszähler	Geräte nach dem Wert des Wartungszählers suchen.
Hersteller	Geräte nach dem Herstellernamen suchen.
Unterstützung der MFP-Funktion	Geräte nach ihrer Unterstützung der Multifunktionsdruckfunktion (MFP) suchen.
Kennzeichnungstechnologie	Geräte nach dem Wert der unterstützten Kennzeichnungstechnologie suchen.
Modell	Geräte nach ihren Modellnamen suchen.
Druckerstatus	Geräte nach dem aktuellen Status suchen (beispielsweise Bereit , Papierstau , Fach 1 fehlt).
Unterstütztes Profil	Geräte nach dem unterstützten Profil suchen.
Unterstützung des Empfangs von Faxnachrichten	Geräte nach der Fähigkeit suchen, eingehende Faxe zu empfangen.
Unterstützung von "Scannen an E-Mail"	Geräten nach ihrer Unterstützung von "Scannen an E-Mail" suchen.
Unterstützung von "Scannen an Fax"	Geräte nach ihrer Unterstützung von "Scannen an Fax" suchen.
Unterstützung von "Scannen an Netzwerk"	Geräten nach ihrer Unterstützung von "Scannen an Netzwerk" suchen.
Seriennummer	Geräte nach ihrer Seriennummer suchen.
Status	Geräte nach ihrem aktuellen Status in der Datenbank suchen.
Verbrauchsmaterialstatus	Geräte nach dem aktuellen Verbrauchsmaterialstatus suchen.
Systemname	Geräte nach ihren Systemnamen suchen.

5 Wählen Sie im Dropdown-Menü "Vorgang" einen Operator aus:

Option	Funktion
Enthält	Geräte mit einem Parameter suchen, der einen bestimmten Wert enthält.
Enthält nicht	Geräte mit einem Parameter suchen, der einen bestimmten Wert nicht enthält.
Entspricht nicht	Geräte mit einem Parameter suchen, der einem exakten Wert nicht entspricht.
Endet mit	Geräte mit einem Parameter suchen, der mit einem bestimmten Wert endet.
Gleich	Geräte mit einem Parameter suchen, der einem bestimmten Wert entspricht.
Beginnt mit	Geräte mit einem Parameter suchen, der mit einem bestimmten Wert beginnt.

6 Geben Sie im Feld "Wert" oder im Dropdown-Menü den Wert des Parameters ein.

Hinweis: Wenn Sie das Kriterium löschen möchten, klicken Sie auf **X**.

7 Klicken Sie auf **OK**, um mit der Suche zu beginnen.

Die gefundenen Geräte werden im Bereich "Suchergebnisse" angezeigt.


8 Wählen Sie aus dem Bereich "Zusammenfassung Suchergebnisse" ein Kriterium aus, mit dem Sie die in den Lesezeichen gespeicherten Ergebnisse schnell und einfach näher eingrenzen können.

Arbeiten mit Lesezeichen

Lesezeichen kennzeichnen eine gespeicherte Suche.

Wenn dem System ein Gerät hinzugefügt wird und dieses den für ein Lesezeichen angegebenen Kriterien entspricht, wird das Gerät immer dann in die Suchergebnisse aufgenommen, wenn das Lesezeichen ausgewählt wird.

Erstellen von Lesezeichen

- 1 Wählen Sie aus dem Dropdown-Menü "Lesezeichen und Suchläufe" das Lesezeichen, das die Gerätegruppe darstellt, in der Sie Ihre Suche starten möchten.
Um die Suche zu verfeinern, klicken Sie auf **Erweiterte Suche**.
- 2 Klicken Sie bei Bedarf unter "Zusammenfassung Suchergebnisse" auf die verfügbaren Unterkategorien, um die Suche weiter zu verfeinern.
- 3 Wenn ein gewünschtes Gerät oder eine gewünschte Gerätegruppe im Suchfenster angezeigt wird, klicken Sie auf .
- 4 Geben Sie einen Namen für das Lesezeichen ein, und klicken Sie auf **OK**.

Zugriff auf Lesezeichen

- 1 Wählen Sie aus dem Dropdown-Menü "Lesezeichen und Suchläufe" das Lesezeichen aus, das Sie anzeigen möchten.
- 2 Klicken Sie bei Bedarf unter "Zusammenfassung Suchergebnisse" auf die verfügbaren Unterkategorien, um die Suche weiter zu verfeinern.

Löschen von Lesezeichen

- 1 Wählen Sie aus dem Menü "Lesezeichen und Suchläufe" **Lesezeichen verwalten**.
- 2 Wählen Sie die zu löschenden Lesezeichen, und klicken Sie dann auf **—**.
- 3 Klicken Sie auf **Ja** und anschließend auf **Schließen**.

Verwenden von Kategorien und Schlüsselwörtern


Mit Schlüsselwörtern können Sie Geräten angepasste Tags zuweisen und die Flexibilität bei der Suche und Organisation von Geräten im System erhöhen. Gruppieren Sie Schlüsselwörter in Kategorien, und weisen Sie einem Gerät dann mehrere Schlüsselwörter mehrerer Kategorien zu.

Bevor Sie ein neues Schlüsselwort erstellen können, müssen Sie zuerst eine Kategorie erstellen, zu der das Schlüsselwort gehört.


Sie können zum Beispiel eine Kategorie mit der Bezeichnung **Standort** erstellen und dann innerhalb dieser Kategorie Schlüsselwörter erstellen. Beispiele von Schlüsselwörtern innerhalb der Kategorie "Standort" können **Gebäude 1**, **Gebäude 2** sein, oder etwas Spezifischeres für die speziellen Anforderungen Ihres Unternehmens.

Nachdem Sie Kategorien und Schlüsselwörter erstellt haben, können Sie die Schlüsselwörter dann mehreren Geräten zuweisen. Sie können auf der Basis der ihnen zugewiesenen Schlüsselwörter nach Geräten suchen und die Ergebnisse Ihrer Suche dann zum späteren Gebrauch in die Lesezeichen aufnehmen.

Hinzufügen, Bearbeiten oder Löschen von Kategorien


- 1 Klicken Sie bei Bedarf auf der Registerkarte "Assets" auf **Schlüsselwörter**, um den Bereich "Schlüsselwörter" anzuzeigen.
- 2 Klicken Sie im Fenster "Kategorie" auf **+**, um  hinzuzufügen, **—** zu bearbeiten oder um eine Kategorie zu löschen.
Hinweis: Mit dem Löschen einer Kategorie werden auch deren Schlüsselwörter gelöscht und aus den Geräten, denen diese Schlüsselwörter zugewiesen sind, entfernt.
- 3 Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Hinzufügen, Bearbeiten oder Löschen von Schlüsselwörtern


- 1 Klicken Sie bei Bedarf auf der Registerkarte "Assets" auf **Schlüsselwörter**, um den Bereich "Schlüsselwörter" anzuzeigen.
- 2 Führen Sie im Fenster "Schlüsselwörter" einen der folgenden Schritte durch:
 - So fügen Sie ein Schlüsselwort hinzu:
 - a Wählen Sie aus dem Fenster "Kategorie" eine Kategorie aus, der das Schlüsselwort angehört.
 - b Klicken Sie im Fenster "Schlüsselwörter" auf **+**.
 - c Geben Sie den Namen des neuen Schlüsselworts ein, und drücken Sie dann die **Eingabetaste**.
 - So bearbeiten Sie ein Schlüsselwort:
 - a Wählen Sie ein vorhandenes Schlüsselwort, und klicken Sie dann auf .
 - b Bearbeiten Sie den Namen, und drücken Sie dann die **Eingabetaste**.
 - So wird ein Schlüsselwort gelöscht:
 - a Wählen Sie ein vorhandenes Schlüsselwort, und klicken Sie dann auf **—**.
 - b Klicken Sie auf **Ja**.

Hinweis: Wenn Sie ein Schlüsselwort löschen, wird es von den Geräten entfernt, denen es zugewiesen ist.

Zuordnen von Schlüsselwörtern zu Geräten

- 1 Klicken Sie bei Bedarf auf der Registerkarte "Assets" auf **Schlüsselwörter**, um den Bereich "Suchprofile" anzuzeigen und ein Schlüsselwort auszusuchen.
Hinweis: Mehrere Schlüsselwörter können Sie mit **Umschalttaste + Klick** oder **Strg + Klick** auswählen.
- 2 Wählen Sie das Kontrollkästchen neben der IP-Adresse des Geräts aus, dem das Schlüsselwort zugewiesen werden soll.
Hinweis: Sie können auch mehrere oder alle Geräte auswählen.
- 3 Klicken Sie auf .
- 4 Prüfen Sie im Bereich "Taskinformationen", ob die Task abgeschlossen ist.
- 5 Um festzustellen, ob dem Gerät ein Schlüsselwort erfolgreich zugewiesen wurde, sehen Sie in den Geräteeigenschaften nach, indem Sie die IP-Adresse des Geräts wählen.
Im Abschnitt "Identifikationseigenschaft" wird der neue Wert des Schlüsselworts für das Gerät angezeigt.

Entfernen zugewiesener Schlüsselwörter aus Geräten

- 1 Wählen Sie auf der Registerkarte "Assets" das Kontrollkästchen neben der IP-Adresse des Geräts aus, aus dem Sie das Schlüsselwort entfernen möchten.
- 2 Klicken Sie bei Bedarf auf **Schlüsselwörter**, um den Bereich "Schlüsselwörter" anzuzeigen.
- 3 Wählen Sie ein Schlüsselwort, und klicken Sie dann auf  .
- 4 Wählen Sie das zu entfernende Schlüsselwort, und klicken Sie dann auf **OK**.
Hinweis: Mehrere Schlüsselwörter können Sie mit **Umschalttaste + Klick** oder **Strg + Klick** auswählen.
- 5 Prüfen Sie im Bereich "Taskinformationen", ob die Task abgeschlossen ist.
- 6 So prüfen Sie, ob das Schlüsselwort erfolgreich aus dem Gerät entfernt wurde:
 - a Wählen Sie die IP-Adresse des Geräts aus.
 - b Stellen Sie im Abschnitt "Identifikationseigenschaft" sicher, dass das Schlüsselwort nicht mehr angezeigt wird.

Verwalten von Richtlinien

Eine Richtlinie ist eine Zusammenstellung von Konfigurationsinformationen, die einem Gerät oder einer Gerätegruppe desselben Modells zugewiesen werden kann. Vergewissern Sie sich, ob die Konfigurationsinformationen eines Geräts oder einer Gerätegruppe einer bestimmten Richtlinie entsprechen, indem Sie eine Übereinstimmungsprüfung durchführen. Wenn die Übereinstimmungsprüfung ergibt, dass das Gerät nicht der Richtlinie entspricht, können Sie entscheiden, ob die Richtlinie für dieses Gerät bzw. die Gerätegruppe durchgesetzt wird.

Erstellen von Richtlinien mit einem voreingestellten Funktionstyp:

- Kopie
- E-Mail/FTP
- Fax
- Flash-Laufwerk
- Firmware
- Allgemein
- Netzwerk
- Papier
- Drucken
- Sicherheit

Hinweis: Weitere Informationen zur Sicherheitsrichtlinie finden Sie unter "Grundlagen zur Sicherheitsrichtlinie" auf Seite 32.



Jeder Richtlinientyp enthält exklusive Einstellungen, mit denen sichergestellt wird, dass bei der Zuweisung mehrerer Richtlinientypen zu einem Gerät keine Einstellungskonflikte auftreten.

Erstellen einer Richtlinie

Erstellen neuer Richtlinien


- 1 Klicken Sie bei Bedarf auf der Registerkarte "Richtlinien" auf **Geräterichtlinien**, um den Abschnitt "Geräterichtlinien" anzuzeigen.
- 2 Klicken Sie auf **+**, und geben Sie dann den Namen der neuen Richtlinie ein.
Hinweis: Stellen Sie sicher, dass der Richtliniename für die einzelnen Gerätemodelle eindeutig ist und noch nicht in der Datenbank existiert.
- 3 Wählen Sie aus der Liste "Unterstützte Modelle" ein Gerät aus.
- 4 Wählen Sie aus dem Dropdown-Menü "Typ" einen Richtlinientyp, und klicken Sie dann auf **OK**.
- 5 Wählen Sie aus dem Dialogfeld "Neue Richtlinie" das Kontrollkästchen **Name einstellen**.
Alle Einstellungen werden automatisch ausgewählt, und Sie können jede einzelne Einstellung anpassen.
- 6 Deaktivieren Sie das Kontrollkästchen neben einer Einstellung, um diese bei der Ausführung einer Übereinstimmungsprüfung oder einer Task zur Durchsetzung einer Richtlinie *auszuschließen*.
- 7 Wählen Sie für jede Einstellung einen Wert, den Sie bei einer Übereinstimmungsprüfung oder einer Task zur Durchsetzung einer Richtlinie hinzufügen möchten.
- 8 Klicken Sie auf **Speichern**.

