

# Dell Wyse-Geräte-Manager

Version 5.7.3 Administratorhandbuch



## Anmerkungen, Vorsichtshinweise und Warnungen

-  **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.
-  **VORSICHT:** Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.
-  **WARNUNG:** Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

© 2018 Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

# Inhaltsverzeichnis

<b>1 Einführung</b> .....	<b>6</b>
Wichtige Funktionen.....	6
Hauptfunktionen der WDM Enterprise Edition.....	7
Support-Matrix.....	8
Technischer Support für Dell Wyse.....	11
Zugehörige Dokumentation und Dienste.....	11
Dell Wyse Online-Community.....	12
<b>2 Zugreifen auf WDM</b> .....	<b>13</b>
<b>3 Dashboard</b> .....	<b>14</b>
Lizenzen.....	16
Hinzufügen einer Workgroup-Lizenz.....	16
Aktivieren der Workgroup-Lizenz.....	16
Upgraden einer Workgroup-Lizenz auf eine Enterprise-Lizenz.....	17
Unlizenzierte Geräte.....	17
WDM-Utilitys.....	18
Importieren von Daten mit dem Import-Dienstprogramm.....	19
Utility für die HA-Konfiguration.....	22
Konto-Utility.....	23
DNS-DHCP-Such-Utility.....	23
<b>4 Geräte</b> .....	<b>24</b>
<b>5 Anwendungen</b> .....	<b>31</b>
Bearbeiten des Paket-Skripts eines registrierten Pakets.....	38
Exportieren des Paket-Skripts eines registrierten Pakets.....	38
Registrieren eines Pakets über eine Skriptdatei – .RSP.....	38
Ein Paket registrieren – nur .exe-, .msi-, .msu- und .bat-Dateien.....	40
PCoIP-Gerätekonfiguration.....	41
<b>6 Updates</b> .....	<b>48</b>
Aufgaben.....	48
Wiederkehrende Aktualisierungen.....	49
Echtzeit Befehle.....	50
Repository-Synchronisierung.....	51
Peer-gestützte Verteilung.....	51
Profile.....	52
Identifizieren von vom Profile-Manager unterstützten Geräten.....	53
Bereitstellen eines Konfigurationspakets mithilfe des Profil-Managers.....	53
Löschen eines PM-Konfigurationspakets.....	54
<b>7 Default Device Configuration – DDC</b> .....	<b>55</b>

<b>8 Berichte.....</b>	<b>57</b>
Erstellen eines Protokollberichts.....	57
Erstellen eines Anwendungsberichts.....	58
Erstellen eines Berichts zu einer Remote-Sitzung.....	58
<b>9 System.....</b>	<b>60</b>
Manuelles Erstellen von Subnetzen.....	61
Registrieren von Remote-Repositorys.....	63
Hinzufügen von Benutzern aus lokalen Konten.....	65
Hinzufügen von Benutzern und Gruppen von Domänencontroller und globalem Katalog.....	66
Bearbeiten von Benutzerberechtigungen.....	66
Löschen von Benutzern.....	73
Konsole.....	73
Konfigurieren der Geräteerkennung.....	77
Über die Services.....	79
Konfigurieren der Protokollierungsebenen.....	81
Planung.....	82
Peer-gestützte Verteilung.....	83
Voraussetzungen für PAD.....	85
Konfigurieren von PAD.....	88
Bereitstellen eines Pakets mit PAD.....	90
Anzeigen von PAD-Details.....	90
Bearbeiten und Löschen von PAD-Zeitplänen.....	92
Wyse ThinOS.....	93
<b>10 Verwaltung von Teradici-Geräten mit WDM.....</b>	<b>94</b>
Schritte zum Erstellen einer DNS_SRV-Datensatzes.....	94
Überwachung und Fehlerbehebung.....	96
Konfigurieren der Firmware 5.x.....	98
Aktualisieren der ThreadX 4.X-Geräte auf ThreadX 5.X über WDM.....	106
Bereitstellen des Zertifikats auf ThreadX 4.x-Geräten .....	107
Aktualisieren der Client-Firmware auf ThreadX 5.x.....	107
<b>11 Fehlerbehebung.....</b>	<b>114</b>
Probleme beim Erkennen von Geräten.....	114
Probleme beim Erkennen von PXE-Geräten.....	115
Paketfehler.....	115
Wake-on-LAN-Befehl wird nicht auf Remote-Geräten ausgeführt.....	115
Probleme bei der Peer-gestützten Verteilung.....	115
Profil-Manager-Fehler.....	116
Tipps zur Behebung von Fehlern beim Repository.....	117
Fehlerbehebung bei T50- und WTOS-Fehlern.....	118
Fehlerbehebung bei WCM-Problemen.....	120
Paketaktualisierung schlägt fehl, wenn das CIFS-Repository aktiviert ist.....	120
PAD Image-Erstellung und Drag-and-Drop-Funktionen funktionieren auf Linux-Geräten nicht.....	121
Standardgerätekonfiguration zeigt exportierte Images nicht an.....	121

