



# cynapspro Endpoint Data Protection

Step-By-Step  
Anleitung



# cynapro Endpoint Data Protection



Alle Rechte vorbehalten, 2004 – 2011 cynapro GmbH. Diese Dokumentation ist urheberrechtlich geschützt. Alle Rechte liegen bei der cynapro GmbH. Jede andere Nutzung, insbesondere die Weitergabe an Dritte, Speicherung innerhalb eines Datensystems, Verbreitung, Bearbeitung, Vortrag, Aufführung und Vorführung ist untersagt. Dies gilt sowohl für das gesamte Dokument, als auch Teile davon.

Änderungen vorbehalten. Die in dieser Dokumentation beschriebene Software unterliegt einer permanenten Weiterentwicklung. Aufgrund dessen kann es zu Unterschieden in der Dokumentation und der tatsächlichen Software kommen.

Cynapro devicepro® sind eingetragene Markenzeichen der cynapro GmbH. Alle verwendeten Produktnamen und Warenzeichen sind Eigentum ihres jeweiligen Besitzers.



cynapro GmbH  
Pforzheimer Str. 134  
76275 Ettlingen  
Germany

Tel. +49 (0)7243 35 495 0  
Fax. +49 (0) 7243 35 495 10  
eMail: [contact@cynapro.com](mailto:contact@cynapro.com)

## Inhaltsverzeichnis

- Hinweis zur Step-By-Step Anleitung
- Vorwort
- Installation des DevicePro Servers
- Erste Schritte nach der Installation
- Informationen zu Geräteklassen
- Aktivierung der Module / Zugriffsrechte
- Priorisierung von Zugriffsrechten
  - Computer-/Benutzerrechte
  - Ports/Geräteklassen
  - Gerätefreigaben
- Nutzung der Geraetefreigabe
- Aktivierung der Protokollierung (optional)
- Verwendung des ShadowCopy Verfahrens (optional)
- Eingrenzen von Zugriffen auf Dateien oder Dateitypen (optional)
- Inbetriebnahme von CryptionPro

## Hinweis zur Step-By-Step Anleitung

Dieses Dokument soll Ihnen eine Schritt für Schritt Unterstützung zur Erstinstallation und Inbetriebnahme der cynapspro Endpoint Data Protection bieten. Sie erhalten die Möglichkeit in kürzester Zeit eine Vielzahl an Funktionen dieser Endpoint Protection Lösung kennenzulernen und einzurichten.

Die Lösungen ApplicationPro, CryptionPro, CryptionPro HDD, DevicePro, ErasePro und PowerPro bieten weit mehr Funktionen als in dieser Step-By-Step Anleitung erwähnt. Jedoch sind viele Funktionen optional und werden daher im Bedienungsleitfaden (<http://handbuch.cynapspro.com>) oder Installationsleitfaden (<http://installation.cynapspro.com>) genauer erläutert.

Ziel dieses Dokumentes ist Ihnen eine Art Best Practices Guide bzw. ein How-To zu bieten.

## Vorwort

Die Software Lösungen des deutschen IT Security Hersteller cynapspro erhalten seit mehr als fünf Jahren ein stets positives Feedback der Kunden, Partner, Presse und IT Spezialisten. Gründe hierfür sind unter anderem die Vorreiterfunktion der Verwendung neuer und innovativer Technologien, welche nun auch bei anderen Herstellern immer mehr zum Einsatz gebracht werden.

Die sichere Kerneltreibertechnologie der Produkte rund um DevicePro und CryptionPro bietet u.a. die Vorteile, dass bei Mitarbeiter die Akzeptanz einer eingeführten DLP Lösung höher ist, als bei Lösungen mit Group Policy Technologie. Gegenüber GPO's bietet die cynapspro Kerneltreibertechnologie eine deutlich größere Sicherheit, höhere Stabilität und ein schnelleres Wirken von Änderungen auf Zugriffsrechten. Der Mitarbeiter muss im Gegensatz zu Group Policies keine Kommandozeilenbefehle ausführen oder gar den Rechner neu starten.

Bestätigt der Administrator bei den Produkten von cynapspro eine Rechteänderung, ist dies sofort dank des intelligenten Push/Pull Verfahrens am Client wirksam. Benötigt der Mitarbeiter schnellst möglich eine Zugriffsänderung, so liegen sowohl im online als auch offline Modus keine technischen Hürden im Weg. Dies schafft große Akzeptanz bei den Mitarbeitern. Dank der Technologie des cynapspro Push/Pull Verfahren ist die Netzwerk-, Client- und Serverauslastung stets auf niedrigstem Level.

Neben der innovative Kerneltreiber- und intelligenten Push/Pull-Technologie, welche von Anfang an in DevicePro zum Einsatz kam, steht cynapspro auch für einen weiteren großen Vorsprung gegenüber Mitbewerbern. Die Verschlüsselung von externen Speichermedien setzt nicht auf Container- oder Partitionsverschlüsselung, sondern auf eine transparente, dateibasierte On-The-Fly-Verschlüsselung. Somit werden trotz Verschlüsselung die Mitarbeiter von cynapspro Kunden bei Ihrer täglichen Arbeit mit externen Datenträgern nicht gestört. Die Daten werden beim Schreib- und Kopiervorgang automatisch im Hintergrund ver- und entschlüsselt. An Firmenrechnern ist weder ein Öffnen von Anwendungen noch Eingeben von Passwörtern erforderlich – der Benutzer hat sich nämlich bereits über die Windows Authentifizierung oder bei Einsatz von CryptionPro HDD's PreBoot Authentication dem System erkenntlich gemacht. An ‚nicht Firmenrechnern‘ können berechnete Mitarbeiter mittels der ausführbaren Datei von CryptionPro Mobile und dem dazugehörigen Passwort weitere Daten ver- und entschlüsseln. Für die dateibasierte Verschlüsselungstechnologie von cynapspro sind Sie nicht an spezielle USB Geräte gebunden. Die Daten jedes USB Datenträger können sofort nach der Entnahme aus dessen Verpackung ohne Vorbereitung verschlüsselt werden. Dies minimiert Betriebskosten und freut nicht nur die Finanzabteilungen der Unternehmen, sondern auch Administration und Mitarbeitern.