Erstellen von Geräte Richtlinien

- 1 Wählen Sie auf der Registerkarte "Richtlinien" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
- 2 Klicken Sie auf **Geräte Richtlinien**, um den Abschnitt "Geräte Richtlinien" anzuzeigen, und klicken Sie dann auf .
- 3 Geben Sie im Feld "Name" den Namen der neuen Richtlinie ein.
- 4 Wählen Sie den Richtlinientyp aus, und klicken Sie dann auf **OK**.
Hinweis: Sie können auch mehrere oder alle Richtlinientypen auswählen.
- 5 Bearbeiten Sie ggf. die Einstellungen der neu erstellten Richtlinie.
 - a Wählen Sie im Abschnitt "Geräte Richtlinien" den Namen der neu erstellten Richtlinie aus, und klicken Sie dann auf .
 - b Wählen Sie für jede Einstellung einen Wert, den Sie bei einer Übereinstimmungsprüfung oder einer Task zur Durchsetzung einer Richtlinie hinzufügen möchten.
 - c Deaktivieren Sie das Kontrollkästchen neben einer Einstellung, um diese bei der Ausführung einer Übereinstimmungsprüfung oder einer Task zur Durchsetzung einer Richtlinie *auszuschließen*.
 - d Klicken Sie auf **Speichern**.
- 6 Stellen Sie sicher, dass die Einstellungen in der aktuell erstellten Richtlinie gültige Werte enthalten.

Wenn die Richtlinie als roter Text angezeigt wird und ihr Name mit einem Ausrufezeichen beginnt, kann sie nicht einem Gerät zugewiesen werden. Das bedeutet, dass eine oder mehrere Einstellungen in der Richtlinie einen ungültigen Wert enthalten und daher nicht für ein Gerät in seinem aktuellem Status durchgesetzt werden können.

Eine Richtlinie wird einem Gerät so zugewiesen:

- a Wählen Sie eine Richtlinie, und klicken Sie dann auf .
- b Geben Sie einen gültigen Wert für die Einstellungen an, und klicken Sie dann auf **Speichern**.
- c Wenn eine Warnmeldung angezeigt wird, notieren Sie sich die Einstellungen mit den ungültigen Werten.
- d Klicken Sie auf **Nein**, und geben Sie dann einen gültigen Wert für jede angegebene Einstellung an.
- e Klicken Sie auf **Speichern**.
- f Bei Bedarf wiederholen Sie Schritt c bis Schritt e so lange, bis die Warnmeldung nicht mehr angezeigt wird.

Grundlagen zur Sicherheitsrichtlinie

Mithilfe von MarkVision kann die Einrichtung sicherheitsaktivierter Lexmark Geräte konfiguriert werden, darunter die Sicherheitseinstellungen der verschiedenen Gerätefunktionen sowie der Modus, in dem die Remote-Kommunikation ausgeführt wird.

Achten Sie bei Verwendung der Sicherheitsrichtlinie darauf, *ausschließlich* MarkVision zur Verwaltung der Sicherheitseinstellungen Ihrer Geräte einzusetzen. Die Verwendung eines anderen Systems in Kombination mit MarkVision kann ein unerwartetes Systemverhalten verursachen.

Die Sicherheitsrichtlinie kann nur einer bestimmten Untergruppe von Geräten zugewiesen werden. Die vollständige Liste unterstützter Geräte finden Sie unter "Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen" auf Seite 61.

Grundlagen zu gesicherten Geräten

Auf ein gesichertes Gerät können unterschiedliche Konfigurationen angewendet werden. Markvision unterstützt derzeit jedoch nur Geräte, die *vollständig uneingeschränkt* oder *vollständig eingeschränkt* sind.

Konfigurationen für vollständig uneingeschränkte und vollständig eingeschränkte Geräte

		Vollständig uneingeschränkt	Vollständig eingeschränkt
Geräteeinstellungen	<i>RM FAC (Remote Management Function Access Control)</i> oder erweitertes Kennwort Hinweis: Eine Liste der Geräte, die RM FAC unterstützen, finden Sie unter "Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen" auf Seite 61.	Keine Sicherheit oder kein Kennwort	RM FAC wird mithilfe einer Sicherheitsvorlage festgelegt oder ein Kennwort ist konfiguriert
	Relevante Anschlüsse	Folgende Anschlüsse sind geöffnet: <ul style="list-style-type: none"> • UDP 161 (SNMP) • UDP 9300/9301/9302 (NPAP) 	Geschlossen
	Sicherheitsbezogene Anschlüsse	Folgende Anschlüsse sind geöffnet: <ul style="list-style-type: none"> • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST) 	Folgende Anschlüsse sind geöffnet: <ul style="list-style-type: none"> • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)

		Vollständig uneingeschränkt	Vollständig eingeschränkt
Markvision-Einstellungen	Suchprofil	Vergewissern Sie sich, dass die Option Gesicherte Drucker in Suche einbeziehen deaktiviert ist.	Vergewissern Sie sich, dass die Option Gesicherte Drucker in Suche einbeziehen ausgewählt ist.
	Sind die für die Kommunikation zwischen Markvision und den Netzwerkgeräten verwendeten Kanäle sicher?	Nein Hinweise: <ul style="list-style-type: none"> Dieser Konfigurationstyp wird empfohlen, sofern keine ausdrücklichen Bedenken hinsichtlich der Sicherheit der Netzwerkkommunikation bestehen. Hiervon ausgenommen sind bestimmte Einstellungen, die <i>ausschließlich</i> über sichere Kanäle gelesen oder geschrieben werden können. 	Ja
	Wie wird die Sicherheitskonfiguration der Netzwerkgeräte ermittelt?	Neben der IP-Adresse eines vollständig uneingeschränkten Geräts wird im Hauptdatenraster von Markvision ein Symbol in Form eines <i>geöffneten</i> Vorhängeschlosses angezeigt.	Neben der IP-Adresse eines vollständig eingeschränkten Geräts wird im Hauptdatenraster von Markvision ein Symbol in Form eines <i>geschlossenen</i> Vorhängeschlosses angezeigt. Hinweis: Falls die Kommunikations-Anmeldeinformationen des Geräts in Markvision nicht bekannt sind, ist das geschlossene Vorhängeschloss zusätzlich rot durchgestrichen. Dies bedeutet, dass in Markvision keine über die einfache Suche hinausgehende Kommunikation mit dem Gerät möglich ist.
	Wie wird nach Geräten mit diesem Konfigurationstyp gesucht?	<ol style="list-style-type: none"> Wählen Sie im Bereich "Lesezeichen und erweiterte Suche" die Option Alle Drucker. Führen Sie im Bereich "Zusammenfassung Suchergebnisse" einen Bildlauf nach unten zur Kategorie "Kommunikation" aus und wählen Sie dann Ungesichert. 	<ol style="list-style-type: none"> Wählen Sie im Bereich "Lesezeichen und erweiterte Suche" die Option Alle Drucker. Führen Sie im Bereich "Zusammenfassung Suchergebnisse" einen Bildlauf nach unten zur Kategorie "Kommunikation" aus und wählen Sie dann Gesichert.

Hinweise:

- Wenn das Gerät oder Suchprofil keinem dieser Szenarien entspricht, kann ein unerwartetes oder nicht definiertes Systemverhalten auftreten.

- Stellen Sie *vor* der Gerätesuche sicher, dass sich das Gerät in einem ordnungsgemäßen Zustand befindet und dass das Suchprofil richtig konfiguriert wurde. Änderungen am Gerät oder Suchprofil nach dem Ausführen des Suchprofils können zu unerwartetem oder nicht definiertem Systemverhalten führen.

Grundlagen zu Einstellungen für Sicherheitsrichtlinien

Verwenden Sie die Sicherheitsrichtlinie, um die Sicherheitseinstellungen eines Netzwerkgeräts anzupassen.

Damit in Markvision Remote-Verwaltungsaufgaben für Netzwerkgeräte effizient ausgeführt werden können, stellen Sie sicher, dass die Sicherheitsrichtlinie folgende Parameter umfasst:

- Im Abschnitt "Allgemeine Einstellungen" der Sicherheitsrichtlinie sind die folgenden Einstellungen für den Anschlusszugriff auf **Aktiviert** oder auf **Sicher/Nicht sicher** festgelegt:
 - Anschlusszugriff: mDNS (UDP 5353)
 - Anschlusszugriff: TCP/UDP (6110/6100)
- Im Abschnitt "Zugriffssteuerungen" (falls für das Gerätemodell verfügbar) sind die Einstellungen "Änderungen der NPA-Netzwerkadapter-Einstellung" und "Firmware-Aktualisierungen" auf **Keine Sicherheit** festgelegt.
- Folgende Abschnitte (falls für das Gerätemodell verfügbar) sind schreibgeschützt und können nicht bearbeitet werden:
 - Zugriffssteuerungen
 - Sicherheitsvorlagen
 - Hinweis:** Für Bausteine in der Spalte "Authentifizierungseinrichtung" müssen u. U. Anmeldeinformationen angegeben werden.
 - Verschiedene Einstellungen
 - Hinweis:** Die Abschnitte "Zugriffssteuerungen", "Sicherheitsvorlagen" und "Verschiedene Einstellungen" sind nicht für alle Gerätemodelle verfügbar. Weitere Informationen finden Sie unter "Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen" auf Seite 61.

Verwenden von Bausteinen aus einer eSF-Anwendung

Falls Sie einen Baustein aus einer *eSF (Embedded Solutions Framework)*-Anwendung für die Sicherheitsrichtlinie verwenden möchten, stellen Sie zunächst sicher, dass die eSF-Anwendung auf allen beteiligten Geräten manuell installiert wurde. Beim Durchsetzen einer Sicherheitsrichtlinie wird die Installation der Anwendung von Markvision *nicht* erzwungen.

Hinweis: Nur die für alle eSF-Anwendungen verfügbaren internen Einstellungen werden geklont, auf Einhaltung überprüft oder entsprechend der Richtlinie durchgesetzt.

Erstellen einer Sicherheitsrichtlinie

Zum Erstellen einer Sicherheitsrichtlinie klonen Sie zunächst eine vorhandene Richtlinie von einem vorkonfigurierten Mastergerät.

Klonen einer Sicherheitsrichtlinie zur Einschränkung von Geräten

Schritt 1. Konfigurieren der Einschränkung eines Geräts mithilfe von Embedded Web Server

Nachdem Sie die Einschränkung eines Geräts konfiguriert haben, verwenden Sie dieses Gerät als Mastergerät, das für eine Sicherheitsrichtlinie geklont wird.

- 1 Wenn das Gerätemodell die Remote-Verwaltungs-Zugriffssteuerung unterstützt, legen Sie die Zugriffssteuerung auf eine vorhandene Sicherheitsvorlage fest. Wenn das Gerät die Remote-Verwaltungs-Zugriffssteuerung nicht unterstützt, konfigurieren Sie ein erweitertes Kennwort. Führen Sie einen der folgenden Schritte durch:

Hinweis: Eine Liste der Geräte, die die Remote-Verwaltungs-Zugriffssteuerung unterstützen, finden Sie unter "Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen" auf Seite 61.

Konfigurieren der Remote-Verwaltungs-Zugriffssteuerung

- a Klicken Sie in Markvision auf **Service Desk**.
- b Suchen Sie das zu konfigurierende Gerät und wählen Sie dessen IP-Adresse aus.
- c Klicken Sie auf **Eingebettete Webseite >Einstellungen >Sicherheit >Sicherheitseinstellung**.
- d Klicken Sie im Abschnitt "Erweiterte Sicherheitseinstellung" auf **Zugriffssteuerungen**.
- e Führen Sie einen Bildlauf zu "Remote-Verwaltung" aus und wählen Sie dann im zugehörigen Dropdown-Menü eine Sicherheitsvorlage aus.
Hinweis: In der Sicherheitsvorlage muss nur die Authentifizierung angegeben sein.
- f Klicken Sie auf **Übernehmen**.

Konfigurieren eines erweiterten Kennworts

- a Klicken Sie in Markvision auf **Service Desk**.
- b Suchen Sie das zu konfigurierende Gerät und wählen Sie dessen IP-Adresse aus.
- c Klicken Sie auf **Eingebettete Webseite >Konfiguration >Sicherheit**.
- d Klicken Sie auf **Kennwort erstellen/ändern** oder **Kennwort erstellen**.
- e Klicken Sie ggf. auf **Erweitertes Kennwort erstellen** und geben Sie dann ein Kennwort ein.
- f Bestätigen Sie das Kennwort, indem Sie es in das nächste Feld ein zweites Mal eingeben, und klicken Sie dann auf **Übernehmen**.

- 2 Stellen Sie sicher, dass die relevanten Anschlüsse geschlossen und die Sicherheitsanschlüsse geöffnet sind.


Hinweis: Sie können ggf. **Sicherer Modus** auswählen und dann mit Schritt 3 fortfahren.

- a Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration** und klicken Sie dann auf **Sicherheit >TCP/IP-Anschlusszugriff**.
- b Suchen Sie die folgenden relevanten Anschlüsse und deaktivieren Sie ggf. die Kontrollkästchen daneben oder wählen Sie **Deaktiviert** aus den Dropdown-Menüs aus.
 - **UDP 161 (SNMP)**
 - **UDP 9300/9301/9302 (NPAP)**

- c Suchen Sie die folgenden Sicherheitsanschlüsse und stellen Sie sicher, dass die daneben angezeigten Kontrollkästchen aktiviert sind oder dass Sie **Sicher/Nicht sicher** aus den Dropdown-Menüs ausgewählt haben.
 - **UDP 5353 (mDNS)**
 - **TCP 6110**
 - **TCP/UDP 6100 (LST)**
 - d Klicken Sie auf **Übernehmen**.
 - 3 Konfigurieren Sie weitere Sicherheitseinstellungen.
 - a Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration** und dann auf **Sicherheit**.
 - b Nehmen Sie ggf. weitere Änderungen an den Sicherheitseinstellungen vor.
 - c Nachdem Sie zusätzliche Änderungen vorgenommen haben, klicken Sie auf **Einstellungen** oder **Konfiguration** und klicken dann auf **Sicherheit > Sicherheitsübersicht anzeigen** (sofern auf dem Gerätemodell verfügbar).
 - d Überprüfen Sie, ob Ihre Änderungen auf der Übersichtsseite angezeigt werden.