VNC-Protokoll wird nicht generiert.....	121
Das Fenster „Update Now“ (Jetzt aktualisieren) wird für den Benutzer für WCM-Linux nicht angezeigt.....	121
Abgerufenes Image kann nicht zurück auf T50-Gerät übertragen werden.....	121
Bereitstellung des PColP-Sprachpakets fehlgeschlagen.....	121
Geräte meldet sich nicht bei japanischem BS an.....	122
Anwendungsfehler nach der WDM-Aktualisierung von Version 5.5 oder MR auf 5.7.....	122
ThinOS-Gerät unterbricht Anmeldung beim WDM-Server.....	125
Problem beim Erkennen von Geräten mit alten HAgents – 6.3.2.54 und niedriger – auf lokalisiertem WDM-Server.....	125
Anmeldeseite erscheint nicht in der Web-UI.....	126
Problem bei der Anmeldung bei der Web-UI.....	126
EMSDK startet nicht aufgrund der Portnummer .....	126
Fehler bei Domain-Benutzeranmeldungen und HAPI-Protokoll.....	126
Probleme beim Zugriff auf die Seite „Device“ (Gerät).....	127
OSD-Logo-Konfigurations- oder Firmware-Übertragungsfehler auf ThreadX 5.X-Geräten.....	127
ThreadX 5.X-Gerätestatus wechselt zu „Offline“ .....	127
Manuelles Konfigurieren von ThreadX 5.X-Geräten unter Verwendung der Teradici-Verwaltungskonsole, wenn keine automatische Konfiguration möglich ist.....	128
Konfiguration von WDM-Dienstprogrammen nicht möglich.....	131
Konfiguration von WCM, Paketregister, Remote-Shadow und PColP nicht möglich.....	131

# Einführung

Dell Wyse Device Manager (WDM)-Software ist eine erstklassige Lösung der Enterprise-Klasse für die einfache und sichere Remote-Verwaltung von Dell Wyse Thin und Zero Clients. Sie ermöglicht IT-Fachleuten die schnelle und unkomplizierte Organisation, Aktualisierung, Steuerung und Unterstützung Tausender Windows Embedded-, Wyse Enhanced Linux-, Wyse ThinLinux-, Wyse ThinOS-, Wyse ThinOS Lite- und PCoIP-Zero-Client-Geräte (ThreadX-Geräte) in einem beliebigen LAN-, WAN- oder Drahtlosnetzwerk.

Die Software nutzt branchenübliche Kommunikationsprotokolle und eine komponentenbasierte Architektur zur effizienten Verwaltung Ihrer Netzwerkgeräte. Dell Wyse Device Manager (WDM) umfasst eine benutzerfreundliche Benutzeroberfläche, mit der Sie leicht alle Geräteverwaltungsfunktionen durchführen können, die für die Ausführung und Wartung Ihrer WDM-Umgebung erforderlich sind. Sie können auf die WDM-Benutzeroberfläche standortunabhängig über einen beliebigen unterstützten Browser zugreifen und auch alle Vorgänge über die Web-UI durchführen. Die Web-UI ist besonders benutzerfreundlich und ermöglicht Ihnen eine einfache Nutzung aller Geräteverwaltungsfunktionen.

Themen:

- [Wichtige Funktionen](#)
- [Hauptfunktionen der WDM Enterprise Edition](#)
- [Support-Matrix](#)
- [Technischer Support für Dell Wyse](#)

## Wichtige Funktionen

Die Hauptfunktionen von WDM sind:

- **Geräteermittlung** – Sie können WDM zur Erkennung von Geräten im Netzwerk konfigurieren, indem Sie unterschiedlichen Subnetze oder IP-Bereiche einrichten. Nach der Konfiguration von WDM können Sie problemlos nach Geräten suchen und automatisch Geräte zum System hinzufügen. Sobald diese dem System hinzugefügt wurden, sind sie für künftige Verwaltung verfügbar.
- **Geräteverwaltung** – WDM ermöglicht jederzeit das Anzeigen des Status Ihrer Geräte. WDM kann so konfiguriert werden, dass die Informationen über die Aktualisierung des Status aller Geräte automatisch bereitgestellt werden.
- **Erfassung von Bestandsinformationen** – WDM überwacht und speichert alle Bestandsinformationen über alle Geräte, einschließlich Hardware-Bestandsinformationen und Informationen zu Software, die auf den einzelnen Geräten installiert ist. Informationen zu Software umfassen das Betriebssystem und Informationen über alle Anwendungen und auf dem Gerät angewandte Add-Ons.
- **Remote-Steuerung von Geräten und Geräte-Spiegelung** – Sie können Geräte in demselben Subnetz herunterfahren, neu starten oder Geräte in verschiedenen Subnetzen über die Remote-Konsole aus dem Ruhezustand aktivieren. Es ist nicht erforderlich, zum Endbenutzer-Desktop zu wechseln. WDM stellt für Ihr Helpdesk eine Spiegelungsfunktion zur Diagnose von Problemen innerhalb von Endbenutzerumgebungen von einem Remote-Standort aus bereit.
- **Geräteorganisation** – WDM ist ein zuverlässiges Verwaltungswerkzeug, mit dem Sie Ihre Geräte nach Gruppen organisieren können, die für Ihre Organisation am sinnvollsten sind, und zwar unabhängig vom physischen Standort oder dem Speicherort der Geräte im Netzwerk.
- **Profile Manager** – WDM ermöglicht die Bereitstellung einer vordefinierten Konfiguration für eine bestimmte Gruppe von Geräten über Profile Manager. Bei diesen Konfigurationen handelt es sich um solche, die Sie mit dem Dell Wyse Configuration Manager (WCM) erstellen und in einem angegebenen Repository speichern.
- **Softwarebereitstellung und Aktualisierungen** – WDM ermöglicht Ihnen die einfache Bereitstellung und Aktualisierung von Software und Images auf Geräten.