Weiter bietet die bewährte Technologie von cynapspro eine erhöhte Manipulationssicherheit, so dass die Mitarbeiter auch durch das Beenden des Prozesses oder anderen Programm schädigenden Maßnahmen nicht an unautorisierte Zugriffsrechte kommen können. Weitere Informationen zu den cynapspro Technologien und deren Vorteilen finden Sie unter: <http://cynapspro.com/DE/technische-informationen>.

Auch die ‚Newcomer‘ Produkte wie ErasePro (Datenvernichtung) und PowerPro (Power Management) bieten wie alle Produkte (ApplicationPro, DevicePro, CryptionPro und CryptionPro HDD) der cynapspro GmbH schon jetzt große Alleinstellungsmerkmale und hohe Mehrwerte für

Unternehmen jeder Größenordnung (von 1-Mann Unternehmen bis Großkonzernen) und Behörden. Weitere Informationen zu den einzelnen Produkten finden Sie hier: <http://cynapro.com/DE/products>.

Bei der Weiterentwicklung der Produkte setzt die cynapro GmbH nicht nur auf eine außergewöhnlich enge Zusammenarbeit mit seinen Kunden (laut Kundenaussagen), sondern u.a. auch auf Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik), europäischer und deutscher Gesetzesgeber im Bereich IT Security und Revisionsicherheit (z.B. Basel II und SOX). Dank der Innovationen von cynapro besitzen die Produkte bereits heute einen technologischen Vorsprung mehrerer Jahre. (Mit einer zu cynapro annähernden Anpassung der Strategien anderer Hersteller ist bereits für die kommenden Jahre zu rechnen. Nicht nur technologisch, sondern auch in Skalierbarkeit und intuitiver Verwaltbarkeit.)

Informationen zum Unternehmen finden Sie unter <http://cynapro.com/DE/company>.

## Installation des DevicePro Servers

Die Sicherheitslösungen der cynapspro GmbH beinhalten lediglich 2 Komponenten - der DevicePro Server und DevicePro Agent. In diesem Abschnitt erläutern wir die Installation der Serverkomponente.

Bevor Sie mit der Installation von DevicePro Ultimate starten, empfiehlt es sich vorher folgendes vorzubereiten:

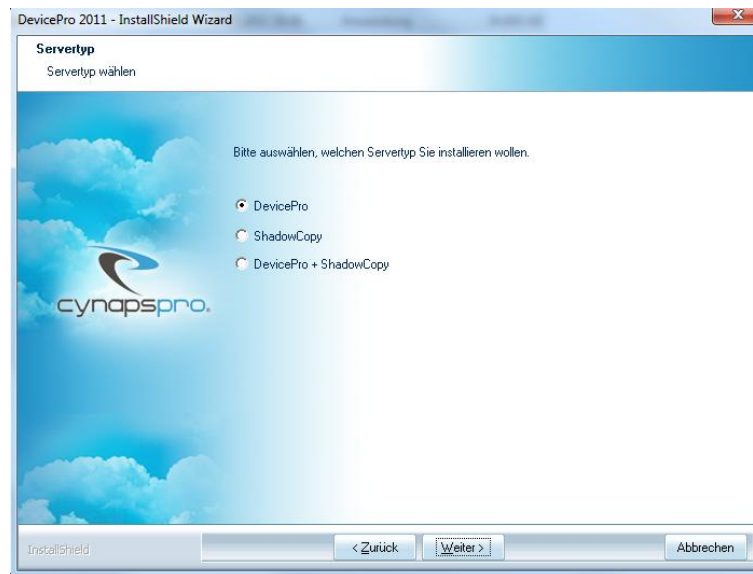
- ✓ DevicePro Installationsdatei
- ✓ Lizenzschlüssel (.lic & .txt) (nicht bei Testinstallation)
- ✓ Mind. 20 MB freier Festplattenspeicher
- ✓ Benutzer mit Leserechte auf Microsoft Active Directory/ Novell eDirectory
- ✓ SQL - Benutzer mit Berechtigung zum Erstellen von Datenbanken (MSDE, SQL Server Express 2005 oder 2008 (+ R2), SQL Server 2000, 2005 oder 2008 (+ R2), bzw. MySQL 5 oder höher)

Um DevicePro nutzen zu können, installieren Sie zuerst die Serverkomponente auf Ihrem späteren DevicePro Server.

Starten Sie hierzu die von uns übergebene Setup Datei. Anschließend öffnet sich die Installationsroutine im InstallShield. Bitte wählen Sie nun die Sprache aus, in der das Setup erfolgen soll. Danach erscheint das Fenster für den Installationsbeginn. Klicken Sie bitte **Weiter**. Wenn Sie mit den Lizenzvereinbarungen einverstanden sind, klicken Sie bitte auf "**Ich akzeptiere die Bedingungen der Lizenzvereinbarung**".

Wenn Sie **Weiter** klicken, wird DevicePro in den vordefinierten Zielordner installiert. Falls Sie ein anderes Verzeichnis für die Installation angeben möchten, können Sie durch Anklicken von **Ändern** den Zielordner selbst bestimmen. Haben Sie den Ordner ausgewählt, klicken Sie auf **Weiter**.

Möchten Sie lediglich DevicePro ohne die ShadowCopy Funktionalität verwenden, können Sie mit der Auswahl **DevicePro** sofort auf **weiter** klicken.



Für den Fall, dass Sie zusätzlich zur Protokollierung von Zugriffen auf externe Speichermedien noch die 1zu1 Ablage von Schattenkopien möchten, haben Sie folgende Auswahlmöglichkeiten:

- Getrennte Serverinstallationen
  - o Ein *DevicePro* Server zur Verwaltung
  - o Ein zweiter *ShadowCopy* Server zur Ablage von Schattenkopien
- Gemeinsame Serverinstallation
  - o Mit der Option *DevicePro + ShadowCopy* befinden sich der Verwaltungs- und ShadowCopy Ablage Server auf einem System

Geben Sie bitte nun folgende Ports ein:

*Client-Server XmlRpcPort* (Standard: 6005) wird von den Clients für eine Verbindung zum Server verwendet

*Server-Client Notification XmlRpcPort* (Standard: 6006) dient der Benachrichtigung der Clients

Achtung: Die eingetragenen Ports müssen in Ihrer Firewall freigeschaltet sein!