Hinweis: Wenn Sie anstelle der Remote-Verwaltungs-Zugriffssteuerung ein erweitertes Kennwort verwenden, muss das Mastergerät nicht mithilfe des Embedded Web Servers eingeschränkt werden. Sie können mithilfe von Markvision eine Sicherheitsrichtlinie für ein beliebiges Gerät erstellen und anschließend das erweiterte Kennwort und die Anmeldeinformationen im Abschnitt "Allgemeine Einstellungen" der Richtlinie konfigurieren.

Schritt 2. Überprüfen, ob das eingeschränkte Gerät, das als Mastergerät dient, von Markvision erkannt wird

- 1 Erstellen Sie ein Suchprofil. Weitere Informationen zum Erstellen eines Suchprofils finden Sie unter "Erstellen eines Suchprofils" auf Seite 18.
- 2 Vergewissern Sie sich im Dialogfeld "Hinzufügen" des Suchprofils, dass "Gesicherte Drucker in Suche einbeziehen" ausgewählt ist.
- 3 Klicken Sie auf , um das Suchprofil auszuführen.

Hinweis: Zu diesem Zeitpunkt wurde das Gerät "teilweise erkannt". Dies bedeutet, dass Markvision begrenzte Informationen zum Gerät gefunden hat, jedoch nicht in der Lage ist, zusätzliche Funktionen auszuführen, beispielsweise die Einhaltung von Richtlinien festzustellen, Richtlinien durchzusetzen sowie das Gerät zu prüfen. Damit die vollständigen Informationen abgerufen werden können müssen Sie die Kommunikations-Anmeldeinformationen des Geräts angeben.

Schritt 3. Starten des Klonvorgangs


- 1 Klicken Sie in Markvision auf **Richtlinien**.
- 2 Suchen Sie das eingeschränkte Mastergerät und aktivieren Sie das Kontrollkästchen neben dessen IP-Adresse.
- 3 Klicken Sie ggf. auf **Geräterichtlinien** und auf .
- 4 Geben Sie im Feld "Name" den Namen der neuen Sicherheitsrichtlinie ein.
- 5 Vergewissern Sie sich, dass der Typ der Sicherheitsrichtlinie ausgewählt ist.
- 6 Geben Sie die erforderlichen Anmeldeinformationen für die Authentifizierung beim Gerät ein und klicken Sie dann auf **OK**.

Hinweis: Verwenden Sie die Anmeldeinformationen aus der in der Remote-Verwaltungs-Zugriffssteuerung festgelegten Sicherheitsvorlage oder verwenden Sie das konfigurierte erweiterte Kennwort.

7 Warten Sie, bis der Klonvorgang abgeschlossen ist.

Wenn der Name der Richtlinie rot dargestellt ist, bedeutet dies, dass keine Anmeldeinformationen angegeben wurden und dass die Richtlinie einem Gerät im aktuellen Zustand nicht zugewiesen werden kann. Damit die Richtlinie einem Gerät zugewiesen werden kann, geben Sie die richtigen Anmeldeinformationen für das Gerät ein.

8 Bearbeiten Sie die Einstellungen der neuen Sicherheitsrichtlinie und stellen Sie sicher, dass die Einstellungen in der Richtlinie gültige Werte enthalten.

a Wählen Sie im Abschnitt "Geräterichtlinien" den Namen der Richtlinie aus und klicken Sie dann auf .

b Wählen Sie für jede Einstellung, die bei einer Prüfung der Richtlinienübereinstimmung oder einer Task zur Durchsetzung einer Richtlinie berücksichtigt werden soll, einen Wert aus.

c Deaktivieren Sie das Kontrollkästchen neben einer Einstellung, um diese aus einer Prüfung der Richtlinienübereinstimmung oder einer Task zur Durchsetzung einer Richtlinie *auszuschließen*.

d Geben Sie das Sicherheitskennwort ein und klicken Sie auf **Speichern**.

Hinweis: Weitere Informationen zu den gültigen Einstellungen für eine Sicherheitsrichtlinie finden Sie unter "Grundlagen zu Einstellungen für Sicherheitsrichtlinien" auf Seite 34.

9 Weisen Sie die Sicherheitsrichtlinie uneingeschränkten Geräten zu, die dasselbe Modell wie das eingeschränkte Mastergerät aufweisen.

Weitere Informationen zum Zuweisen einer Richtlinie zu mehreren Geräten finden Sie unter "Richtlinien zuweisen" auf Seite 41.

10 Setzen Sie die Sicherheitsrichtlinie für die ausgewählten Geräte durch.

Weitere Informationen zum Durchsetzen einer Richtlinie finden Sie unter "Durchsetzen von Richtlinien" auf Seite 42.

11 Suchen Sie erneut nach den Geräten.

Die Geräte unterliegen jetzt Einschränkungen. Darüber hinaus sind die Kommunikations-Anmeldeinformationen des Geräts jetzt in Markvision bekannt und können verwendet werden, um sowohl im Servicebereich "Bestand" als auch im Servicebereich "Richtlinien" Tasks auszuführen.

Klonen einer Sicherheitsrichtlinie, um die Einschränkung von Geräten aufzuheben

Schritt 1. Aufheben der Einschränkung eines Geräts mithilfe von Embedded Web Server

Nachdem Sie die Einschränkung eines Geräts aufgehoben haben, verwenden Sie dieses Gerät als Mastergerät, das für eine Sicherheitsrichtlinie geklont wird.

- 1** Wenn das Gerätemodell die Remote-Verwaltungs-Zugriffssteuerung unterstützt, legen Sie die Zugriffssteuerung auf **Keine Sicherheit** fest. Wenn das Gerät die Remote-Verwaltungs-Zugriffssteuerung nicht unterstützt, entfernen Sie das erweiterte Kennwort. Führen Sie einen der folgenden Schritte durch:

Hinweis: Eine Liste der Geräte, die die Remote-Verwaltungs-Zugriffssteuerung unterstützen, finden Sie unter "Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen" auf Seite 61.

Konfigurieren der Remote-Verwaltungs-Zugriffssteuerung

- a** Klicken Sie in Markvision auf **Service Desk**.
- b** Suchen Sie das zu konfigurierende Gerät und wählen Sie dessen IP-Adresse aus.
- c** Klicken Sie auf **Eingebettete Webseite >Einstellungen >Sicherheit >Sicherheitseinstellung**.
- d** Klicken Sie im Abschnitt "Erweiterte Sicherheitseinstellung" auf **Zugriffssteuerungen**.

- e Führen Sie einen Bildlauf zu **Remote-Verwaltung** aus und wählen Sie dann aus dem Dropdown-Menü **Keine Sicherheit** aus.
- f Klicken Sie auf **Übernehmen**.

Entfernen des erweiterten Kennworts

- a Klicken Sie in Markvision auf **Service Desk**.
- b Suchen Sie das zu konfigurierende Gerät und wählen Sie dessen IP-Adresse aus.
- c Klicken Sie auf **Eingebettete Webseite >Konfiguration >Sicherheit**.
- d Klicken Sie auf **Kennwort erstellen/ändern** oder **Kennwort erstellen**.
- e Klicken Sie ggf. auf **Erweitertes Kennwort erstellen**.
- f Löschen Sie die Kennwortfelder und klicken Sie dann auf **Übernehmen**.

2 Stellen Sie sicher, dass die relevanten Anschlüsse und die Sicherheitsanschlüsse geöffnet sind.

- a Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration** und klicken Sie dann auf **Sicherheit >TCP/IP-Anschlusszugriff**.
- b Suchen Sie die folgenden Anschlüsse und stellen Sie dann sicher, dass sie ausgewählt oder auf **Sicher/Nicht sicher** festgelegt sind.

Relevante Anschlüsse

- **UDP 161 (SNMP)**
- **UDP 9300/9301/9302 (NPAP)**

Sicherheitsanschlüsse

- **UDP 5353 (mDNS)**
- **TCP 6110**
- **TCP/UDP 6100 (LST)**


- c Klicken Sie auf **Übernehmen**.

3 Konfigurieren Sie weitere Sicherheitseinstellungen.


- a Klicken Sie im Embedded Web Server auf **Einstellungen** oder **Konfiguration** und dann auf **Sicherheit**.
- b Nehmen Sie ggf. weitere Änderungen an den Sicherheitseinstellungen vor.
- c Nachdem Sie zusätzliche Änderungen vorgenommen haben, klicken Sie auf **Einstellungen** oder **Konfiguration** und klicken dann auf **Sicherheit >Sicherheitsübersicht anzeigen** (sofern auf dem Gerätemodell verfügbar).
- d Überprüfen Sie, ob Ihre Änderungen auf der Übersichtsseite angezeigt werden.

Hinweis: Wenn Sie anstelle der Remote-Verwaltungs-Zugriffssteuerung ein erweitertes Kennwort verwenden, muss die Einschränkung des Mastergeräts nicht mithilfe des Embedded Web Servers aufgehoben werden. Sie können mithilfe von Markvision eine Sicherheitsrichtlinie für ein beliebiges Gerät erstellen und anschließend das erweiterte Kennwort und die Anschlusseinstellungen im Abschnitt "Allgemeine Einstellungen" der Richtlinie konfigurieren.


Schritt 2. Überprüfen, ob das uneingeschränkte Gerät, das als Mastergerät dient, von Markvision erkannt wird

- 1 Erstellen Sie ein Suchprofil. Weitere Informationen zum Erstellen eines Suchprofils finden Sie unter "Erstellen eines Suchprofils" auf Seite 18.
- 2 Vergewissern Sie sich im Dialogfeld "Hinzufügen" des Suchprofils, dass das Kontrollkästchen **Gesicherte Drucker in Suche einbeziehen** deaktiviert ist.
- 3 Klicken Sie auf , um das Suchprofil auszuführen.

Schritt 3. Starten des Klonvorgangs

- 1 Klicken Sie in Markvision auf **Richtlinien**.
- 2 Suchen Sie das uneingeschränkte Gerät und aktivieren Sie das Kontrollkästchen neben dessen IP-Adresse.
- 3 Klicken Sie ggf. auf **Geräterichtlinien** und auf .
- 4 Geben Sie im Feld "Name" den Namen der neuen Sicherheitsrichtlinie ein.
- 5 Vergewissern Sie sich, dass der Typ der Sicherheitsrichtlinie ausgewählt ist.
- 6 Geben Sie die erforderlichen Anmeldeinformationen für die Authentifizierung beim Gerät ein und klicken Sie dann auf **OK**.

Hinweis: Verwenden Sie die Anmeldeinformationen aus der in der Remote-Verwaltungs-Zugriffssteuerung festgelegten Sicherheitsvorlage oder verwenden Sie das konfigurierte erweiterte Kennwort.

- 7 Warten Sie, bis der Klonvorgang abgeschlossen ist.
Wenn der Name der Richtlinie rot dargestellt ist, bedeutet dies, dass keine Anmeldeinformationen angegeben wurden und dass die Richtlinie einem Gerät im aktuellen Zustand nicht zugewiesen werden kann. Damit die Richtlinie einem Gerät zugewiesen werden kann, geben Sie die richtigen Anmeldeinformationen für das Gerät ein.
- 8 Bearbeiten Sie die Einstellungen der neuen Sicherheitsrichtlinie und stellen Sie sicher, dass die Einstellungen in der Richtlinie gültige Werte enthalten.
 - a Wählen Sie im Abschnitt "Geräterichtlinien" den Namen der Richtlinie aus und klicken Sie dann auf .
 - b Wählen Sie für jede Einstellung, die bei einer Prüfung der Richtlinienübereinstimmung oder einer Task zur Durchsetzung einer Richtlinie berücksichtigt werden soll, einen Wert aus.
 - c Deaktivieren Sie das Kontrollkästchen neben einer Einstellung, um diese aus einer Prüfung der Richtlinienübereinstimmung oder einer Task zur Durchsetzung einer Richtlinie *auszuschließen*.
 - d Klicken Sie auf **Speichern**.

Hinweis: Weitere Informationen zu den gültigen Einstellungen für eine Sicherheitsrichtlinie finden Sie unter "Grundlagen zu Einstellungen für Sicherheitsrichtlinien" auf Seite 34.

- 9 Weisen Sie die Sicherheitsrichtlinie uneingeschränkten Geräten zu, die dasselbe Modell wie das uneingeschränkte Mastergerät aufweisen.

Hinweise:

- Weitere Informationen zum Zuweisen einer Richtlinie zu mehreren Geräten finden Sie unter "Richtlinien zuweisen" auf Seite 41.
- Falls eines der ausgewählten Geräte eingeschränkt ist, wird dessen Einschränkung nach Durchsetzung der Richtlinie aufgehoben.