- **Erfassung und Bereitstellung der Gerätesoftware** – Mit WDM, können Sie ein Referenz-Gerät erstellen, das die für die Installation erforderliche Software enthält, und dieses Geräte-Abbild erfassen. Auf diese Weise können Sie die Gerätekonfiguration und die auf dem Gerät während der gesamten Installation installierte Software klonen.
- **Planung der Geräteaktualisierungen** – WDM-Konfigurationen ermöglichen eine Planung der Softwarebereitstellung und Updates für Geräte (Verhinderung von Ausfallzeiten). Geräteaktualisierungen können entweder sofort, zu einem festgelegten Zeitpunkt oder beim nächsten Start des Geräts durchgeführt werden.
- **Wiederholungsplaner** – Damit können Pakete wiederholt geplant werden: täglich (oder an bestimmten Wochentagen), wöchentlich oder monatlich, bis zu einem bestimmten Datum oder für eine feste Anzahl an Wiederholungen.
- **Bereitstellung der Gerätekonfiguration** – Sie können verschiedene Konfigurationen erstellen, die unabhängig von einem Image für ein Gerät bereitgestellt werden können.
- **Repository-Erstellung und -Verwaltung** – Mit WDM können Sie ganz einfach ein Repository an Software, Images und Konfigurationsaktualisierungen für die Verteilung erstellen und verwalten.
- **Geräteansichten** – In den Geräteansichten können Sie Geräteinformationen einfach anzeigen und ändern und so praktische Protokolle und Geräteberichte erstellen.
- **Verteilte Verwaltung** – Bietet Ihnen granulare Kontrollmöglichkeiten der Administratorrechte basierend auf Benutzergruppen oder einzelnen Benutzern. Sie können beispielsweise Administrator A das Recht zuweisen, Aktualisierungen für Gruppe 1, 2 und 3 aber nicht für 4 anzuzeigen und bereitzustellen und gleichzeitig Administrator B das Recht zuweisen, nur für Gruppe 4 Aktualisierungen anzuzeigen und bereitzustellen.
- **Administratorspezifizierte Bandbreitensteuerung** – Hier können Sie die für die Serverkommunikation zu verwendende Bandbreite steuern (zum Beispiel können Sie einen Server so konfigurieren, dass basierend auf der Verfügbarkeit eine geringere Bandbreite verwendet wird; oder Sie können DFÜ-Verbindungen durch die Verwendung einer einfachen Profileinrichtung mit einer niedrigeren Geschwindigkeit als Breitbandgeschwindigkeit konfigurieren).
- **Option zum Neustart fehlgeschlagener Aktualisierungen** – Diese Option kann konfiguriert und verwendet werden, um fehlgeschlagene Aktualisierungen einfach neu zu starten. Sie können festlegen, wie oft WDM versuchen soll, Aktualisierungen zu wiederholen (entweder ein Paket oder ein Image), bevor eine Fehlermeldung angezeigt wird (die Anzahl der Wiederholungsversuche und Fehler kann in der WDM-Konsole eingesehen werden).
- **Default Device Configuration (DDC) Support (Unterstützung für Standardgerätekonfiguration)** – Mit WDM können Sie auf einfache Weise DDCs erstellen und verwalten. Sie können mehrere Pakete auf ein Gerät über eine einzige DDC anwenden.
- **WDM--Benutzer hinzufügen** – Sie können Active Directory-Benutzer oder lokale Benutzer in der WDM-Benutzeroberfläche hinzufügen und Berechtigungen zuweisen.
- **Verbesserte Remote-Unterstützung** – Die folgenden Berichte sind in der Web-UI von WDM verfügbar:
  - **Anwendungsberichte** – Dies ermöglicht dem Benutzer die Erstellung eines Berichts, der die Geräte, auf denen bestimmte Software installiert ist, sowie die vom Benutzer ausgewählte Version aufführt.
  - **Berichte zu Remote-Sitzungen** – Der Bericht für Remote-Sitzungen enthält Informationen zu Remote-Sitzungsverbindungen auf allen Geräten.
  - **Protokollberichte** – Diese Berichte enthalten wichtige Informationen über Ereignisse oder Aktivitäten, die hinsichtlich WDM-Komponenten auf dem WDM-Server stattgefunden haben.

## Hauptfunktionen der WDM Enterprise Edition

Die zusätzlichen WDM Enterprise Edition-Funktionen umfassen:

- **Secure Communication between a WDM Server, Repository, and a Device** (Sichere Kommunikation zwischen einem WDM-Server, Repository und einem Gerät) – Ermöglicht die sichere Kommunikation zwischen Client und Webserver durch Verschlüsselung des Datenverkehrs zum und vom Client und Server und Ausgabe von Zertifikaten. Zertifikate müssen von einer Zertifizierungsstelle signiert werden, die bestätigt, dass der Zertifikatinhaber die Entität ist, die er vorgibt zu sein. Organisationen können wählen, ob Sie die Zertifizierungsstelle für internen Webserverzugriff sein möchten.  
WDM-Web-UI unterstützt **Federal Information Processing Standards (FIPS)**.
- **Merlin Imaging System** (Merlin Imaging-System) – Bietet HTTP-, HTTPS- und CIFS-basiertes Imaging und eine bessere Leistung bei der Bereitstellung von großen Images.
- **Added Scalability with Remote Repositories** (Zusätzliche Skalierbarkeit mit Remote-Repositories) – Skalieren Sie Ihre Lösung durch Hinzufügen von Remote-Repositories zu Ihrer Infrastruktur. Mit dieser Funktion können Sie Remote-Serverspeicherorte für die

Speicherung von Terminal-Firmware und -Software verwenden. Dadurch reduziert sich die Menge des Netzwerk-Datenverkehrs über ein Wide Area Network (WAN), weil der Großteil des Update-Datenverkehrs (das tatsächliche Image) nur einmal über das WAN an das Remote-Repository übertragen wird. Geräte können die Aktualisierungssoftware vom Remote-Server statt vom zentralen Server abrufen. Zudem wird die Geschwindigkeit des Gesamtaktualisierungsvorgangs erhöht. WDM ermöglicht weiterhin die Durchführung aller Geräteverwaltungsaufgaben vom zentralen Server aus (z. B. von Ihrem Rechenzentrum).