Bitte wählen Sie im nächsten Schritt den bereits im Einsatz befindlichen Verzeichnisdienst aus und klicken auf Weiter. Als Verzeichnisdienste dürfen Sie *Microsoft Active Directory*, *Novell eDirectory* (4.91 SP2 oder höher) oder das DevicePro *eigene Directory* (z.B. beim Einsatz von Windows Arbeitsgruppen) verwenden.

Möchten Sie später ihr openLDAP auslesen, können Sie erst einmal das *eigene Directory* wählen und später über das AdminTool auf LDAP umstellen.

Im darauf folgenden Fenster werden die Einstellungen für den Verzeichnis-Dienst vorgenommen:

### Active Directory Anmeldungsdaten

Geben Sie den Namen Ihres Domain Controllers ein. Weitere Domaincontroller können später in der Management Konsole hinzugefügt werden. Nun hinterlegen Sie noch den Active Directory Administrator oder einen anderen Benutzer mit mindestens Leserechten und tragen das dazugehörige Passwort ein.

## Novell eDirectory Anmeldungsdaten

Bei NDS Server wird der Name des NDS Servers hinterlegt. Unter Context geben Sie den Context Ihrer Novell Umgebung ein. Tragen Sie den Novell Supervisor als Benutzer und das dazugehörige Passwort ein.

Nach korrekter Eingabe der Anmeldedaten gehen Sie auf **Weiter**. Als nächstes wird der Datenbank-Server konfiguriert. Geben Sie hier bitte den Namen ihres SQL-Servers ein. Mit Durchsuchen haben Sie die Möglichkeit, den verfügbaren Datenbank-Server auszuwählen.

**Achtung:** Wenn Sie die MSDE benutzen, muss der entsprechende Haken gesetzt werden. (siehe auch Vorbereitung der Installation unter MSDE)

Falls Sie keine zuvor angelegte Datenbank für DevicePro auswählen bzw. angeben, wird eine neue Datenbank mit dem Namen „Device\_Pro“ automatisch generiert.

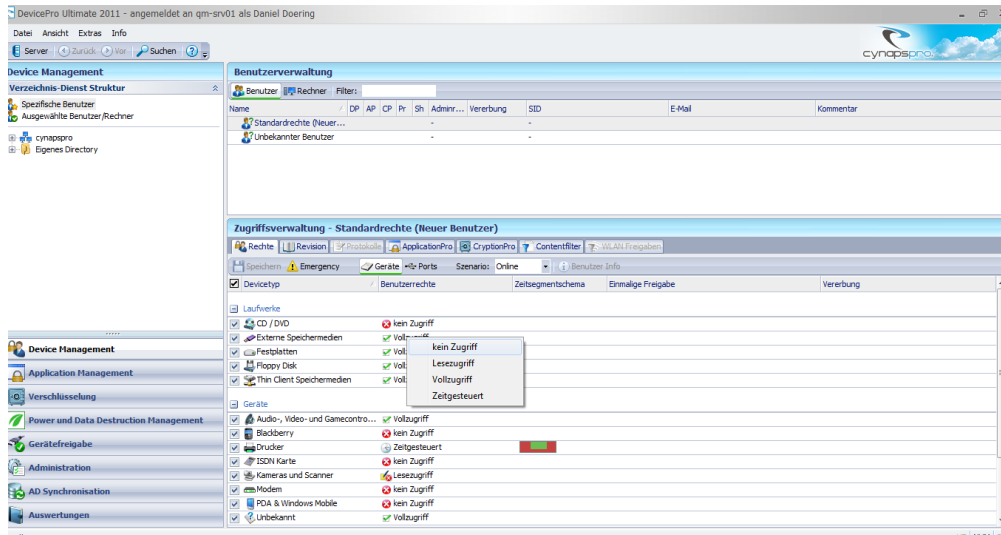
Klicken Sie nun bitte auf SQL Authentifizierung und tragen gegebenenfalls Ihr „sa“ Kennwort ein. Sie können aber auch die Windows-Authentifizierung verwenden. Klicken Sie anschließend auf **Weiter** und **Installieren**. Das InstallShield installiert nun die Serverkomponente von DevicePro. Klicken Sie auf **Fertigstellen**, um den Assistenten zu verlassen.

## Das Supervisor Passwort

Wenn das Supervisor Passwort definiert wurde, haben Sie die Möglichkeit auch ohne Administratorrechte, Einstellungen in der Konsole vorzunehmen. Dazu müssen Sie das Passwort bei der Anmeldung an der MMC eingeben um sich zu Authentifizieren. Dies wäre bei der vorhergehenden Wahl des **eigenen Directory** empfehlenswert.

## Erste Schritte nach der Installation

Nachdem Sie die Installation der Serverkomponente vorgenommen haben, können Sie nun zur Erstkonfiguration übergehen.



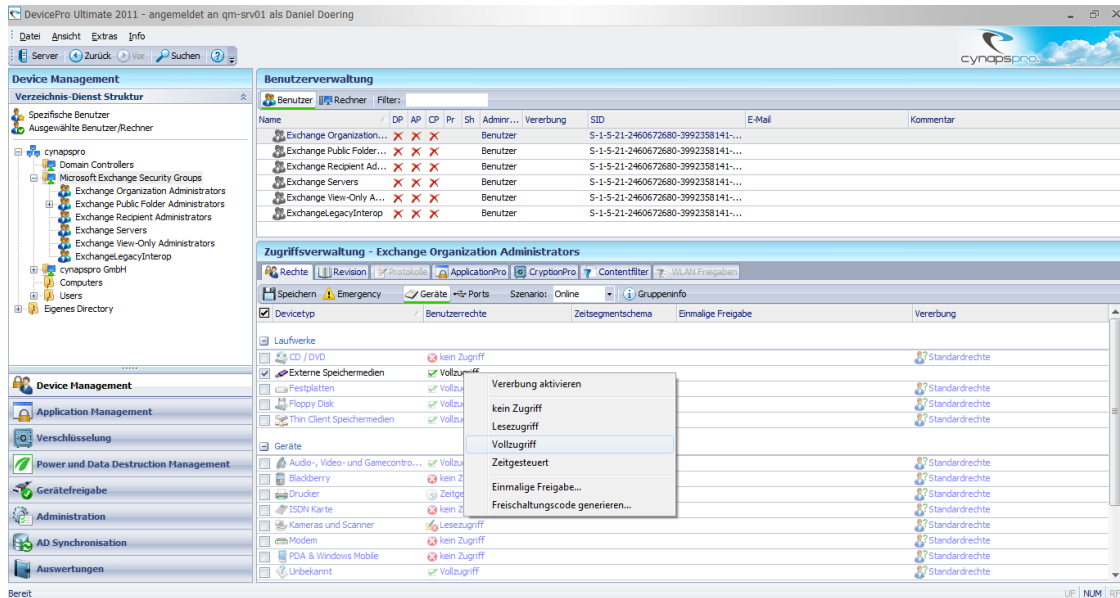
Hierfür befindet sich nun die Verknüpfung zur **DevicePro Management Konsole** auf Ihrem Desktop. Nach dem Aufruf dieser Datei können Sie nun unter **DeviceManagement/spezifische Benutzer** die **Standardrechte** definieren. Diese werden später als Standardkonfiguration für die Reiter **Rechte**, **ApplicationPro**, **CryptionPro** und **Contentfilter** den Benutzern, Gruppen und Computern automatisch zugewiesen.