- 10 Setzen Sie die Sicherheitsrichtlinie für die ausgewählten Geräte durch.

Weitere Informationen zum Durchsetzen einer Richtlinie finden Sie unter "Durchsetzen von Richtlinien" auf Seite 42.

- 11 Suchen Sie erneut nach den Geräten.

Die Geräte unterliegen jetzt keinen Einschränkungen mehr und können von allen Servicebereichen genutzt werden.

Ändern der Kommunikations-Anmeldeinformationen eines eingeschränkten Geräts

Die *Kommunikations-Anmeldeinformationen* werden zur Authentifizierung eines Netzwerkgeräts mithilfe von Lexmark Secure Transport (LST) benötigt. Die Kommunikations-Anmeldeinformationen können folgende Angaben beinhalten: Benutzername, Bereich, Kennwort und *PIN* (persönliche Identifikationsnummer).


Hinweis: Einige Gerätemodelle unterstützen nur Kennwörter. Weitere Informationen finden Sie unter "Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen" auf Seite 61.

Kommunikations-Anmeldeinformationen können aus zwei Arten von Bausteinen bestehen:


- **Endgültige Autorität:** Bei der Authentifizierung oder Autorisierung der Anmeldeinformationen stellt der Baustein die endgültige Autorität dar. Beispiele sind Kennwörter oder PINs.
- **Pass-Through-Autorität:** Bei der Authentifizierung oder Autorisierung werden die Anmeldeinformationen vom Baustein an eine externe Autorität weitergeleitet. Beispiele für eine externe Autorität sind Lightweight Directory Access Protocol (LDAP) und Kerberos.

Ändern der Anmeldeinformationen eines Bausteins für eine endgültige Autorität

Hinweis: Die Sicherheitsrichtlinienoptionen "Zugriffssteuerungen" und "Sicherheitsvorlagen" sind nicht für alle Gerätemodelle verfügbar. Weitere Informationen finden Sie unter "Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen" auf Seite 61.



- 1 Klicken Sie bei Bedarf auf der Registerkarte "Richtlinien" auf **Geräterichtlinien**, um den Abschnitt "Geräterichtlinien" anzuzeigen.
- 2 Wählen Sie die gewünschte eingeschränkte Sicherheitsrichtlinie aus und klicken Sie auf  **>Zugriffssteuerungen**.
- 3 Suchen Sie **Remote-Verwaltung** und notieren Sie sich den zugehörigen Wert.
- 4 Klicken Sie auf **Sicherheitsvorlagen**.
- 5 Wählen Sie in der Spalte "Authentifizierungseinrichtung" den Baustein neben dem unter Schritt 3 notierten Wert.
- 6 Geben Sie in das Feld "Kennwort" das neue Kennwort ein.
- 7 Bestätigen Sie das Kennwort, indem Sie es in das nächste Feld ein zweites Mal eingeben, und klicken Sie dann auf **Speichern**.
- 8 Setzen Sie die eingeschränkte Sicherheitsrichtlinie für die zugewiesenen Geräte durch.
Nachdem die Task zur Durchsetzung erfolgreich abgeschlossen wurde, werden die Kommunikations-Anmeldeinformationen der Geräte aktualisiert.

Ändern der Anmeldeinformationen eines Bausteins für eine Pass-Through-Autorität


- 1 Ändern Sie die Anmeldeinformationen über die von Ihnen verwendete externe Autorität.
- 2 Klicken Sie auf der Markvision Webseite auf **Richtlinien >Geräterichtlinien**, um den Abschnitt "Geräterichtlinien" anzuzeigen.
- 3 Wählen Sie die gewünschte eingeschränkte Sicherheitsrichtlinie aus und klicken Sie auf  **>Geräteanmeldeinformationen**.
- 4 Aktualisieren Sie im Abschnitt "Geräteanmeldeinformationen" die aktuellen Werte auf die neuen Werte, die Sie unter Verwendung der externen Autorität eingegeben haben.

- 5 Klicken Sie auf **Speichern**.
- 6 Setzen Sie die eingeschränkte Sicherheitsrichtlinie für die zugewiesenen Geräte durch.
Nachdem die Task zur Durchsetzung erfolgreich abgeschlossen wurde, kann Markvision wieder erfolgreich mit den Geräten kommunizieren.

Bearbeiten oder Löschen von Richtlinien


- 1 Klicken Sie bei Bedarf auf der Registerkarte "Richtlinien" auf **Geräterichtlinien**, um den Abschnitt "Geräterichtlinien" anzuzeigen.
- 2 Wählen Sie eine Richtlinie aus, und gehen Sie anschließend wie folgt vor:
 - Um die Richtlinie zu bearbeiten, klicken Sie auf .
 - a Geben Sie bei Bedarf im Feld "Name der Richtlinie" den neuen Namen der Richtlinie ein.
 - b Wählen Sie für jede Einstellung einen Wert, den Sie bei einer Übereinstimmungsprüfung oder einer Task zur Durchsetzung einer Richtlinie hinzufügen möchten.
 - c Deaktivieren Sie das Kontrollkästchen neben einer Einstellung, um diese bei der Ausführung einer Übereinstimmungsprüfung oder einer Task zur Durchsetzung einer Richtlinie *auszuschließen*.
 - d Klicken Sie auf **Speichern**.
 - Um eine Richtlinie zu löschen, klicken Sie auf  und anschließend auf **Ja**.

Richtlinien zuweisen

- 1 Klicken Sie bei Bedarf auf der Registerkarte "Richtlinien" auf **Geräterichtlinien**, um den Abschnitt "Geräterichtlinien" anzuzeigen.
- 2 Wählen Sie eine Richtlinie aus.
Hinweise:
 - Mehrere Richtlinien können Sie mit **Umschalttaste + Klick** oder **Strg + Klick** auswählen.
 - Sie können einem Gerät gleichzeitig mehrere Richtlinientypen zuweisen, aber nur eine Richtlinie je Richtlinientyp verwenden.
- 3 Wählen Sie das Kontrollkästchen neben der IP-Adresse des Geräts, dem die Richtlinie zugewiesen werden soll.
Hinweis: Sie können auch mehrere oder alle Geräte auswählen.
- 4 Klicken Sie auf .
In der Spalte "Richtlinientyp" wird neben dem ausgewählten Gerät ein Fragezeichen angezeigt.
Mit dem Fragezeichen wird angezeigt, dass das Gerät noch nicht auf Übereinstimmung der zugewiesenen Richtlinie geprüft wurde.


Überprüfen der Übereinstimmung mit Richtlinien

- 1 Wählen Sie auf der Registerkarte "Richtlinien" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
Hinweis: Sie können auch mehrere oder alle Geräte auswählen.
- 2 Klicken Sie auf **Übereinstimmung**.

- 3 Wählen Sie im Dialogfeld "Richtlinien für Übereinstimmungsüberprüfung" einen Richtlinientyp, und klicken Sie anschließend auf **OK**.
- 4 Prüfen Sie, ob in der Spalte "Richtlinientyp" neben dem ausgewählten Gerät ein Häkchen angezeigt wird.
- 5 Wenn ein Fragezeichen oder X angezeigt wird, klicken Sie auf , um die Einzelheiten dazu anzuzeigen.


Hinweis: Eine Übereinstimmungsprüfung einer Richtlinie kann zu einem festgelegten Zeitpunkt oder in regelmäßigen Abständen ausgeführt werden. Weitere Informationen finden Sie unter "Planen von Tasks" auf Seite 56.

Durchsetzen von Richtlinien

- 1 Wählen Sie auf der Registerkarte "Richtlinien" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
Hinweis: Sie können auch mehrere oder alle Geräte auswählen.
- 2 Klicken Sie auf **Durchsetzen**.
- 3 Wählen Sie im Dialogfeld "Richtlinien durchsetzen" einen Richtlinientyp aus, und klicken Sie anschließend auf **OK**.
- 4 Klicken Sie auf , um zu überprüfen, ob die Durchsetzung der Richtlinie abgeschlossen ist.

Hinweis: Eine Task zur Durchsetzung einer Richtlinie kann zu einem festgelegten Zeitpunkt oder in regelmäßigen Abständen ausgeführt werden. Weitere Informationen finden Sie unter "Planen von Tasks" auf Seite 56.

Entfernen von Richtlinien

- 1 Wählen Sie auf der Registerkarte "Richtlinien" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
- 2 Klicken Sie bei Bedarf auf **Geräterichtlinien**, um den Abschnitt "Geräterichtlinien" anzuzeigen, und klicken Sie dann auf .
- 3 Wählen Sie im Dialogfeld "Richtlinie entfernen" eine Richtlinie aus, und klicken Sie dann auf **OK**.
Hinweis: Sie können auch mehrere Richtlinien auswählen.

Verwalten des Service Desks

Arbeiten mit Richtlinien

Bevor Sie mit der Behebung eines Geräteproblems beginnen, stellen Sie zunächst sicher, dass das Gerät den zugewiesenen Richtlinien entspricht.

Überprüfen der Übereinstimmung des Geräts mit Richtlinien

- 1 Wählen Sie auf der Registerkarte "Service Desk" das Kontrollkästchen neben der IP-Adresse des Geräts aus.

Hinweis: Sie können auch mehrere oder alle Geräte auswählen.

- 2 Klicken Sie auf **Übereinstimmung**.

- 3 Wählen Sie im Dialogfeld "Richtlinien für Übereinstimmungsüberprüfung" einen Richtlinientyp, und klicken Sie anschließend auf **OK**.

- 4 Warten Sie im Bereich "Taskinformationen", bis die Task abgeschlossen ist.

- 5 Klicken Sie auf , um die Prüfungsergebnisse anzusehen.

Durchsetzen von Richtlinien


- 1 Wählen Sie auf der Registerkarte "Service Desk" das Kontrollkästchen neben der IP-Adresse des Geräts aus.

Hinweis: Sie können auch mehrere oder alle Geräte auswählen.

- 2 Klicken Sie auf **Durchsetzen**.

- 3 Wählen Sie im Dialogfeld "Richtlinien durchsetzen" einen Richtlinientyp aus, und klicken Sie anschließend auf **OK**.

- 4 Warten Sie im Bereich "Taskinformationen", bis die Task abgeschlossen ist.

- 5 Klicken Sie auf , um zu überprüfen, ob die Durchsetzung der Richtlinie abgeschlossen ist.

Arbeiten mit einem Gerät




Überprüfen des Gerätestatus

- 1 Suchen Sie mit Lesezeichen oder der erweiterten Suche ein Gerät.

Hinweis: Mit den Kategorien im Bereich "Zusammenfassung Suchergebnisse" können Sie die Liste der gefundenen Geräte eingrenzen.

- 2 Wählen Sie das Kontrollkästchen neben der IP-Adresse des Geräts, und klicken Sie dann auf **Aktuellen Status erfassen**.

- 3 Beachten Sie das Symbol neben dem Gerät in den Spalten "Druckerstatus" und "Verbrauchsmaterialstatus".

Symbol	Status
	OK: Das Gerät ist betriebsbereit, und es sind ausreichend Verbrauchsmaterialien vorhanden.
	Warnung: Das Gerät ist in Betrieb, aber die Verbrauchsmaterialien gehen eventuell zur Neige, oder es wird eine Wartung fällig.
	Fehler: Das Gerät oder die Verbrauchsmaterialien müssen umgehend gewartet bzw. aufgefüllt werden.

4 Klicken Sie auf **Mit dem Gerät arbeiten**, um Details zum Gerätestatus anzuzeigen.

Anzeigen von Geräten von einem entfernten Standort aus

Hinweis: Diese Funktion ist nur für Geräte mit Unterstützung der Anzeige von einem entfernten Standort aus verfügbar.

- 1 Wählen Sie auf der Registerkarte "Service Desk" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
- 2 Klicken Sie auf **Mit Gerät arbeiten**.
Ein Dialogfeld mit den Gerätedetails und einem Bild des Geräts wird angezeigt.
- 3 Klicken Sie auf **Druckerferne Bedienerkonsole > Klicken Sie hier, um fortzufahren**.
Ein weiteres Dialogfeld mit einer dynamischen Anzeige des Gerätebedienfelds in seinem aktuellen Status wird geöffnet.
- 4 Von der unteren linken Seite aus finden Sie die den einzelnen Schaltflächenbefehlen entsprechenden Tasten.
Hinweis: Die Position der Tastenentsprechung kann sich je nach Gerätemodell unterscheiden.

Anzeigen der eingebetteten Webseite

Hinweis: Diese Funktion ist nur für Geräte verfügbar, die die Anzeige ihrer eingebetteten Webseite von einem entfernten Standort aus unterstützen.

- 1 Wählen Sie auf der Registerkarte "Service Desk" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
- 2 Klicken Sie auf **Mit Gerät arbeiten**.
Ein Dialogfeld mit den Gerätedetails und einem Bild des Geräts wird angezeigt.
- 3 Klicken Sie auf **Eingebettete Webseite**.
Hinweis: Sie können auch im unteren Bereich des Dialogfensters die gewünschte Sprache auswählen.