- **Distributed Architecture** (Verteilte Architektur) – Mit dieser Funktion können Sie WDM-Komponenten auf einem oder mehreren Computern in Ihrem Netzwerk platzieren.
- **Default Device Configuration** (Standardgerätekonfiguration) – Diese Funktion ermöglicht Ihnen die Konfiguration standardmäßiger Software sowie Gerätekonfigurationen für eine Gruppe von Geräten. Mit dieser Funktion wird sichergestellt, dass das Gerät sowohl mit der Software- als auch mit der Gerätekonfiguration übereinstimmt. Bei einer Abweichung von Standardkonfigurationen setzt WDM das Gerät auf die von Ihnen angegebenen Konfigurationen zurück. Diese Funktion dient zur Automatisierung der Wiederherstellung ausgefallener Geräte, der Zweckanpassung vorhandener Geräte und der Hinzufügung neuer Geräte innerhalb der bestehenden Infrastruktur.
- **Expanded Hierarchical Views** (Erweiterte hierarchische Ansichten) – Mit dieser Funktion können Sie bis zu 30 verschiedene Organisationsansichten Ihrer Geräte erstellen und so die visuellen Geräteverwaltungsmöglichkeiten Ihres WDM-Servers erweitern.
- **Automated Grouping** (Automatisches Gruppieren) – Diese Funktion wird verwendet, um automatisch jedes neue Gerät, das dem System hinzugefügt wurde, den gewünschten vordefinierten Gruppen zuzuordnen.
- **Support for Multiple Databases** (Unterstützung für mehrere Datenbanken) – Dank der Unterstützung für mehrere Datenbanken bei der Installation von WDM für eine SQL 2008- oder 2012-Umgebung können Sie Ihre bereits vorhandene Back-End-Infrastruktur verwenden.
- **Active Directory Integration** (Active Directory-Integration) – Damit können Sie WDM-Benutzergruppen oder einzelne Benutzer ganz einfach aus Ihrer vorhandenen Active Directory-Einrichtung importieren.
- **Peer Assisted Deployment** (Peer-gestützte Verteilung) – Peer Assisted Deployment (PAD) ist ein Mechanismus, der Updates wie z. B. Basis-Images und Add-Ons für Thin Client-Geräte bereitstellt, die über den WDM-Server verwaltet werden. Dieser Mechanismus funktioniert am besten in Umgebungen, in denen Geräte auf mehrere Subnetze verteilt sind.

Die PAD-Funktion ist für die folgenden Plattformen anwendbar:

- Windows 10 IoT Enterprise
- SUSE Linux
- Windows Embedded Standard 7 (WES7)
- Windows Embedded 8 Standard (WE8S)
- ThinLinux

- **Profile Manager** (Profil-Manager) – Der PM ermöglicht die Bereitstellung einer vordefinierten Konfiguration auf einer bestimmten Gruppe von Geräten. Bei diesen Konfigurationen handelt es sich um solche, die Sie mit dem Dell Wyse Configuration Manager (WCM) erstellen und in einem angegebenen Repository speichern. Die Konfigurationen des Profil-Managers sind eindeutig für ein Betriebssystem, und Sie können nur eine Konfiguration gleichzeitig auf eine Gruppe von Geräten anwenden.
- **Chargeback Accounting** – Diese Funktion wird auf Geräten mit Windows, Linux und Wyse Thin OS (ThinOS) unterstützt. Hier wird die Remote-Sitzung erfasst und gespeichert.

## Support-Matrix

Tabelle 1. Support-Matrix

<p><b>Unterstützte Betriebssysteme für WDM Server</b></p>	<ul style="list-style-type: none"> <li>• Windows Server 2008 R2 Enterprise SP1</li> <li>• Windows Server 2012 Standard</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2016</li> <li>• Windows 7 Enterprise SP1 – 64-Bit</li> </ul>
<p><b>Unterstützte Betriebssysteme für das Upgrade aller WDM-Komponenten</b></p>	<ul style="list-style-type: none"> <li>• Windows 2008 R2 SP1 Enterprise</li> <li>• Windows 2008 Service Pack 2 32-Bit</li> <li>• Windows 7 Enterprise SP1—32-Bit</li> <li>• Windows Server 2012 Standard</li> <li>• Windows Server 2012 R2</li> </ul>

<p><b>Unterstützte Datenbanken</b></p>	<ul style="list-style-type: none"> <li>· Microsoft SQL Server 2008 R2 – Englisch</li> <li>· Microsoft SQL Server 2008 Enterprise – 32-Bit</li> <li>· Microsoft SQL Server 2012</li> <li>· Microsoft SQL Server 2014</li> <li>· Microsoft SQL Server 2016</li> <li>· Microsoft SQL Server 2012 Enterprise Edition für hohe Verfügbarkeit</li> <li>· Microsoft SQL Server 2016 Express SP1</li> </ul>
<p><b>Unterstützte Thin Clients</b></p>	<p><b>Wyse ThinOS</b></p> <ul style="list-style-type: none"> <li>· Wyse 3010 Thin Client mit ThinOS</li> <li>· Wyse 3020 Thin Client mit ThinOS</li> <li>· Wyse 3040 Thin Client mit ThinOS</li> <li>· Wyse 5010 Thin Client mit ThinOS</li> <li>· Wyse 5040 Thin Client mit ThinOS</li> <li>· Wyse 3030 LT Thin Client mit ThinOS</li> <li>· Wyse 5060 Thin Client mit ThinOS</li> <li>· Wyse 7010 Thin Client mit ThinOS</li> </ul> <p><b>Wyse ThinOS PCoIP</b></p> <ul style="list-style-type: none"> <li>· Wyse 5040 AIO Thin Client mit PCoIP</li> <li>· Wyse 5010 Thin Client mit PCoIP</li> <li>· Wyse 3030 LT Thin Client mit PCoIP</li> <li>· Wyse 5060 Thin Client mit PCoIP</li> </ul> <p><b>Wyse Enhanced Microsoft Windows Embedded Standard 7 – Build 818 und höher</b></p> <ul style="list-style-type: none"> <li>· Wyse 5010 Thin Client mit WES7</li> <li>· Wyse 5020 Thin Client mit WES7</li> <li>· Wyse 7010 Thin Client mit WES7</li> <li>· Wyse 7020 Thin Client mit WES7</li> <li>· Wyse 7010 erweiterte Gehäuse Thin Client mit WES7</li> <li>· Wyse 3030 Thin Client mit WES7</li> </ul> <p><b>Wyse Enhanced Microsoft Windows Embedded Standard 7P – Build 850 und höher</b></p> <ul style="list-style-type: none"> <li>· Wyse 7010 Thin Client mit WES7P</li> <li>· Wyse 7010 erweiterte Gehäuse Thin Client mit WES7P</li> <li>· Wyse 5020 Thin Client mit WES7P</li> <li>· Wyse 7020 Thin Client mit WES7P</li> <li>· Wyse 7040 Thin Client mit WES7P</li> <li>· Dell Latitude E7270 Mobile Thin Client</li> <li>· Wyse 5060 Thin Client mit WES7P</li> <li>· Latitude 3460 Mobile Thin Client</li> </ul> <p><b>Wyse Enhanced Microsoft Windows Embedded 8 Standard – 64-Bit</b></p> <ul style="list-style-type: none"> <li>· Wyse 5010 Thin Client mit WE8S</li> <li>· Wyse 5020 Thin Client mit WE8S</li> <li>· Wyse 7010 Thin Client mit WE8S</li> </ul>