Nachdem Sie die Standardrechte definiert haben, können Sie den Verzeichnisdienst auslesen. Hierfür klicken Sie entsprechend auf **AD Synchronisation** oder **NDS Synchronisation**. Falls Sie das **eigene Directory** bei der Installation gewählt haben, können Sie diesen Schritt überspringen. Im Fenster der Synchronisation klicken Sie zum Auslesen des Verzeichnisdienstes einfach auf den Button **Start**. Falls Sie weitere Domänen auslesen wollen, können Sie diese unter **Domaincontroller Verwaltung** hinterlegen. Der Scheduler ermöglicht eine automatisierte Synchronisation nach bestimmten Zeitpunkten oder -intervallen.

Der nächste und vorletzte Schritt ist das Erstellen des MSI Paketes für den Clientrollout. Sie finden die Einstellungen dazu unter dem Menüpunkt **Administration/MSI Paket für den Client generieren**. Im Normalfall reicht es aus, dass Sie hier lediglich das **Passwort zur Deinstallation** hinterlegen und anschließend auf den Button **Generieren** klicken. Nun können Sie den Rollout des DevicePro Agenten per Softwareverteilung, Gruppenrichtlinie, manuell oder per DevicePro Management Konsole vornehmen.

Für den Rollout per DevicePro Management Konsole gehen Sie bitte auf den Menüpunkt **Administration/Installation/Update der Agenten**. Vorab klicken Sie nun auf den Reiter **Einstellungen** und hinterlegen hier einen Benutzer mit Domain-Admin Rechten nach dem Schema `username`, `<domaine>\<username>` oder `<username>@<domaine>.<endung>` und dessen Passwort. Nachdem Sie die Gruppenrichtlinie für Remoteverwaltungsausnahmen umgesetzt haben, können Sie im Reiter **Installation/Update** mit dem Rollout des DP-Agenten beginnen. Über die Ansicht **Alle** oder **nur die Rechner ohne Agenten**, sehen Sie die Rechner ohne installierten DevicePro Agent. Diese (Clients) können Sie auswählen und per Button **Install/Update** mit der Clientsoftware ausstatten.

Der letzte Schritt wäre die individuelle Konfiguration von Benutzerrechten. Hierfür können Sie z.B. Ihre Arbeit per Gruppenvererbung erleichtern, indem Sie Sonderberechtigungen auf eine Gruppe gewähren. Hierfür gehen Sie bitte unter **Device Management** auf die jeweilige Gruppe und stellen das Sonderrecht ein. Dies wird den jetzigen und zukünftigen Gruppenmitgliedern nach dem Klicken auf **Speichern** vererbt.



Name	DP	AP	CP	Pr	Sh	Admnr...	Vererbung	SID	E-Mail	Kommentar
Exchange Organization...	X	X	X	X	X	X	Benutzer	S-1-5-21-2460672680-3992358141-...		
Exchange Public Folder...	X	X	X	X	X	X	Benutzer	S-1-5-21-2460672680-3992358141-...		
Exchange Recipient Ad...	X	X	X	X	X	X	Benutzer	S-1-5-21-2460672680-3992358141-...		
Exchange Servers	X	X	X	X	X	X	Benutzer	S-1-5-21-2460672680-3992358141-...		
Exchange View-Only A...	X	X	X	X	X	X	Benutzer	S-1-5-21-2460672680-3992358141-...		
ExchangeLegacyInterop	X	X	X	X	X	X	Benutzer	S-1-5-21-2460672680-3992358141-...		

Natürlich können Sie die Vererbung auf Benutzer- oder Computerebene zu jederzeit deaktivieren (Spalte Vererbung) oder weitere Sonderregelungen auf einzelne Geräteklassen bei Bedarf einstellen.

## Informationen zu Geräteklassen

DevicePro erleichtert Ihnen die Arbeit, da die Geräteklassen eines Rechners bereits vordefiniert sind. Hier sehen Sie entsprechende Beispiele und Erläuterungen zu den Geräteklassen.

- CD/DVD
  - o CD oder DVD Brenner und Laufwerke, virtuelle CD Laufwerke z.B. von U3 Sticks
- Externe Speichermedien
  - o USB Sticks, externe Festplatten, SD/MMC/SM/MS/CF Karten oder Kartenlesegeräte, Wechseldatenträger von z.B. Digitalkameras, eToken oder Smartphones
  - o Massenspeichergeräte per Anschluss an USB, PCMCIA und Firewire
- Festplatten
  - o Über eSATA, SATA, IDE und SCSI angeschlossene physikalische Festplatten (ausgeschlossen ist die Festplatte mit Windows System Volume Drive)
- Floppy Disk
  - o Diskettenlaufwerke
- Thin Client Speichermedien
  - o Netzlaufwerke in Windows Terminal Session, welche durch einen angeschlossenen USB Datenträger am Host-Rechner gemountet wurden.
- Audio-, Video- und Gamecontroller
  - o Soundkarten, Lautsprecher, Headset, Mikrofon
- Blackberry
  - o Synchronisationsfunktion des Blackberry Desktop Manager
- Drucker (Verwaltung benötigt Aktivierung der *Druckerkontrolle* unter *Administration \ Clienteneinstellungen*)
  - o Lokale USB Drucker, Lokale LPT Drucker
- ISDN Karte
  - o ISDN Interneteinwahlgeräte an PCMCIA, USB und Serial Port
- Kameras und Scanner
  - o Digitalkameras, Webcams, Scanner
- Modem
  - o Interne Faxmodem, UMTS Sticks/Karten, eingebaute Modems
- PDA & Windows Mobile
  - o Synchronisationsfunktion von Smartphones z.B. per ActiveSync
- Unbekannt
  - o Anmeldefunktion von eToken und Smartcards, Dongles, USB Verbundgeräte
- Bluetooth
- Infrarot
- TV Tuner
- WiFi (WLAN Freigabe nur mit Aktivierung des *WLAN Kerneltreibers* unter *Administration/MSI Paket für den Client generieren*)