Verwalten von Geräteereignissen

Mit dem Ereignis-Manager können Sie den Druckerpool proaktiv überwachen und verwalten. Legen Sie ein Ziel fest, sodass Sie oder andere angegebene Benutzer benachrichtigt werden, wenn ein bestimmtes Ereignis auftritt. Erstellen Sie ein automatisches Ereignis, wenn ein Gerät eine Warnung an das Netzwerk sendet.

Erstellen eines Ziels


Ein Ziel ist eine vordefinierte Aktion, die einen bestimmten Befehl ausführt, wenn ein bestimmtes Ereignis bei einer Reihe von Geräten auftritt. Ein Ziel kann eine E-Mail-Benachrichtigung oder eine Befehlszeilenaufforderung sein, wenn eine benutzerdefinierte Aktion benötigt wird.



- 1 Klicken Sie bei Bedarf in der Registerkarte "Ereignis-Manager" auf **Ziele**, damit der Bereich "Ziele" angezeigt wird.
- 2 Klicken Sie auf **+**, und geben Sie dann einen eindeutigen Namen für das Ziel ein.
- 3 Führen Sie einen der folgenden Schritte durch:
 - Wählen Sie **Befehl** aus, und klicken Sie dann auf **Weiter**.
 - a Geben Sie den Namen eines ausführbaren Befehls in das Feld "Befehlspfad" ein.
 - b Fügen Sie Schlüsselwörter zu den Befehlsparametern hinzu, indem Sie ein Schlüsselwort aus der Platzhalterliste auswählen, und klicken sie dann auf **►**.
 - Wählen Sie **E-Mail** aus, und klicken Sie dann auf **Weiter**.
 - a Stellen Sie sicher, dass Sie die E-Mail-Einstellungen im Dialogfeld "Systemkonfiguration" richtig konfiguriert haben.
Weitere Informationen finden Sie unter "Konfigurieren der E-Mail-Einstellungen" auf Seite 48.
 - b Geben Sie die Werte in die entsprechenden Felder ein.
 - **Von** – Geben Sie die E-Mail-Adresse des Absenders ein.
 - **An** – Geben Sie die E-Mail-Adresse des Empfängers ein.
 - **CC** – Geben Sie die E-Mail-Adressen anderer Empfänger ein, die eine Kopie der E-Mail erhalten sollen.
 - **Betreff** – Geben Sie bei Bedarf eine Betreffzeile für die E-Mail ein.
 - **Nachricht** – Geben Sie die standardmäßige E-Mail-Nachricht ein.

Hinweis: Sie können in der Spalte mit den Platzhaltern die verfügbaren *Platzhalter* teilweise oder vollständig als Betreffzeile verwenden. Sie können Platzhalter auch als Teil einer E-Mail-Nachricht verwenden. Platzhalter stellen variable Elemente dar, die bei Verwendung durch den tatsächlichen Wert ersetzt werden.

- 4 Klicken Sie auf **Fertig stellen**.

Bearbeiten oder Löschen eines Ziels


- 1 Klicken Sie bei Bedarf in der Registerkarte "Event-Manager" auf **Ziele**, damit aktive Ziele angezeigt werden.
- 2 Wählen Sie ein Ziel aus, und gehen Sie anschließend wie folgt vor:
 - Um das Ziel zu bearbeiten, klicken Sie auf .
 - a Bearbeiten Sie bei Bedarf den Zielnamen, und klicken Sie anschließend auf **Weiter**.
 - b Bearbeiten Sie bei Bedarf den Namen des ausführbaren Befehls im Feld "Befehlspfad".

- c Um ein Schlüsselwort aus dem Feld "Befehlsparameter" zu löschen, doppelklicken Sie auf das Schlüsselwort, und wählen Sie anschließend **Löschen**.
- d Um weitere Schlüsselwörter zu dem Feld "Befehlsparameter" hinzuzufügen, wählen Sie ein Schlüsselwort aus der Platzhalterliste aus, und klicken Sie anschließend auf .
- Um das Ziel zu löschen, klicken Sie auf  und anschließend auf **Ja**.



Warnung - Mögliche Schäden: Wenn Sie ein Ziel löschen, werden die zugeordneten Ereignisse ebenfalls gelöscht.

3 Klicken Sie auf **Fertig stellen**.


Erstellen von Ereignissen

- 1 Klicken Sie bei Bedarf in der Registerkarte "Ereignis-Manager" auf **Ereignisse**, damit der Bereich "Ereignisse" angezeigt wird.
- 2 Klicken Sie auf , und geben Sie anschließend einen eindeutigen Namen für das Ereignis und eine Beschreibung ein.
- 3 Wählen Sie im Bereich "Warnungen" eine Warnung aus, und klicken Sie anschließend auf **Weiter**.
Hinweis: Sie können auch mehrere oder alle Warnungen auswählen.
- 4 Wählen Sie ein Ziel aus, und gehen Sie anschließend wie folgt vor:
 - Um das Ereignis auszulösen, wenn die Warnung aktiviert wird, wählen Sie **Nur bei Aktiv** aus.
 - Um das Ereignis auszulösen, wenn die Warnung aktiviert und entfernt wird, wählen Sie **Bei Aktiv und Löschen** aus.
- 5 Klicken Sie auf **Fertig stellen**.


Bearbeiten oder Löschen von Ereignissen

- 1 Klicken Sie bei Bedarf in der Registerkarte "Ereignis-Manager" auf **Ereignisse**, damit die aktiven Ereignisse angezeigt werden.
- 2 Wählen Sie ein Ereignis aus, und gehen Sie anschließend wie folgt vor:
 - Um das Ereignis zu bearbeiten, klicken Sie auf .
 - a Bearbeiten Sie bei Bedarf den Ereignisnamen und die Beschreibung.
 - b Fügen Sie im Bereich "Warnungen" weitere Warnungen durch Auswählen hinzu, oder entfernen Sie eine Warnung, indem Sie das Kontrollkästchen daneben deaktivieren.
 - c Klicken Sie auf **Weiter**.
 - d Fügen Sie im Bereich "Ziele" weitere Ziele durch Auswählen hinzu, oder entfernen Sie ein Ziel, indem Sie das Kontrollkästchen daneben deaktivieren.
 - e Wählen Sie ein Auslöseziel, und klicken Sie anschließend auf **Fertig stellen**.
 - Um ein Ereignis zu löschen, klicken Sie auf  und anschließend auf **Ja**.

Zuordnen von Ereignissen zu einem Gerät

- 1 Wählen Sie in der Registerkarte "Ereignis-Manager" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
- 2 Klicken Sie bei Bedarf auf **Ereignisse**, damit aktive Ereignisse angezeigt werden.
- 3 Wählen Sie ein Ereignis aus, und klicken Sie anschließend auf .

Entfernen von Ereignissen aus Geräten

- 1 Wählen Sie auf der Registerkarte "Ereignis-Manager" das Kontrollkästchen neben der IP-Adresse des Geräts aus.
- 2 Klicken Sie bei Bedarf auf **Ereignisse**, damit aktive Ereignisse angezeigt werden.
- 3 Wählen Sie ein Ereignis aus, und klicken Sie anschließend auf .


Anzeigen von Ereignisdetails

- 1 Suchen Sie auf der Registerkarte "Ereignis-Manager" mit Lesezeichen oder der erweiterten Suche ein Gerät.
Hinweis: Mit den Kategorien im Bereich "Zusammenfassung Suchergebnisse" können Sie die Liste der gefundenen Geräte eingrenzen.
- 2 Wählen Sie im Bereich "Suchergebnisse" das Kontrollkästchen neben der IP-Adresse eines Geräts aus.
Hinweis: Wenn Sie die IP-Adresse des Geräts nicht kennen, suchen Sie das Gerät in der Spalte "Systemname".
- 3 Klicken Sie auf **Eigenschaften**.
Ein Dialogfeld wird aufgerufen, das die aktuell aktiven, dem Gerät zugewiesenen Bedingungen und Ereignisdetails anzeigt.

Ausführen weiterer Verwaltungsaufgaben

Herunterladen generischer Dateien

Mit der Anwendung können Sie verschiedene Dateien vom Markvision-Server auf eines oder mehrere Geräte im Netzwerk herunterladen. Damit können verschiedene Dateitypen, einschließlich *universeller Konfigurationsdateien* (UCF), auf die von der Anwendung verwalteten Geräte direkt verteilt werden.


- 1 Klicken Sie im Kopfzeilenbereich auf .
- 2 Wählen Sie aus dem Dropdown-Menü "Mit Druckern" eine Gerätegruppe oder ein verfügbares Lesezeichen aus.
- 3 Klicken Sie auf **Durchsuchen** und navigieren Sie dann zu dem Ordner, in dem die Datei gespeichert ist.
- 4 Wählen Sie die Datei aus, die Sie herunterladen möchten, und klicken Sie auf **Öffnen**.
- 5 Wählen Sie im Dropdown-Menü "Ziel" eine der folgenden Optionen:
 - **Konfiguration (HTTP)**: Download einer Drucker-UCF.
 - **Konfiguration (FTP)**: Download einer Netzwerk-UCF.
 - **Firmware-Aktualisierung**: Download einer Firmware-Aktualisierung für die Geräte.
 - **Druck (FTP)**: Download einer druckbaren Datei über ein FTP-Netzwerk.
 - **Druck (Raw Socket)**: Download einer druckbaren Datei vom Computer.
- 6 Klicken Sie auf **Herunterladen**.

Hinweise:

- Wenn die Druckersperre aktiviert ist, ist die Task "Download generischer Dateien" nicht verfügbar.
- Eine Task "Download generischer Dateien" kann zu einem festgelegten Zeitpunkt oder in regelmäßigen Abständen ausgeführt werden. Weitere Informationen finden Sie unter "Planen von Tasks" auf Seite 56.


Konfigurieren der E-Mail-Einstellungen

Hinweis: Sie müssen die Einstellungen für das Simple Mail Transfer Protocol (SMTP) konfigurieren, damit Markvision E-Mail-Benachrichtigungen für Warnungen oder Fehlermeldungen senden kann.


- 1 Klicken Sie im Kopfzeilenbereich auf das Register  > **E-Mail**.
- 2 Geben Sie die Werte in die entsprechenden Felder ein.
 - **SMTP-Mailserver**: Geben Sie die Mailserverinformationen ein.
 - **Port**: Geben Sie die Port-Nummer des SMTP-Mailservers ein.
 - **Von**: Geben Sie die E-Mail-Adresse des Absenders ein.

- 3 Wenn ein Benutzer sich vor dem Senden der E-Mail anmelden muss, aktivieren Sie das Kontrollkästchen **Anmeldung erforderlich**.
 - a Geben Sie die Anmeldeinformationen und das Passwort ein.
 - b Bestätigen Sie das Passwort durch erneute Eingabe.
- 4 Klicken Sie auf **Anwenden** > **Schließen**.


Konfigurieren von Systemeinstellungen

- 1 Klicken Sie im Kopfzeilenbereich auf die Registerkarte  > **Allgemein**.
- 2 Wählen Sie aus dem Abschnitt "Hostnamen-Quelle" die Quelle des Systems, aus der der Hostname eines Geräts übernommen wird, und klicken Sie dann auf **Anwenden**.
- 3 Legen Sie im Abschnitt "Ereignis-Manager" den Zeitraum fest, nach dem das System sich für Warnungen erneut bei den Geräten registrieren muss, und klicken Sie dann auf **Anwenden**.

Hinzufügen, Bearbeiten oder Löschen von Benutzern im System

- 1 Klicken Sie im Kopfzeilenbereich auf die Registerkarte  > **Benutzer**.
- 2 Führen Sie einen der folgenden Schritte durch:
 - Um einen Benutzer hinzuzufügen, klicken Sie auf **+**.
 - a Geben Sie die erforderlichen Details ein.
 - b Wählen Sie im Abschnitt "Rollen" die Rolle des neuen Benutzers aus, und klicken Sie dann auf **OK**.

Einem Benutzer können einzelne oder mehrere Rollen zugewiesen werden.

 - **Admin**: Der Benutzer kann auf allen Registerkarten auf alle Tasks zugreifen und diese ausführen. Nur Benutzer, denen diese Rolle zugewiesen wurde, verfügen über Administratorrechte, zum Beispiel das Hinzufügen weiterer Benutzer zum System oder die Konfiguration von Systemeinstellungen.
 - **Assets**: Der Benutzer kann nur auf Tasks auf der Registerkarte "Assets" zugreifen und diese ausführen.
 - **Ereignis-Manager**: Der Benutzer kann nur auf Tasks auf der Registerkarte "Ereignis-Manager" zugreifen und diese ausführen.
 - **Richtlinien**: Der Benutzer kann nur auf Tasks auf der Registerkarte "Richtlinien" zugreifen und diese ausführen.
 - **Service Desk**: Der Benutzer kann nur auf Tasks auf der Registerkarte "Service Desk" zugreifen und diese ausführen.
 - Wählen Sie einen vorhandenen Benutzer aus, und klicken Sie dann zum Bearbeiten auf  oder zum Löschen auf **—**.
- 3 Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Hinweis: Drei hintereinander fehlgeschlagene Anmeldeversuche deaktivieren das Benutzerkonto; es kann nur durch einen Administrator wieder aktiviert werden. Wenn jedoch der Benutzer der einzige Benutzer mit Admin-Rolle im System ist, wird das Konto nur ca. fünf Minuten lang deaktiviert.