- Wyse 7020 Thin Client mit WE8S

#### **Windows 10 IoT Enterprise – 64-Bit**

- Wyse 5020 Thin Client mit Win10 IoT
- Wyse 7020 Thin Client mit Win10 IoT
- Wyse 7040 Thin Client mit Win10 IoT

#### **Wyse Enhanced SUSE Linux Enterprise**

- Wyse 5010 Thin Client mit Linux
- Wyse 5020 Thin Client mit Linux
- Wyse 7010 Thin Client mit Linux
- Wyse 7020 Thin Client mit Linux

#### **ThinOS Lite**

- Wyse 3010 Zero Client für Citrix
- Wyse 3020 Zero Client für Citrix
- Wyse 5010 Zero Client für Citrix

#### **ThreadX/View Zero Client**

- Wyse 5030 Zero Client
- Wyse 7030 Zero Client
- Wyse 5050 AIO Zero Client mit PCoIP

#### **ThinLinux**

- Wyse 3030 LT Thin Client mit ThinLinux
- Wyse 3040 Thin Client mit ThinLinux
- Wyse 7020 Thin Client mit ThinLinux
- Wyse 5020 Thin Client mit ThinLinux
- Wyse 5060 Thin Client mit ThinLinux

#### **Unterstützte EOL Dell Wyse Thin Client-Plattformen**

#### **Wyse Enhanced Microsoft Windows Embedded Standard 7 – Build 818 und höher**

- C90LE7
- R90L7
- R90LE7
- X90c7
- X90m7
- Z90s7

#### **Wyse Enhanced Microsoft Windows Embedded Standard 7P**

- X90m7P
- Z90s7P

#### **Wyse Enhanced Microsoft Windows Embedded 8 Standard – 32-Bit**

- Wyse 5010 Thin Client mit WE8S
- Wyse 7010 Thin Client mit WE8S
- Z90D8E

#### **Wyse Enhanced SUSE Linux Enterprise**

- C50LE
- R50L
- R50LE
- X50c
- X50M
- Z50S

#### **ThinOS Lite**

- C00X
- R00X

#### **ThreadX/View Zero Client**

- P20

#### **Wyse ThinOS**

- C10LE
- R10L

#### **Wyse Enhanced Microsoft Windows Embedded Standard 2009 —Build 641 und höher**

- C90LEW
- 5010
- R90LW
- R90LEW
- V90LEW
- X90CW
- X90MW
- 7010
- Z90SW

## Technischer Support für Dell Wyse

Technische Ressourcen des Self-Service-Portals, der Knowledge Base, Software-Downloads, Registrierung, Serviceverlängerungen/RMAs, Referenzhandbücher usw. finden Sie unter [www.dell.com/wyse/support](http://www.dell.com/wyse/support). Informationen zum Kunden-Support finden Sie unter [www.dell.com/support/contents/us/en/19/article/Contact-Information/International-Support-Services/international-contact-center?ref=contactus](http://www.dell.com/support/contents/us/en/19/article/Contact-Information/International-Support-Services/international-contact-center?ref=contactus) und Telefonnummern für Basic und Pro Support sind unter [www.dell.com/supportcontacts](http://www.dell.com/supportcontacts) verfügbar.

HINWEIS: Vergewissern Sie sich vor dem Fortfahren, ob Ihr Produkt über eine Dell-Service-Tag-Nummer verfügt. Weitere Informationen zu Produkten mit Dell-Service-Tag-Nummer finden Sie unter [www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse](http://www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse).

## Zugehörige Dokumentation und Dienste

Technische Datenblätter mit Funktionen von Hardwareprodukten sind auf der Dell Wyse-Website verfügbar. Rufen Sie <http://www.dell.com/wyse> auf, wählen Sie Ihr Hardwareprodukt und laden Sie das technische Datenblatt herunter.

Um Support für Ihr Wyse-Produkt zu erhalten, überprüfen Sie die Service-Tag- oder Seriennummer Ihres Produkts.

- Für Produkte, die mit einer Dell Service Tag-Nummer gekennzeichnet sind, finden Sie Knowledge Base-Artikel und Treiber auf den Dell Wyse-Produktseiten.

- Für Produkte, die nicht mit einer Dell Service Tag-Nummer gekennzeichnet sind, finden Sie alle erforderlichen Support-Materialien in der Wyse Support-Domäne.