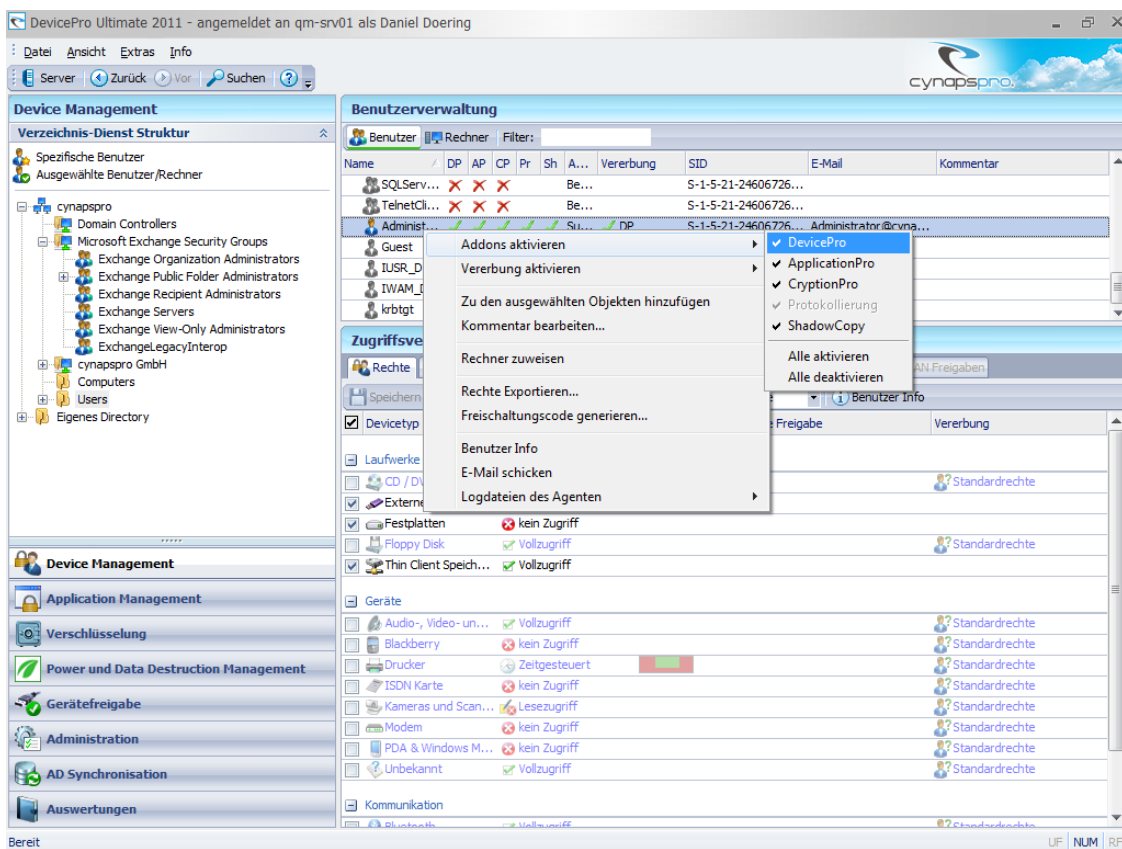
## Aktivierung der Module / Zugriffsrechte

Sie haben bereits schon den DevicePro Agent auf den Rechnern ausgerollt, sowie die Zugriffsrechte definiert.

Damit z.B. bei DevicePro Rechte auf USB Geräte eingeschränkt, bei CryptionPro USB Sticks verschlüsselt oder bei ApplicationPro Anwendungen verwaltet werden können, bedarf es noch der Aktivierung der Benutzer oder Computer.

Hierfür gehen Sie bitte unter **Device Management** mit der rechten Maustaste auf das jeweilige Objekt und sehen dort die Option **Addons aktivieren**.

Nach der Aktivierung von **DevicePro** werden die entsprechenden Einstellungen für den Computer oder Benutzer wirksam. Haben Sie **ApplicationPro** aktiviert, so können Sie mit dem Lernmodus die vom Benutzer ausgeführten Programme aufzeichnen lassen oder nur noch bestimmte Anwendungen freigeben. Ab der Aktivierung von **CryptionPro** werden Datentransfers auf externe Datenträger automatisiert im Hintergrund verschlüsselt.



The screenshot displays the 'Benutzerverwaltung' (User Management) window in DevicePro Ultimate 2011. The left sidebar shows the 'Device Management' tree with categories like 'Spezifische Benutzer', 'Ausgewählte Benutzer/Rechner', and 'Gerätefreigabe'. The main area shows a list of users, with 'Administrator@cynapspro' selected. A context menu is open over this user, showing options to activate various addons. The 'DevicePro' option is checked, while 'ApplicationPro', 'CryptionPro', 'Protokollierung', and 'ShadowCopy' are unchecked. Below the menu, there are sections for 'Zugriffsrechte' (Access Rights) and 'Geräte' (Devices) with checkboxes for different hardware components and their access levels (e.g., 'kein Zugriff', 'Vollzugriff').

## Priorisierung von Zugriffsrechten

Sie haben die Möglichkeit, je nach Szenario unterschiedliche Zugriffsrechte zu vergeben. Hier eine kurze Erläuterung welche Zugriffsrechte sich vorrangig auswirken.