Aktivieren der LDAP-Serverauthentifizierung


Lightweight Directory Access Protocol (LDAP) ist ein standardbasiertes, plattformübergreifendes, erweiterbares Protokoll, das direkt über TCP/IP ausgeführt und für den Zugriff auf spezielle Datenbanken verwendet wird. Diese Datenbanken werden *Verzeichnisse* genannt.

MarkVision-Administratoren können Benutzer-IDs und Kennwörter mithilfe des firmeneigenen LDAP-Servers authentifizieren. Auf diese Weise benötigen Benutzer keine separaten Anmelde-IDs und Kennwörter ausschließlich für MarkVision.

MarkVision führt zuerst einen Authentifizierungsversuch mit den im System vorhandenen gültigen Anmeldeinformationen der Benutzer durch. Wenn der Benutzer von MarkVision beim ersten Versuch nicht authentifiziert werden kann, wird ein neuer Versuch anhand der auf dem LDAP-Server registrierten Benutzer durchgeführt. Wenn ein Benutzer jedoch sowohl auf dem internen MarkVision-Server als auch auf dem externen LDAP-Verzeichnisserver über denselben Benutzernamen verfügt, verwendet MarkVision die auf dem internen Server gespeicherten Anmeldeinformationen. Dies bedeutet, dass der Benutzer das MarkVision-Kennwort und *nicht* das LDAP-Kennwort verwenden muss.

Eine Voraussetzung dafür ist, dass der LDAP-Server Benutzergruppen enthält, die den unter "Hinzufügen, Bearbeiten oder Löschen von Benutzern im System" auf Seite 49 definierten Rollen entsprechen.

Schritt 1. Konfigurieren der Authentifizierungseinstellungen

- 1 Klicken Sie im Kopfzeilenbereich auf  > Registerkarte **LDAP**.
- 2 Geben Sie im Abschnitt "Authentifizierungsinformationen" die Werte in die entsprechenden Felder ein.
 - **Server:** Geben Sie die IP-Adresse oder den Hostnamen des LDAP-Verzeichnisseservers ein, auf dem die Authentifizierung stattfindet.

Wenn die Kommunikation zwischen MVE-Server und LDAP-Verzeichnisserver verschlüsselt werden soll, verfahren Sie wie folgt:

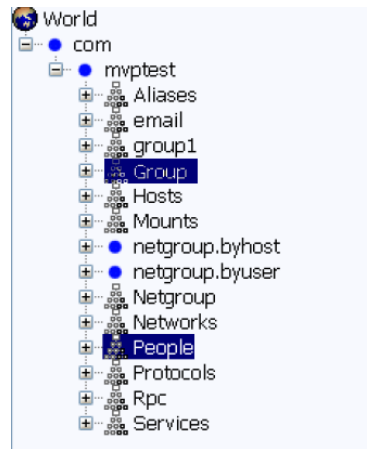
 - a Verwenden Sie den *vollqualifizierten Domänennamen (FQDN)* des Serverhosts.
 - b Öffnen Sie die Datei für den Netzwerkhost und erstellen Sie einen Eintrag, um den Serverhostnamen der zugehörigen IP-Adresse zuzuordnen.

Hinweise:

 - In einem UNIX-/Linux-Betriebssystem befindet sich die Datei für den Netzwerkhost normalerweise unter `/etc/hosts`.
 - In einem Windows-Betriebssystem befindet sich die Datei für den Netzwerkhost normalerweise unter `%SystemRoot%\system32\drivers\etc`.
 - Das TLS (Transport Layer Security)-Protokoll erfordert, dass der Serverhostname dem Namen des im TLS-Zertifikat angegebenen Hosts entspricht, für den das Zertifikat ausgestellt wurde.- **Anschluss:** Geben Sie die Anschlussnummer ein, die vom lokalen Computer zur Kommunikation mit dem LDAP-Community-Server verwendet wird.

Die Standardanschlussnummer lautet 389.

- **Root-DN:** Geben Sie den Basis-DN (definierter Name) des Root-Knotens ein. Dies sollte in der LDAP-Community-Serverhierarchie der direkte Vorgänger des Benutzerknotens und Gruppenknotens sein. In diesem Beispiel würden Sie `dc=mvptest,dc=com` in das Feld "Root-DN" eingeben.

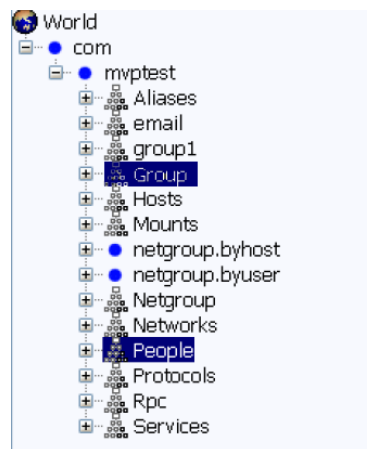


Hinweis: Beachten Sie bei der Angabe des Root-DNs, dass der Ausdruck "Root-DN" ausschließlich `dc` und `o` enthält. Wenn entweder `ou` oder `cn` für den gemeinsamen Vorgänger des Benutzer- und Gruppenknotens angegeben ist, verwenden Sie `ou` oder `cn` in den Ausdrücken "Benutzersuchbasis" und "Gruppensuchbasis".

- 3 Wenn MarkVision geschachtelte *Benutzer* innerhalb des LDAP-Community-Servers suchen soll, wählen Sie **Suche nach geschachtelten Benutzern aktivieren**.

Um die Suchabfrage näher einzugrenzen, geben Sie die Werte in die entsprechenden Felder ein.

- **Benutzersuchbasis:** Geben Sie den Knoten im LDAP-Community-Server ein, in dem das Benutzerobjekt enthalten ist. Dies ist gleichzeitig der Knoten unterhalb des Root-DNs, in dem alle Benutzerknoten aufgeführt sind. In diesem Beispiel würden Sie `ou=people` in das Feld "Benutzersuchbasis" eingeben.

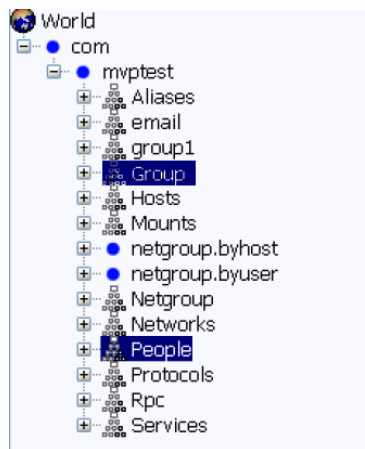


Wenn sich die Benutzer im LDAP-Community-Server auf mehreren hierarchischen Verzeichnisebenen befinden, verfahren Sie wie folgt:

- a Berechnen Sie eine gemeinsame Upstreamhierarchie aller möglichen Speicherorte des Benutzerknotens.
- b Fügen Sie die Konfiguration in das Feld "Benutzersuchbasis" ein.

Hinweis: Alternativ können Sie auch **Suche nach geschachtelten Benutzern aktivieren** aktivieren und das Feld "Benutzersuchbasis" leer lassen. Auf diese Weise wird MarkVision angewiesen, die gesamte LDAP-Struktur beginnend beim Basis-/Root-DN für Benutzer zu durchsuchen.

- **Filter für Benutzersuche:** Geben Sie den Parameter zum Suchen eines Benutzerobjekts im LDAP-Community-Server ein. In diesem Beispiel würden Sie `(uid={0})` in das Feld "Filter für Benutzersuche" eingeben.



Die Funktion "Filter für Benutzersuche" unterstützt die Angabe mehrerer Bedingungen und komplexer Ausdrücke, wie aus der folgenden Tabelle ersichtlich.

Benutzeranmeldung unter Verwendung von	Eingabe im Feld "Filter für Benutzersuche"
Gemeinsamer Name	<code>(CN={0})</code>
Anmeldename	<code>(sAMAccountName={0})</code>
Telefonnummer	<code>(telephoneNumber={0})</code>
Anmeldename oder gemeinsamer Name	<code>((sAMAccountName={0}) (CN={0}))</code>

Hinweise:

- Diese Ausdrücke gelten *ausschließlich* für den LDAP-Server von Windows Active Directory.
- Das einzig gültige Muster für das Feld "Filter für Benutzersuche" lautet `{0}`, wobei MVE nach dem Anmeldenamen des MVE-Benutzers sucht.

4 Wenn MarkVision geschachtelte *Gruppen* innerhalb des LDAP-Community-Servers suchen soll, wählen Sie **Suche nach geschachtelten Gruppen aktivieren**.

Um die Suchabfrage näher einzugrenzen, geben Sie die Werte in die entsprechenden Felder ein.

- **Gruppensuchbasis:** Geben Sie den Knoten im LDAP-Community-Server ein, in dem die den MarkVision-Rollen entsprechenden Benutzergruppen enthalten sind. Dies ist gleichzeitig der Knoten unterhalb des Root-DNs, in dem alle Gruppenknoten (Rollenknoten) aufgeführt sind.

In diesem Beispiel würden Sie **ou=group** in das Feld "Gruppensuchbasis" eingeben.



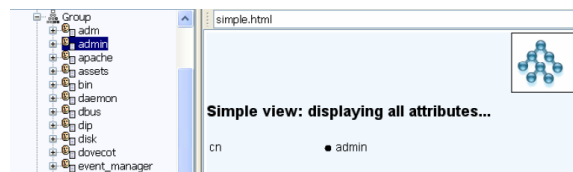
Hinweis: Eine Suchbasis besteht aus mehreren Attributen, wie z. B. cn (gemeinsamer Name), ou (Organisationseinheit), o (Organisation), c (Land) und dc (Domäne), die durch Kommas getrennt sind.

- **Gruppensuchfilter:** Geben Sie den Parameter für die Suche nach einem Benutzer innerhalb einer Gruppe ein, die einer Rolle in MarkVision entspricht.

Hinweis: Abhängig von der Schemakonfiguration Ihres LDAP-Community-Backendservers können Sie die Muster **{0}** und **{1}** verwenden. Bei Verwendung von **{0}** sucht MVE den DN (Distinguished Name, definierten Namen) des LDAP-Benutzers. Der Benutzer-DN wird intern während der Benutzerauthentifizierung abgerufen. Bei Verwendung von **{1}** sucht MVE den Anmeldenamen des MVE-Benutzers.

- **Gruppenrollenattribut:** Geben Sie das Attribut ein, in dem der vollständige Name der Gruppe (Rolle) enthalten ist.

In diesem Beispiel würden Sie **cn** in das Feld "Gruppenrollenattribut" eingeben.



Hinweis: Durch Auswahl von **Suche nach geschachtelten Benutzern aktivieren** und **Suche nach geschachtelten Gruppen aktivieren** wird die Suchtiefe für den LDAP-Community-Server angegeben. Standardmäßig erfolgt die LDAP-Benutzersuche und LDAP-Gruppensuche maximal eine Ebene unter der angegebenen Benutzersuchbasis bzw. Gruppensuchbasis. Daher wird mithilfe der geschachtelten Suche (SubTree) angegeben, dass die festgelegte Benutzersuchbasis und Gruppensuchbasis einschließlich aller Einträge auf allen darunter geschachtelten Ebenen durchsucht werden.

Schritt 2. Konfigurieren der Verbindungseinstellungen

In diesem Abschnitt wird das Protokoll festgelegt, das vom MVE-Server zur Kommunikation mit dem externen LDAP-Verzeichnisserver verwendet wird.

- 1 Klicken Sie auf **Verbindungsinformationen**.

Hinweise:

- Wenn in MarkVision keine LDAP-Konfiguration gespeichert ist, wird automatisch "Anonyme LDAP-Bindung" ausgewählt. Dies bedeutet, dass der MVE-Server weder seine Identität, noch Anmeldeinformationen gegenüber dem LDAP-Server offenlegt, um dessen Suchfunktion zu verwenden. Die Kommunikation während der anschließenden Sitzung für die LDAP-Suche ist vollständig unverschlüsselt.
- Der LDAP-Server von Windows Active Directory unterstützt *keine* Option für anonyme Bindungen.

2 Falls der MVE-Server seine Identität gegenüber dem LDAP-Server offenlegen soll, um dessen Suchfunktion nutzen zu können, konfigurieren Sie die Option "Einfache Verbindung".

- a** Wählen Sie **Einfache Verbindung**.
- b** Geben Sie im Feld "Verbindungs-DN" den Verbindungs-DN (definierter Name) ein.
- c** Geben Sie das Verbindungskennwort ein und bestätigen dann das Kennwort durch erneute Eingabe.

Hinweise:

- Das Verbindungskennwort ist von den Einstellungen für den Verbindungsbenutzer im LDAP-Verzeichnisserver abhängig. Wenn der Verbindungsbenutzer im LDAP als **Nicht leer** festgelegt ist, muss ein Verbindungskennwort angegeben werden. Wenn der Verbindungsbenutzer im LDAP als **Leer** festgelegt ist, muss *kein* Verbindungskennwort angegeben werden. Informationen zu den Einstellungen für den Verbindungsbenutzer im LDAP erhalten Sie bei Ihrem LDAP-Administrator.
- Bei Verwendung der Option "Einfache Verbindung" ist die Kommunikation zwischen MVE und LDAP unverschlüsselt.