## Dell Wyse Online-Community

Dell Wyse bietet eine Online-Community, innerhalb der Benutzer unserer Produkte nach Informationen zu Benutzerforen suchen und diese austauschen können. Besuchen Sie die Dell Wyse Online-Community-Foren unter: [en.community.dell.com/techcenter/enterprise-client/wyse\\_general\\_forum/](https://en.community.dell.com/techcenter/enterprise-client/wyse_general_forum/).

# Zugreifen auf WDM

Um auf die WDM-UI zuzugreifen, gehen Sie wie folgt vor:

- 1 Öffnen Sie den unterstützten Browser für die WDM-UI. Im Folgenden werden die unterstützten Webbrowser für den Zugriff auf die WDM-Web-UI aufgeführt.
    - Internet Explorer 11
    - Chrome v40 und höhere Versionen
    - Firefox V43 und höhere Versionen
    - Microsoft Edge
  - 2 Geben Sie die folgende URL in den Browser ein:  
**https://<WDM Server Host Name/IP Address>/WebUI/app/indexf.html#**
  - 3 Drücken Sie die **Eingabetaste**.
  - 4 Um sich bei der WDM-UI anzumelden, gehen Sie wie folgt vor:
    - Standardmäßig können Sie den in der WDM-UI vorhandenen Benutzernamen mit denselben Anmeldeinformationen verwenden.
    - Benutzer können als lokale oder Domänenbenutzer hinzugefügt werden.
      - Um sich als Domänenbenutzer bei der Web-UI anzumelden, müssen Sie den Domänennamen zusammen mit dem Benutzernamen angeben. Zum Beispiel Domänenname\Benutzername.
- ⓘ ANMERKUNG: Benutzer@Domäne wird nicht unterstützt.**
- Geben Sie für den lokalen Benutzer nur den Benutzernamen an. Zum Beispiel **Benutzername**. Der **lokale Benutzer** ist ein lokal auf der Maschine, auf der der Verwaltungsserver installiert ist, erstellter Benutzer.

**ⓘ ANMERKUNG: Löschen Sie die Cookies und den Cache vor dem Durchsuchen der Web-UI.**

Funktionen der WDM-Web-UI-Anwendung:

- Dashboard
- Geräte
- Anwendung
- Updates
- Berichte
- System

# Dashboard

Die Dashboard-Seite ermöglicht die Anzeige der Details des Serverstatus, des Funktionszustands des Geräts, der Aufgabenliste, der Warnungen, Ereignisse und Informationen über den eingetragenen Server. Sie können schnell eine Zusammenfassung der Informationen für jeden Funktionsbereich des Systems anzeigen. Angezeigt werden die Informationen für die folgenden Attribute:

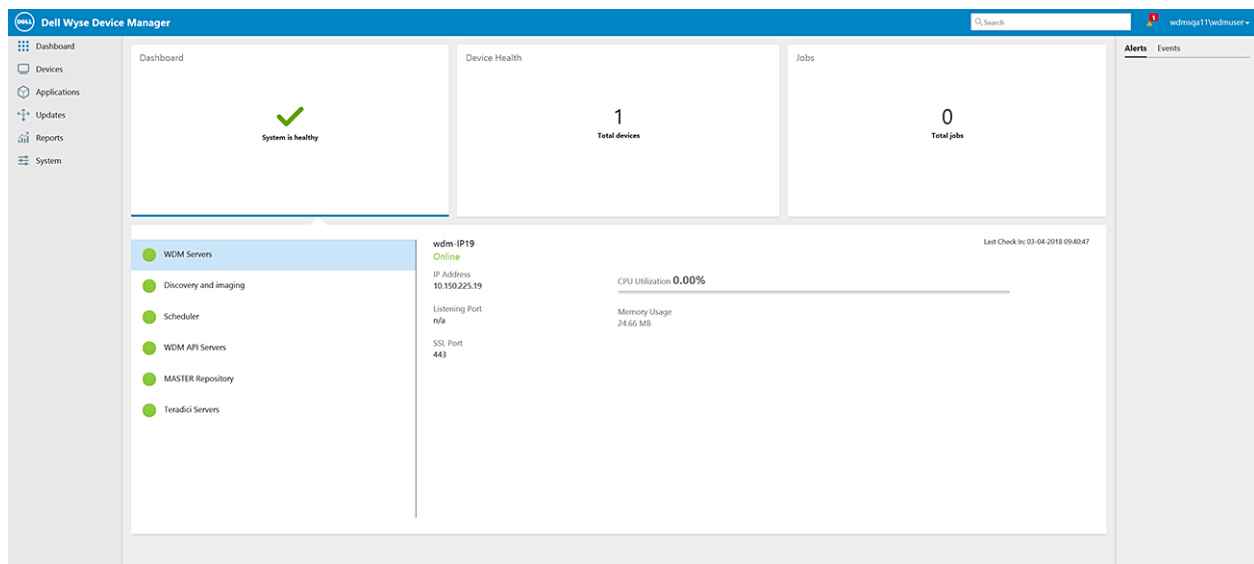


Abbildung 1. Dashboard

- Serverstatus
- Geräte Gesundheit
- Aufgaben

Datum und Uhrzeit für den zuletzt eingetragenen Server werden angezeigt.

Sie können auch die Systemaktualisierungen anzeigen, indem Sie oben rechts auf der Seite „Dashboard“ auf die folgenden Registerkarten klicken.

- Warnungen
- Ereignisse

Sie müssen über Administratorrechte verfügen, um Aktualisierungen auszuwählen, die Auswahl von Aktualisierungen aufzuheben und Aktualisierungen zu löschen. So löschen Sie Warnungen oder Ereignisse:

- Wählen Sie eine Warnung oder ein Ereignis aus.
- Sie können die gesamte Liste der Warnungen oder Ereignisse durch Klicken auf **Select all** (Alles auswählen) oder **Deselect all** (Gesamte Auswahl aufheben) auswählen oder die Auswahl aufheben.
- Klicken Sie auf **Clear** (Löschen), um ausgewählte Warnungen oder Ereignisse zu löschen.