### 1. Computer-/Benutzerrechte

- a. Ist ein Computer in DevicePro aktiviert, greifen stets die Rechte des Computers. Egal, welcher Benutzer sich anmeldet.
- b. Ist ein Computer in DevicePro deaktiviert, so greifen die Rechte des an Windows angemeldeten Benutzers
- c. Sind Benutzer und Computer beide deaktiviert, verhält sich der DevicePro Agent, wie wenn er nicht installiert wäre (alle Rechte bleiben inaktiv)

### 2. Ports/Geräteklassen

- a. Sie können bei Bedarf Ports generell sperren und somit alle an (diesen) Ports wie USB angeschlossenen Geräte verbieten – egal um welche Geräteklasse es sich handelt.
- b. Erlauben Sie jedoch die Verwendung von Ports, so können Sie z.B. USB Geräte je nach Geräteklasse erlauben oder unterbinden.

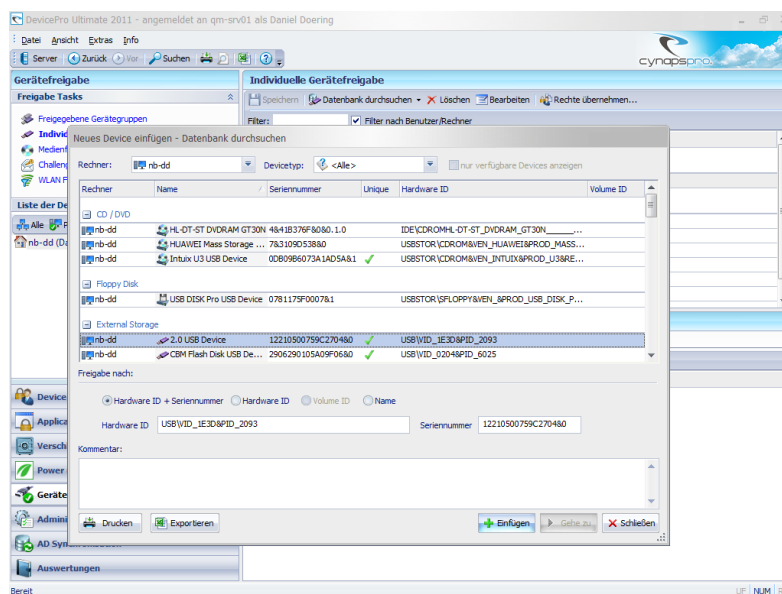
### 3. Gerätefreigaben

- a. Die *individuelle Gerätefreigabe* ignoriert die Einstellungen von Benutzer- oder Rechnerrechten. Geben Sie hier ein Gerät für bestimmte User, Computer, Gruppen oder die ganze Firma frei, so sind diese Geräte als Ausnahme freigegeben.
- b. Die Freigabe per *Freigegebene Gerätegruppen* ist eine Whitelist, welche sich nach Benutzer- oder Computerrechten richtet. Hat z.B. ein Benutzer einen Vollzugriff auf externe Speichermedien, so kann er nur die externen Speichermedien verwenden, welche in dieser Liste explizit genannt wurden?

## Nutzung der Gerätefreigabe

Haben Sie den Mitarbeitern unterbunden, dass z.B. externe Speichermedien verwendet werden, so können Sie autorisierte USB Sticks wieder nach Seriennummer, VolumeID, HardwareID oder Name freigeben.

Hierfür gehen Sie bitte auf den Navigationspunkt **Gerätefreigabe**. Sie befinden sich nun automatisch in der **individuellen Gerätefreigabe**. Um die Liste aller bereits installierten und eingeschalteten Rechner zu erhalten, klicken Sie unter **Verzeichnis Dienst Struktur** nun auf den Button **alle**. Nun wählen Sie einen oder mehrere Rechner aus, von welchen Sie scannen möchten, was für Geräte an diesen Computern angeschlossen sind oder waren. Als nächstes klicken Sie auf den Button **Rechner scannen**. Möchten Sie diese Daten von einem Offline Rechner beziehen, so wählen Sie neben dem Button **Rechner scannen** per DropDown Icon die Option **Datenbank durchsuchen**. Wählen Sie nun ein Gerät aus und klicken auf **Einfügen**. Anschließend können Sie entweder sofort auf **Speichern** gehen, um das Gerät der ganzen Firma zur Verfügung zu stellen oder einzelnen Benutzern, Gruppen oder Computer zuweisen.



## Aktivierung der Protokollierung (optional)

Sie können bei Bedarf einsehen, welche Daten Ihre Mitarbeiter auf oder von externen Datenträgern transferiert haben. Einer solchen Protokollierung bedarf es aus Datenschutzgründen dem 4 Augen Prinzip. Um die Protokollierung aktivieren zu können, benötigen Sie die Passwörter der readme.txt.

Gehen Sie nun auf **Administration/Protokollierung**. Hier klicken Sie auf **Aktivieren**. Wählen Sie, ob die Protokollierung **für alle Mitarbeiter** oder **nur für ausgewählte Mitarbeiter** verwendet werden soll, den entsprechenden Passwortschutz für die Einsicht der Protokollierung und gehen dann auf **Bestätigen**.

Haben Sie die Methode **nur für ausgewählte Mitarbeiter** gewählt, so können Sie die Protokollierung für einzelne Gruppen oder Benutzer starten, indem Sie über **Device Management** mit der rechten Maustaste auf das Objekt klicken und **Addons aktivieren/ Protokollierung** wählen.

Die Protokollierung des Datentransfer finden Sie entweder beim Benutzer im Reiter **Protokollierung** oder unter **Auswertungen/Protokollierung**.

## Verwendung des ShadowCopy Verfahrens (optional)

Zusätzlich zur Protokollierung können Sie von Datentransfers der externen Speichermedien eine Schattenkopie erzeugen.

Hierfür müssen Sie entweder den **DevicePro Server + ShadowCopy Server** bei der Installation ausgewählt, oder jeweils eine Installation für den **DevicePro** Server und den **ShadowCopy** Server vorgenommen haben. Nachträglich können Sie diese Einstellung über das **AdminTool** ändern, welches Sie im Startmenü unter Alle Programme/cynapspro GmbH auf dem Server finden.

Haben Sie einen DevicePro und ShadowCopy Server, so können Sie nun unter **Administration/ShadowCopy** die Pfade zur Ablage der Schattenkopien bestimmen. Weiter könnten Sie bestimmen, wie groß das zwischengespeicherte Datenvolumen werden darf, wenn ein Client offline ist, bzw. wann die Daten vom Client zum ShadowCopy Server übertragen werden sollen.