3 Wenn die Kommunikation zwischen MVE-Server und LDAP-Verzeichnisserver verschlüsselt werden soll, wählen Sie **Transport Layer Security (TLS)** oder **Kerberos V5 (Windows Active Directory)**.

Wenn Sie **TLS** auswählen, muss sich der MVE-Server unter Verwendung der MVE-Serveridentität (Verbindungs-DN) und der zugehörigen Anmeldeinformationen (Verbindungskennwort) vollständig gegenüber dem LDAP-Verzeichnisserver authentifizieren.

- a** Geben Sie im Feld "Verbindungs-DN" den Verbindungs-DN (definierten Namen) ein.
- b** Geben Sie das Verbindungskennwort ein und bestätigen dann das Kennwort durch erneute Eingabe.

Hinweis: Das Verbindungskennwort ist erforderlich.

Bei selbst signierten Zertifikaten muss der TLS-Fingerabdruck dem systemweiten JVM-Schlüsselspeicher (*Java Virtual Machine*) namens **cacerts** zur Verfügung stehen. Dieser Schlüsselspeicher ist im Ordner "[mve.home]/jre/lib/security" enthalten, wobei "[mve.home]" dem Installationsordner von MarkVision entspricht.

Bei Auswahl von **Kerberos V5 (Windows Active Directory)** verfahren Sie wie folgt:

- a** Geben Sie im Feld für den KDC-Benutzernamen den KDC (Key Distribution Center)-Namen ein.
- b** Geben Sie das KDC-Kennwort ein und bestätigen Sie dann das Kennwort durch erneute Eingabe.
- c** Klicken Sie auf **Durchsuchen** und wechseln Sie dann zu dem Ordner, in dem die Datei *krb5.conf* gespeichert ist.

Hinweise:

- Weitere Informationen zur Kerberos-Konfigurationsdatei finden Sie in der Dokumentation zum Kerberos-Sicherheitsprotokoll.
- Das Kerberos-Sicherheitsprotokoll wird *ausschließlich* in Windows Active Directory mit bestätigter GSS-API-Unterstützung unterstützt.

d Wählen Sie die Datei aus und klicken Sie anschließend auf **Öffnen**.

Schritt 3. Konfigurieren der Einstellungen für Rollenzuordnungen

1 Klicken Sie auf **Rollenzuordnung**.

2 Geben Sie die Werte in die entsprechenden Felder ein.

- **Admin:** Geben Sie die vorhandene Rolle im LDAP ein, die in MVE über Administratorrechte verfügen soll.
- **Bestand:** Geben Sie die vorhandene Rolle im LDAP ein, mit der das Bestandsmodul in MVE verwaltet wird.
- **Richtlinien:** Geben Sie die vorhandene Rolle im LDAP ein, mit der das Richtlinienmodul in MVE verwaltet wird.
- **Service Desk:** Geben Sie die vorhandene Rolle im LDAP ein, mit der das Service Desk-Modul in MVE verwaltet wird.
- **Ereignis-Manager:** Geben Sie die vorhandene Rolle im LDAP ein, mit der das Ereignis-Manager-Modul in MVE verwaltet wird.

Hinweise:

- MVE ordnet die angegebene LDAP-Gruppe (Rolle) automatisch der entsprechenden MVE-Rolle zu.
- Sie können eine LDAP-Gruppe mehreren MVE-Rollen zuordnen und dürfen in ein Feld "MVE-Rolle" auch mehr als eine LDAP-Gruppe eingeben.
- Verwenden Sie bei der Eingabe mehrerer LDAP-Gruppen in die Rollenfelder einen senkrechten Strich (|), um mehrere LDAP-Gruppen voneinander zu trennen. Wenn Sie beispielsweise die Gruppe **admin** und **assets** in die Admin-Rolle einschließen möchten, geben Sie **admin | assets** in das Feld "Admin" ein.

3 Die Felder für *nicht* verwendete MVE-Rollen können leer gelassen werden.

Hinweis: Dies gilt für alle anderen Rollen *außer* der Admin-Rolle.

4 Klicken Sie zum Überprüfen der Konfiguration auf **LDAP testen**.


5 Geben Sie Ihren LDAP-Benutzernamen und Ihr Kennwort ein und klicken Sie auf **Testanmeldung**.

Das Dialogfeld "Ergebnisse des LDAP-Konfigurationstests" wird angezeigt. Falls Fehler auftreten, gehen Sie wie folgt vor:

- a Lesen Sie die Informationen im Dialogfeld, um die Fehlerursache zu ermitteln.
- b Aktualisieren Sie die Einträge, die Sie auf den Registerkarten "Authentifizierungsinformationen", "Verbindungsinformationen" und "Rollenzuordnung" vorgenommen haben.
- c Wiederholen Sie Schritt 4 bis Schritt 5, bis im Dialogfeld "Ergebnisse des LDAP-Konfigurationstests" keine weiteren Fehler angezeigt werden.

6 Klicken Sie auf **Anwenden >Schließen**.

Generieren von Berichten

1 Klicken Sie im Kopfzeilenbereich auf .


2 Wählen Sie aus dem Dropdown-Menü "Mit Druckern" eine auf früheren Lesezeichensuchen basierende Gerätegruppe aus.

3 Wählen Sie aus dem Dropdown-Menü "Berichtstyp" den Datentyp aus, den Sie anzeigen möchten.

Auswählen	Zum Anzeigen von
Lebenszyklus – Zusammenfassung	Ein zusammenfassender Bericht über die Lebenszyklen der Geräte.
Druckerhersteller – Zusammenfassung	Ein zusammenfassender Bericht der Gerätehersteller.
Druckermodell – Zusammenfassung	Ein zusammenfassender Bericht der Gerätemodell-Namen und -Nummern.
Druckerfunktionen	Eine Tabelle mit Gerätefunktionen.
Druckerfunktionen – Zusammenfassung	Ein zusammenfassender Bericht der Gerätefunktionen.
Lebenszyklus	Eine Tabelle mit den Lebenszyklen von Geräten.
Insgesamt gedruckte Seiten	Eine Tabelle mit den insgesamt gedruckten Seiten von Geräten.
Wartungszähler	Eine Tabelle mit Wartungszählern der Geräte.
Firmwareversionen	Eine Tabelle mit den Firmware-Versionen der Geräte.
eSF Solutions	Eine Tabelle mit den verschiedenen in den Geräten installierten eSF-Lösungen (Embedded Server Framework).
Statistiken:Jobs nach gedruckten Seiten	Eine Tabelle mit der Anzahl der von den Geräten ausgeführten Druckjobs.
Statistiken:Jobs nach Medienseiten/Anzahl	Eine Tabelle mit der Anzahl der von den Geräten ausgeführten Einzüge von Druck-, Fax- und Kopierjobs.
Statistiken:Jobs nach Scannerverwendung	Eine Tabelle mit der Anzahl der von den Geräten ausgeführten Scanjobs.
Statistiken:Jobs nach Faxverwendung	Eine Tabelle mit der Anzahl der von den Geräten ausgeführten Faxjobs.
Statistiken:Jobs nach Materialinformationen	Eine Tabelle mit wichtigen Details zu den einzelnen Verbrauchsmaterialien in den Geräten.


- 4 Wählen Sie aus dem Dropdown-Menü "Berichtformat" **PDF** oder **CSV**.
- 5 Wenn Sie "PDF" ausgewählt haben, können Sie im Feld "Titel" den Titel des Berichts anpassen.
- 6 Sie können ggf. aus dem Dropdown-Menü "Gruppe" eine Gruppe auswählen.
- 7 Klicken Sie auf **Generiere (Generieren)**.

Planen von Tasks

- 1 Klicken Sie im Kopfzeilenbereich auf .
- 2 Führen Sie im Dropdown-Menü "Hinzufügen" einen der folgenden Schritte aus:
 - Wählen Sie **Prüfen** und wählen Sie dann eine Gerätegruppe aus.
 - Wählen Sie **Suche** und wählen Sie dann ein Suchprofil aus.
 - Wählen Sie **Übereinstimmung** und wählen Sie dann eine Gerätegruppe und einen Richtlinientyp aus.
 - Wählen Sie **Durchsetzung** und wählen Sie dann eine Gerätegruppe und einen Richtlinientyp aus.
 - Wählen Sie **Download generischer Dateien** und wählen Sie dann eine Gerätegruppe, eine Datei und ein Ziel aus. Diese Option kann nur von Benutzern mit der Admin-Rolle verwendet werden.
- 3 Klicken Sie auf **Weiter**.

- 4 Geben Sie im Feld "Name" den Namen des neuen geplanten Ereignisses ein.
- 5 Nehmen Sie Ihre Einstellungen vor und klicken Sie anschließend auf **Fertig stellen**.

Anzeigen des Systemprotokolls

- 1 Klicken Sie im Kopfzeilenbereich auf .
- Standardmäßig wird die letzte Aktivität in der Datenbank zuerst aufgeführt.
- 2 So werden Aktivitäten nach Kategorien sortiert angezeigt:
 - a Klicken Sie auf **Filter**.
 - b Wählen Sie aus dem Abschnitt "Zeitraum" das Start- und Enddatum aus.
 - c Geben Sie im Feld "ID(s)" die ID-Nummern der Task ein.
Hinweis: Die Eingabe in diesem Feld ist optional.
 - d Deaktivieren Sie im Abschnitt "Task-Name" das Kontrollkästchen neben der nicht in das Protokoll einzufügenden Task.
 - e Deaktivieren Sie im Abschnitt "Kategorien" das Kontrollkästchen neben der nicht in das Protokoll einzufügenden Kategorie.
 - f Klicken Sie auf **OK**.
- 3 Klicken Sie auf **Vorbereiten für Export > Export abschließen**.
- 4 Navigieren Sie im Dropdown-Menü "Speichern unter" zu dem Ordner, in dem Sie die Protokolldatei speichern möchten.
- 5 Geben Sie im Feld "Dateiname" den Namen der Datei ein, und klicken Sie dann auf **Speichern**.
- 6 Navigieren Sie zu dem Ordner, in dem die Protokolldatei gespeichert ist, und öffnen Sie diese, um das Systemprotokoll anzuzeigen.

Häufig gestellte Fragen

Welche Geräte unterstützt die Anwendung?

Eine vollständige Liste der unterstützten Geräte finden Sie in den Versionshinweisen.

Wie ändere ich mein Passwort?

Klicken Sie im Kopfzeilenbereich auf **Password ändern**, und befolgen Sie dann die Anweisungen auf dem Computerbildschirm.

Warum kann ich im Dialogfeld "Erstellen einer neuen Richtlinie" in der Liste "Unterstützte Modelle" nicht mehrere Geräte auswählen?

Konfigurationseinstellungen und Befehle sind für die Modelle unterschiedlich. Ein Einstellungsbefehl, der bei einem Modell funktioniert, funktioniert möglicherweise bei einem anderen Modell nicht. Richtlinien beschränken sich auf jeweils ein Modell, um die Möglichkeit einer nicht ordnungsgemäß funktionierenden Richtlinie auszuschalten.

Am besten vermeidet man die Erstellung nicht effektiver Richtlinien, indem man zuerst eine neue Richtlinie erstellt und dann die neu erstellte Richtlinie mehreren Geräten zuweist.

Können andere Benutzer auf meine Lesezeichen zugreifen?

Ja. Lesezeichen sind global und können von jedem Benutzer gesehen und verwaltet werden.

Wo befinden sich die Protokolldateien?

Die folgenden Protokolldateien des Installationsprogramms befinden sich in diesem Verzeichnis: %TEMP%\

- *mve-*.log*
- **.isf*

Die Anwendungsprotokolldateien befinden sich in folgendem Verzeichnis:



<INSTALL_DIR>\tomcat\logs, wobei <INSTALL_DIR> dem Installationsordner von Markvision entspricht.

Dateien in diesem Verzeichnis, die das Format **.log* aufweisen, sind Anwendungsprotokolldateien.

Fehlerbehebung

Benutzer hat das Passwort vergessen

Sie benötigen zur Rücksetzung des Passworts Administratorrechte.

- 1 Klicken Sie im Kopfzeilenbereich auf .
- 2 Wählen Sie auf der Registerkarte "Benutzer" einen Benutzer aus, und klicken Sie dann auf .
- 3 Ändern Sie das Passwort.
- 4 Klicken Sie auf **OK** und anschließend auf **Schließen**.
- 5 Bitten Sie den Benutzer, sich erneut anzumelden.

Die Anwendung kann das Netzwerkgerät nicht finden

ALLE DRUCKERVERBINDUNGEN ÜBERPRÜFEN

- Stellen Sie sicher, dass das Netzkabel sicher an den Drucker und eine ordnungsgemäß geerdete Netzsteckdose angeschlossen ist.
- Überprüfen Sie, ob der Drucker eingeschaltet ist.
- Überprüfen Sie, ob andere elektrische Geräte funktionieren, die an diese Steckdose angeschlossen werden.
- Stellen Sie sicher, dass das LAN-Kabel mit dem Druckserver und den LAN verbunden ist.
- Vergewissern Sie sich, dass das LAN-Kabel ordnungsgemäß funktioniert.
- Starten Sie den Drucker und den Druckserver neu.