Tabelle 2. Dashboard

Parameter	Beschreibung
Serverstatus	<p>Wenn Sie auf die Kachel <b>Server Status</b> (Serverstatus) klicken, zeigt diese den Status des Servers und Informationen über die ausgeführten Dienste an.</p> <p>Auf der Benutzeroberfläche werden folgende Dienste aufgeführt:</p> <ul style="list-style-type: none"> <li>• WDM Servers (WDM-Server)</li> <li>• Discovery and imaging (Erkennung und Imaging)</li> <li>• Scheduler (Planer)</li> <li>• WDM-API-Server</li> <li>• Master-Repository</li> <li>• Teradici-Server</li> </ul> <p>Wenn einer der Dienste aus irgendeinem Grund angehalten wurde, wird als Status des Servers <b>System is down</b> (System ist ausgefallen) angezeigt. Wenn die Dienste in Betrieb sind, wird als Status des Servers <b>System is healthy</b> (System ist funktionsfähig) angezeigt.</p>
Geräte Gesundheit	<p>Beim Klicken auf die Kachel <b>Geräte Gesundheit</b> wird die Gesamtzahl der beim WDM-Server registrierten Geräte angezeigt. Im unteren Bereich der Seite „Geräte Gesundheit“ werden der Systemzustand jeder Plattform (horizontal aufgeführt) und eine Liste der mit dem WDM-Server verbundenen Geräte sowie Anwendungen und Hardwareversion (vertikal aufgeführt) angezeigt.</p> <p>Der Status des Geräts wird wie folgt klassifiziert:</p> <ul style="list-style-type: none"> <li>• Fehlerfrei</li> <li>• Ausgelastet</li> <li>• Offline</li> <li>• Sleeping (Im Ruhemodus)</li> </ul>
Aufgaben	<p>Beim Klicken auf die Kachel <b>Aufgaben</b> wird die Gesamtzahl der geplanten Aufgaben angezeigt. Darüber hinaus wird der Status der geplanten Aufgaben wie folgt angezeigt:</p> <ul style="list-style-type: none"> <li>• Waiting (Wartet)</li> <li>• Running (Wird ausgeführt)</li> <li>• With errors (Mit Fehlern)</li> </ul>
Warnungen	<p>Mit diesem Parameter können Sie Systemereignisse sowie Warnungen wie beispielsweise Lizenzfehler anzeigen und überwachen.</p> <p><b>ANMERKUNG:</b> Für Threadx 5.x-Geräte werden folgende Warnungen angezeigt, wenn die in der WDM-Bereitstellung verfügbare volle Kapazität pro Teradici Proxy-Server erreicht wird.</p> <ul style="list-style-type: none"> <li>• Bei 15 000 Geräten wird eine Warnung zur vollen Kapazität angezeigt.</li> <li>• Bei 18 000 Geräten wird eine Fehlermeldung angezeigt.</li> </ul>
Ereignisse	<p>Oben rechts auf dem Bildschirm „Dashboard“ können Sie die Liste der Ereignisse oder durchgeführten Aktionen wie das manuelle Hinzufügen eines Geräts, Echtzeitbefehle, Paketverteilung etc. sehen.</p>

Klicken Sie auf die Dropdown-Listenoption **Logged in Username** (Benutzername des angemeldeten Benutzers), um die folgenden Aktionen in der WDM-Anwendung durchzuführen.

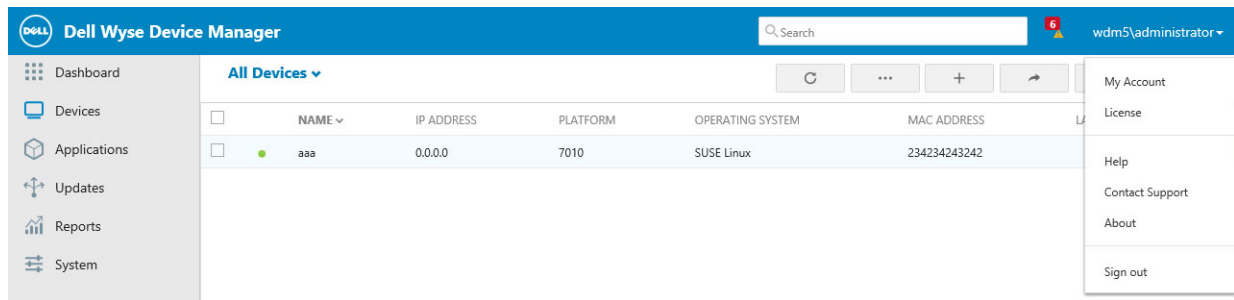


Abbildung 2. Alle Geräte

- **My Account** (Mein Konto) – Klicken Sie auf diese Option, um das Profil des eingeloggteten Benutzers anzuzeigen.
- **License** (Lizenz) – Wählen Sie diese Option zum Anzeigen der WDM-Lizenzinformationen. Weitere Informationen finden Sie unter [Lizenzen](#).
- **Help** (Hilfe) – Klicken Sie auf diese Option, um das Administratorhandbuch herunterzuladen.
- **Contact Support** (Support kontaktieren) – Wenn Sie auf diese Option klicken, werden Sie zur Dell Support-Website weitergeleitet, auf der Sie die entsprechenden Kontaktinformationen finden.
- **About** (Info) – Klicken Sie auf diese Option, um Details zu Buildnummer, Hotfix, Beschreibung und Installation der WDM-Version anzuzeigen.
- **Sign out** (Abmelden) – Klicken Sie auf diese Option, um sich von der WDM-Web-UI-Anwendung abzumelden.