Schattenkopien werden nach dem Abziehen eines Datenträgers gesammelt zum Server übertragen und können in der DevicePro Management Konsole entweder beim Benutzer im Reiter **Protokollierung** oder unter **Auswertungen/Protokollierung** eingesehen werden. Hierbei sehen Sie hinter den Dateinamen das entsprechende Symbol zum Aufruf oder Speichern der jeweiligen ShadowCopy.

DevicePro Ultimate 2011 - angemeldet an qm-srv01 als Daniel Doering

Server Zurück Vor Rechteverwaltung

**Auswertungen**

**Auswertungen Tasks**

- Rechteübersicht - detailliert
- Rechteübersicht - Zusammenfassung
- Abweichungen von Standardrechten
- Einmalige Freigaben
- Freischaltungscode Übersicht
- Individuelle Gerätefreigabe
- Zugewiesene Contentheaderfilter
- Protokollierung**
- Gesperrte Zugriffe
- Zugriffsstatistik
- Power Management - Ihr Gewinn
- Verdächtige Aktivitäten

**Verzeichnis-Dienst Struktur**

- cynapspro
- Eigenes Directory

**Device Management**

**Application Management**

**Verschlüsselung**

**Power und Data Destruction Management**

**Gerätefreigabe**

**Administration**

**AD Synchronisation**

**Auswertungen**

**Protokollierung**

Anzeigen  Sofort berechnen Filter: Datenbank

Filter - Operation

Datum: von  24.05.2011 bis  31.05.2011 Device: <Alle> Operation: <Alle>

Filter - Datei

Änderung: von  31.05.2011 bis  31.05.2011 Dateiname:

Größe: > <  Doppelte ausblenden Zeitabschnitt: 5 Sekunden

Device	Benutzer	Rechner	Datum	Uhrzeit	Zugriff	Dateiname	Größe	Datum
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:18	Löschen	U:\SystemManufacturer...	1074 B	
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:58	Lesen	U:\Eigene Bilder\Winter.jpg		
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:50	Lesen	U:\Winter.jpg		
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:57	Lesen/Schr...	U:\Eigene Bilder\Winter.jpg	103 KB	02.04.2...
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:49	Lesen/Schr...	U:\Winter.jpg	103 KB	02.04.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	26.05.2011	10:59:21	Lesen	D:\AutoPlay\Images\CD...	180 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	26.05.2011	11:00:06	Lesen	D:\AutoPlay\Images\CD...	180 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	30.05.2011	10:32:25	Lesen	D:\AutoPlay\Images\CD...	180 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	30.05.2011	10:36:36	Lesen	D:\AutoPlay\Images\CD...	180 KB	10.10.2...
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:35	Lesen	U:\Eigene Bilder\Desktop...	193 B	30.05.2...
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:41	Lesen	U:\Eigene Bilder\Desktop...	193 B	30.05.2...
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:53	Lesen	U:\Eigene Bilder\Desktop...	193 B	30.05.2...
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:53:03	Lesen	U:\Eigene Bilder\Desktop...	193 B	30.05.2...
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:29	Lesen/Schr...	U:\Eigene Bilder\Desktop...	193 B	07.07.2...
Corsair Voyage...	nb-tes...	nb-test01.c...	30.05.2011	16:52:29	Lesen/Schr...	U:\Eigene Bilder\Desktop...	193 B	07.07.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	26.05.2011	10:59:18	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	26.05.2011	11:00:05	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	26.05.2011	11:00:19	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	26.05.2011	11:00:29	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	30.05.2011	10:32:22	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	30.05.2011	10:36:33	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	30.05.2011	10:36:48	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...
TEAC DV-W24E	nb-tes...	nb-test01.c...	30.05.2011	10:36:58	Lesen	D:\AutoPlay\autorun.cdd	198 KB	10.10.2...

Bereit

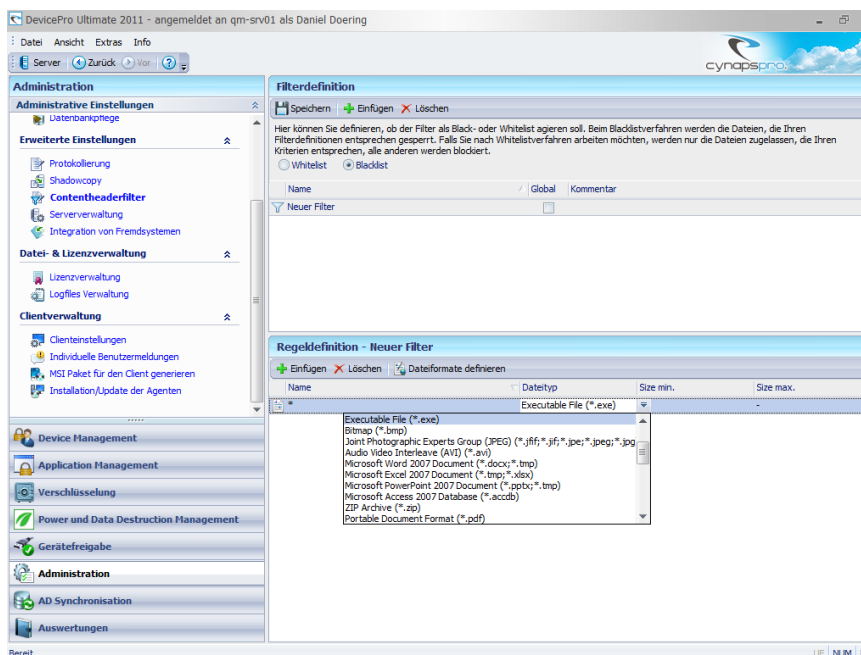
## Eingrenzen von Zugriffen auf Dateien oder Dateitypen (optional)

Möchten Sie verhindern, dass Mitarbeiter unkontrolliert Dateien und Dateitypen in die Firma bringen oder herausschleusen, so können Sie den Contentheaderfilter verwenden.

Hierfür gehen Sie auf [Administration/Contentheaderfilter](#).

Legen Sie mit dem Button **Einfügen** einen neuen Filter an und definieren anschließend die Regeln für diesen Filter.