SICHERSTELLEN, DASS DER INTERNE DRUCKSERVER RICHTIG INSTALLIERT UND AKTIVIERT IST

- Drucken Sie eine Einrichtungsseite für den Drucker. Der Druckserver sollte auf der Einrichtungsseite in der Liste der Optionen aufgeführt werden.
- Vergewissern Sie sich, dass das TCP/IP-Protokoll auf dem Druckserver aktiviert ist. Dies ist Voraussetzung für die ordnungsgemäße Funktion des Druckservers und der Anwendung. Sie können diese Überprüfung von der Bedienerkonsole des Druckers aus vornehmen.
- Weitere Informationen finden Sie in der Dokumentation zum Druckserver.

VERGEWISSEN SIE SICH, DASS DER GERÄTENAME IN DER ANWENDUNG MIT DEM IM DRUCKSERVER EINGESTELLTEN NAMEN ÜBEREINSTIMMT.

- 1 Überprüfen Sie den in der Anwendung eingestellten Gerätenamen.
Sehen Sie im Bereich "Suchergebnisse" nach, wie die IP-Adresse des Druckers lautet.
Der Name des Geräts wird neben seiner IP-Adresse angezeigt. Hierbei handelt es sich um den Gerätenamen der Anwendung, *nicht* um den Gerätenamen des Druckservers.
- 2 Überprüfen Sie den im Druckserver eingestellten Gerätenamen. Weitere Informationen finden Sie in der Dokumentation zum Druckserver.

STELLEN SIE SICHER, DASS DER DRUCKSERVER IM NETZWERK KOMMUNIZIERT

- 1 Senden Sie einen Ping-Befehl an den Druckserver.
- 2 Wenn der PING-Test erfolgreich ist, überprüfen Sie, ob IP-Adresse, Netzmaske und Gateway des Druckservers korrekt sind.
- 3 Schalten Sie den Drucker aus, und führen Sie den PING-Test erneut aus, um nach doppelten IP-Adressen zu suchen.
Wenn der PING-Test nicht erfolgreich ist, drucken Sie eine Einrichtungsseite und überprüfen, ob die IP aktiviert ist.
- 4 Wenn TCP/IP aktiviert ist, überprüfen Sie, ob IP-Adresse, Netzmaske und Gateway korrekt sind.
- 5 Vergewissern Sie sich, dass Brücken und Router ordnungsgemäß funktionieren und konfiguriert sind.
- 6 Vergewissern Sie sich, dass alle physischen Verbindungen zwischen Druckserver, Drucker und Netzwerk funktionieren.

Geräteinformationen sind falsch

Wenn die Anwendung offensichtlich falsche Geräteinformationen anzeigt, führen Sie eine Geräteprüfung durch.

Anhang

Lexmark Drucker, die die Sicherheitsrichtlinie unterstützen

Lexmark C520*	Lexmark E460	Lexmark T640*	Lexmark W840*	Lexmark X463	Lexmark X790
Lexmark C522*	Lexmark E462	Lexmark T642*	Lexmark W850	Lexmark X464	Lexmark X850*
Lexmark C524*		Lexmark T644*		Lexmark X466	Lexmark X852*
Lexmark C530*		Lexmark T650		Lexmark X548	Lexmark X854*
Lexmark C532*		Lexmark T652		Lexmark X642*	Lexmark X860
Lexmark C534*		Lexmark T654		Lexmark X650	Lexmark X862
Lexmark C734				Lexmark X651	Lexmark X864
Lexmark C736				Lexmark X652	Lexmark X925
Lexmark C770*				Lexmark X654	Lexmark X940*
Lexmark C772*				Lexmark X656	Lexmark X945*
Lexmark C780*				Lexmark X658	Lexmark X950
Lexmark C782*				Lexmark X734	Lexmark X952
Lexmark C792				Lexmark X736	Lexmark X954
Lexmark C920*				Lexmark X738	
Lexmark C925					
Lexmark C930*					
Lexmark C935*					
Lexmark C950					
Lexmark Pro5500 Series*					
Lexmark Pro710 Series*					
Lexmark Pro910 Series*					
Lexmark Pro4000 Series*					

* Diese Geräte bieten keine Unterstützung für:

- Abschnitte "Zugriffssteuerungen", "Sicherheitsvorlagen" und "Verschiedene Einstellungen" der Sicherheitsrichtlinieneinstellungen
- Remote-Verwaltungs-Zugriffssteuerung von Embedded Web Server
- Kommunikations-Anmeldeinformationen "Benutzername", "Bereich" und "PIN"

Glossar der Sicherheitsbegriffe

Authentifizierung	Eine Methode zur sicheren Identifizierung eines Benutzers.
Autorisierung	Eine Methode, mit der angegeben wird, welche Funktionen für einen Benutzer verfügbar sind, beispielsweise welche Aktionen er ausführen darf.
Baustein	Im Embedded Web Server verwendete Authentifizierungs- und Autorisierungstools. Sie umfassen: Kennwort, PIN, interne Konten, LDAP, LDAP +GSSAPI, Kerberos 5 und NTLM.
Gruppe	Ein Kreis von Benutzern, die die gleichen Merkmale aufweisen.
Sicherheitsvorlage	Ein im Embedded Web Server erstelltes und gespeichertes Profil, das zusammen mit Zugriffssteuerungen zur Verwaltung von Gerätefunktionen verwendet wird.
Zugriffssteuerungen	Einstellungen, durch die gesteuert wird, ob und für wen einzelne Gerätemenüs, -funktionen und -einstellungen verfügbar sind. Wird bei einigen Geräten auch als Funktionszugriffskontrolle bezeichnet.

Index

A

Aktivieren der LDAP-
Serverauthentifizierung 50
Aktualisieren auf die neueste
Version von MarkVision 9
Allgemein (Registerkarte)
verwenden 49
Anschlüsse
Grundlagen 15
Anwendungsprotokolldateien
suchen 58
Anzeigen der eingebetteten
Webseite 44
Anzeigen des Systemprotokolls 57
Anzeigen eines Geräts von einem
entfernten Standort aus 44
Anzeigen von Ereignisdetails 47
Anzeigen von
Geräteigenschaften 23

Ä

Ändern von Kennwörtern 58

B

Bausteine
aus eSF-Anwendung
verwenden 34
Bearbeiten einer Richtlinie 41
Bearbeiten eines Benutzers 49
Bearbeiten eines Ereignisses 46
Bearbeiten eines Suchprofils 20
Bearbeiten eines Ziels 45
Benutzer
bearbeiten 49
hinzufügen 49
löschen 49
Berichte
generieren 55
Bestand (Registerkarte)
verwenden 12

C

Computer-RAM 8

D

Dateien
herunterladen 48

Datenbankserver
unterstützte 8
Druckerstatus 43
Durchsetzen einer Richtlinie 42
Durchsetzen von Richtlinien 43

E

Eigenschaften, Gerät
anzeigen 23
Eingebettete Webseite
anzeigen 44
Eingeschränkte Geräte
Sicherheitsrichtlinie klonen 35
Eingeschränktes Gerät
Kommunikations-
Anmeldeinformationen
ändern 40
E-Mail
Einstellungen konfigurieren 48
Empfangen von
Gerätewarnungen 49
Entfernen einer Richtlinie 42
Entfernen eines Ereignisses von
einem Gerät 47
Entfernen eines zugewiesenen
Schlüsselworts von einem Gerät 29
Ereignis
bearbeiten 46
Details anzeigen 47
erstellen 46
löschen 46
von einem Gerät entfernen 47
Ereignis-Manager (Registerkarte)
verwenden 12
Erstellen einer neuen Richtlinie 30
Erstellen einer Richtlinie von einem
Gerät 31
Erstellen eines Ereignisses 46
Erstellen eines Suchprofils 18
Erstellen von Lesezeichen 27
Erste Schritte
Startbildschirm 14
Erweiterte Suche, verwenden 24

F

Fehlerbehebung
Benutzerkennwort
zurücksetzen 59

fehlerhafte
Geräteinformationen 60
Netzwerkgerät wird nicht
gefunden 59
Fehlerhafte
Geräteinformationen 60
Firebird-Datenbank
sichern 9
wiederherstellen 10

G

Generieren von Berichten 55
Gerät
aus einer Datei importieren 20
Eigenschaften anzeigen 23
Ereignisdetails anzeigen 47
Ereignis entfernen 47
Ereignis zuweisen 47
prüfen 22
Schlüsselwörter zuweisen 28
Status überprüfen 43
von einem entfernten Standort
aus anzeigen 44
zugewiesenes Schlüsselwort
entfernen 29
Gerät, Hostname
abrufen 49
Gerät, Warnungen
empfangen 49
Geräte
suchen 18
suchen nach 24
Geräte, gesichert
Grundlagen 32
Gerätstatus
überprüfen 43
Grundlagen zu Anschlüssen 15
Grundlagen zu gesicherten
Geräten 32
Grundlagen zum Startbildschirm 14
Grundlagen zu Protokollen 15

H

Herunterladen generischer
Dateien 48
Hinweise 2
Hinzufügen eines Benutzers 49

- I**
Importieren von Geräten aus einer Datei 20
Installationsprogramm, Protokolldateien suchen 58
- K**
Kategorien
bearbeiten 28
hinzufügen 28
löschen 28
verwenden 27
Kennwort, Benutzer zurücksetzen 59
Kommunikations-Anmeldeinformationen ändern 40
Konfigurieren von E-Mail-Einstellungen 48
Konfigurieren von Systemeinstellungen 49
Kopfzeilenbereich 14
- L**
LDAP-Server
Authentifizierung aktivieren 50
Lesezeichen
erstellen 27
löschen 27
zugreifen auf 27
Lesezeichen und erweiterte Suche (Bereich) 14
Löschen einer Richtlinie 41
Löschen eines Benutzers 49
Löschen eines Ereignisses 46
Löschen eines Suchprofils 20
Löschen eines Ziels 45
Löschen von Lesezeichen 27
- M**
MarkVision
installieren 8
verwenden 12
zugreifen auf 10
MarkVision Enterprise auf die neueste Version aktualisieren 9
Definition 7
- MarkVision Professional zu MarkVision Enterprise migrieren 11
Migrieren von MarkVision Professional zu MarkVision Enterprise 11
MVE migrieren zu 11
MVP
in MarkVision Enterprise importieren 11
zu MarkVision Enterprise migrieren 11
- N**
Netzwerkgerät wird nicht gefunden 59
- P**
Planen von Tasks 56
Platzhalter 45
Protokolldateien suchen 58
Protokolle
Grundlagen 15
Prozessorgeschwindigkeit 8
Prüfen eines Geräts 22
- R**
Richtlinie
bearbeiten 41
durchsetzen 42
entfernen 42
erstellen 30
löschen 41
Typen 30
Übereinstimmung überprüfen 41
von einem Gerät erstellen 31
zuweisen 41
Richtlinien
durchsetzen 43
Übereinstimmung des Geräts überprüfen 43
verwalten 30
Richtlinien (Registerkarte) verwenden 12
- S**
Schlüsselwörter
bearbeiten 28
hinzufügen 28
- löschen 28
verwenden 27
von einem Gerät entfernen 29
zu Gerät zuweisen 28
Service Desk (Registerkarte) verwenden 12
Sicherheitsrichtlinie
Einstellungen anpassen 34
unterstützte Lexmark Drucker 61
zum Aufheben von Geräteeinschränkungen klonen 37
zur Einschränkung von Geräten klonen 35
Sichern einer Firebird-Datenbank 9
Standardlesezeichen, verwenden 24
Startbildschirm
Grundlagen 14
Status des Gerätelebenszyklus festlegen 21
Nicht verwaltet 21
Stillgelegt 21
Verwaltet 21
Verwaltet (fehlt) 21
Verwaltet (geändert) 21
Verwaltet (gefunden) 21
Verwaltet (normal) 21
Suchen nach Geräten 24
Suchen von Geräten 18
Suchergebnisse (Bereich) 14
Suchprofil
bearbeiten 20
erstellen 18
löschen 20
Systemeinstellungen konfigurieren 49
Systemnamen überprüfen 59
Systemprotokoll anzeigen 57
Systemvoraussetzungen
Bildschirmauflösung 8
Prozessorgeschwindigkeit 8
RAM 8
Speicherplatz auf Computerfestplatte 8
- T**
Taskinformationen (Bereich) 14
Tasks
planen 56

U

- Uneingeschränkte Geräte
 - Sicherheitsrichtlinie klonen 37
- Unterstützte Datenbankserver 8
- Unterstützte Geräte 58
- Unterstützte Modelle (Liste) 58

Ü

- Überprüfen der Geräteübereinstimmung mit Richtlinien 43
- Überprüfen der Übereinstimmung mit einer Richtlinie 41
- Überprüfen des Gerätestatus 43
- Übersicht 7

V

- Verbrauchsmaterialstatus 43
- Vergessenes Benutzerkennwort 59
- Verwenden von Kategorien 27
- Verwenden von Schlüsselwörtern 27

W

- Wiederherstellen einer Firebird-Datenbank 10

Z

- Ziel
 - bearbeiten 45
 - erstellen 45
 - löschen 45
- Zurücksetzen des Benutzerkennworts 59
- Zusammenfassung Suchergebnisse (Bereich) 14
- Zuweisen einer Richtlinie 41
- Zuweisen eines Ereignisses zu einem Gerät 47
- Zuweisen von Schlüsselwörtern zu einem Gerät 28