Hierbei können Sie z.B. im unteren Teil des Fensters auf den Button **Einfügen** klicken und in der Spalte Dateityp aus der Bibliothek die Option „executable File (\*.exe)“ auswählen.

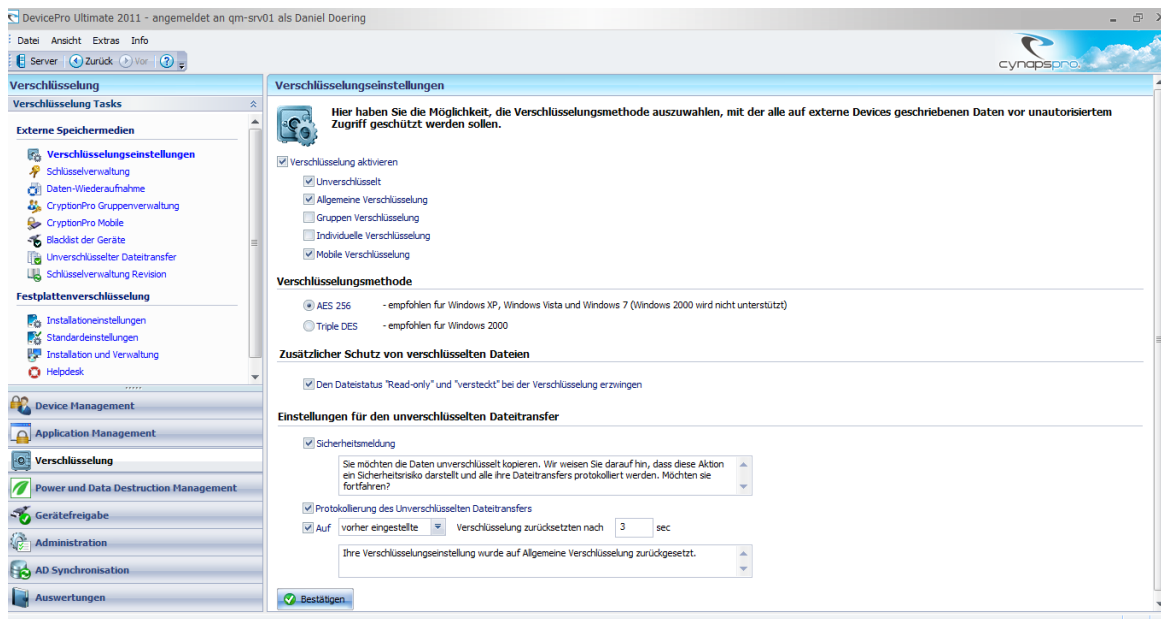


Setzen Sie den Haken bei **Global**, greift dieser Filter für die ganze Firma. Möchten Sie dies nicht, so können Sie unter **Device Management** diesen Filter Gruppen oder Benutzern im Reiter **Contentfilter** zuweisen.

## Inbetriebnahme von CryptionPro

Die Verschlüsselung von CryptionPro lässt sich mit wenigen Mausklicks in Betrieb nehmen. Gehen Sie hierfür in der DevicePro Management Konsole auf den Navigationspunkt **Verschlüsselung**. Dort wählen Sie nun die Checkbox **Verschlüsselung aktivieren** und hinterlegen, welche Optionen später für die Mitarbeiter aktivierbar sein sollen. Folgende Möglichkeiten stehen Ihnen zur Verfügung:

- **Unverschlüsselt** – Mitarbeiter können auch Daten nicht verschlüsselt ablegen
- **Allgemeine Verschlüsselung** – Jeder Mitarbeiter darf die Daten der (anderen) Kollegen entschlüsseln
- **Gruppenverschlüsselung** – Bilden Sie später unter Gruppenverwaltung entsprechende Gruppen, in denen nur Gruppenmitglieder oder die Gruppenmitglieder von untergeordneten Gruppen die Daten (anderer Gruppenmitglieder) entschlüsseln dürfen
- **Individuelle Verschlüsselung** – Gewähren Sie den Mitarbeitern, dass nur sie selbst ihre Daten wieder entschlüsseln dürfen
- **Mobile Verschlüsselung** – Eine ausführbare Datei wird automatisiert auf USB Sticks abgelegt und kann mit einem Passwort an Fremdrechnern zur Ent- oder Verschlüsselung verwendet werden.



Nachdem Sie nun auf Bestätigen geklickt haben, können Sie CryptionPro bei den Benutzern aktivieren. Hierfür gehen Sie bitte auf **Device Management** zum jeweiligen Benutzer und klicken mit der rechten Maustaste auf diesen. Wählen Sie nun bei **Addons aktivieren** das **CryptionPro**. Ab jetzt werden bei diesen Benutzern automatisiert im Hintergrund die Datentransfers auf externen Speichermedien verschlüsselt.

Möchten Sie dem Mitarbeiter noch weitere Optionen zur Verfügung stellen, so können Sie dies im unteren Teil vornehmen. Diese Optionen finden Sie im Reiter **CryptionPro**. Hier können Sie beispielsweise die **Mobile Verschlüsselung** zur Verfügung stellen und **automatisch aktivieren** lassen. In diesem Fall erscheint beim Benutzer beim nächsten Anstecken eines USB Sticks ein Popup, in welchem er ein Passwort zum zukünftigen Verwenden der CryptionProMobile.exe an „Nicht-Firmenrechnern“ eingeben kann. Hat er das Passwort hinterlegt, so wird automatisiert das

CryptionPro Mobile auf den USB Stick geschrieben. Verschlüsselte Dateien können dann auch außerhalb der Firma entschlüsselt werden.



## Gratulation

Nun sind Sie mit der kompletten cynapro Endpoint Data Protection Lösung bestens vertraut.  
Für weitere Unterstützung stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Gerne stehen wir Ihnen aber auch bei aufkommenden Fragen unterstützend zur Seite.

### **cynapro GmbH**

Pforzheimer Straße 134  
76275 Ettlingen  
Germany

**Tel.** +49 (0)7243-35495-0

**Fax.** +49 (0)7243-35495-10

**eMail:** [contact@cynapro.com](mailto:contact@cynapro.com)

**Website:** <http://www.cynapro.com>

**Wir wünschen Ihnen viel Spaß mit unseren Produkten.**