Themen:

- [Lizenzen](#)
- [Unlizenzierte Geräte](#)
- [WDM-Utilities](#)

## Lizenzen

Die Seite **Licenses** (Lizenzen) enthält Details über WDM Enterprise-Lizenzen wie den Verkaufsschlüssel, nicht aktivierten Schlüssel, Aktivierungscode, Lizenz und Beschreibung.

Der Standardzeitraum für die Testlizenz ist 30 Tage. Sie können den Testlizenzzeitraum von 30 Tagen auf 60 Tage verlängern.

**ANMERKUNG:** Die Workgroup-Lizenz muss aktiviert werden.

Am 29. Tag der Lizenzierung oder einen Tag vor 30 Tagen läuft die Probezeit ab. Zum Verlängern des Lizenzzeitraums klicken Sie auf **Extend License** (Lizenz verlängern) auf der Lizenzseite. Die Probezeit wird um weitere 30 Tage verlängert.

## Hinzufügen einer Workgroup-Lizenz

- 1 Klicken Sie auf **Add license** (Lizenz hinzufügen).
- 2 Geben Sie den Lizenzschlüssel im Format 7 Zeichen-6 Zeichen-6 Zeichen-7 Zeichen ein oder kopieren Sie die Lizenz und fügen Sie sie ein.
- 3 Klicken Sie auf **Save** (Speichern).

## Aktivieren der Workgroup-Lizenz

- 1 Wählen Sie die nicht aktivierte Workgroup-Lizenz aus.

2 Klicken Sie auf **Activate License** (Lizenz aktivieren) in der rechten Ecke der Lizenzseite.

① **ANMERKUNG: Notieren Sie die nicht aktivierte Lizenz für die Verwendung beim WDM-Online-Lizenzierungsformular. Sie können die nicht aktivierte Lizenz auch kopieren und im WDM-Online-Lizenzierungsformular einfügen.**

3 Geben Sie die WDM-Lizenzierungsdetails im Fenster **Get Activation code** (Aktivierungscode beziehen) ein. Sie benötigen die folgenden Informationen, um das Formular ausfüllen:

- Kontaktnamen des Unternehmens
- E-Mail-Adresse des Unternehmens
- Adresse des Unternehmens
- Einen WDM-Verkaufsschlüssel und einen nicht aktivierten Schlüssel

4 Der Aktivierungscode wird angezeigt. Darüber hinaus erhalten Sie eine E-Mail mit Ihrem Aktivierungscode.

5 Geben Sie den Aktivierungscode in das Feld **Add Activation Code** (Aktivierungscode hinzufügen) ein oder kopieren Sie ihn und fügen Sie ihn ein und klicken Sie dann auf **Activate Key** (Schlüssel aktivieren).

Sie können die Lizenzdetails auf der Seite **Licenses** (Lizenzen) überprüfen.

① **ANMERKUNG: Wenn Ihr WDM-Server über keine Internetverbindung verfügt, wechseln Sie zum Aktivieren des WDM-Verkaufsschlüssels zur folgenden URL:**<https://www.rapportlicensing.com/clientframe/rapport.aspx>.

## Upgraden einer Workgroup-Lizenz auf eine Enterprise-Lizenz

Nachdem Sie eine aktivierte oder nicht aktivierte Workgroup-Lizenz zu Ihrer WDM-Installation hinzugefügt haben, können Sie die Lizenz auf eine Enterprise-Lizenz upgraden.

① **ANMERKUNG: Beim Upgrade auf eine Enterprise-Lizenz werden alle Workgroup-Lizenzen gelöscht.**

1 Klicken Sie auf **Add license** (Lizenz hinzufügen).

2 Geben Sie die neue Enterprise-Lizenz ein oder kopieren Sie sie und fügen Sie sie ein.

3 Klicken Sie auf **Save** (Speichern).

4 Nach dem Abschluss des Upgrades zeigt die Seite **Licenses** (Lizenzen) Ihre neuen, nicht aktivierten Enterprise-Lizenz-Informationen.

5 Aktivieren Sie die Lizenz, indem Sie die Schritte im Abschnitt [Aktivieren einer Workgroup-Lizenz](#) befolgen.

## Unlizenzierte Geräte

Wenn die Zahl der ermittelten Geräte die in WDM verfügbaren Lizenzen überschreitet, werden die zusätzlich ermittelten Geräte in der Liste „Unlicensed device“ (Nicht lizenziertes Gerät) aufgelistet. Sie können diese nicht lizenzierten Geräte zu den lizenzierten Geräten verschieben, indem Sie die Option **Add to Licensed Devices** (Zu lizenzierten Geräten hinzufügen) auswählen und anklicken.

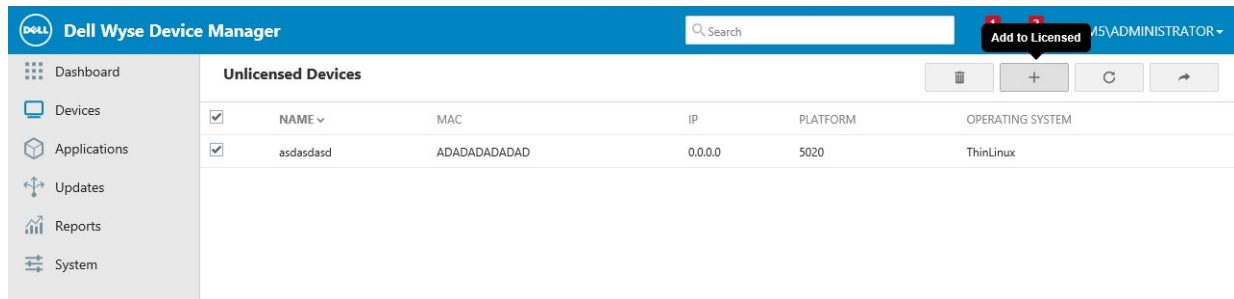
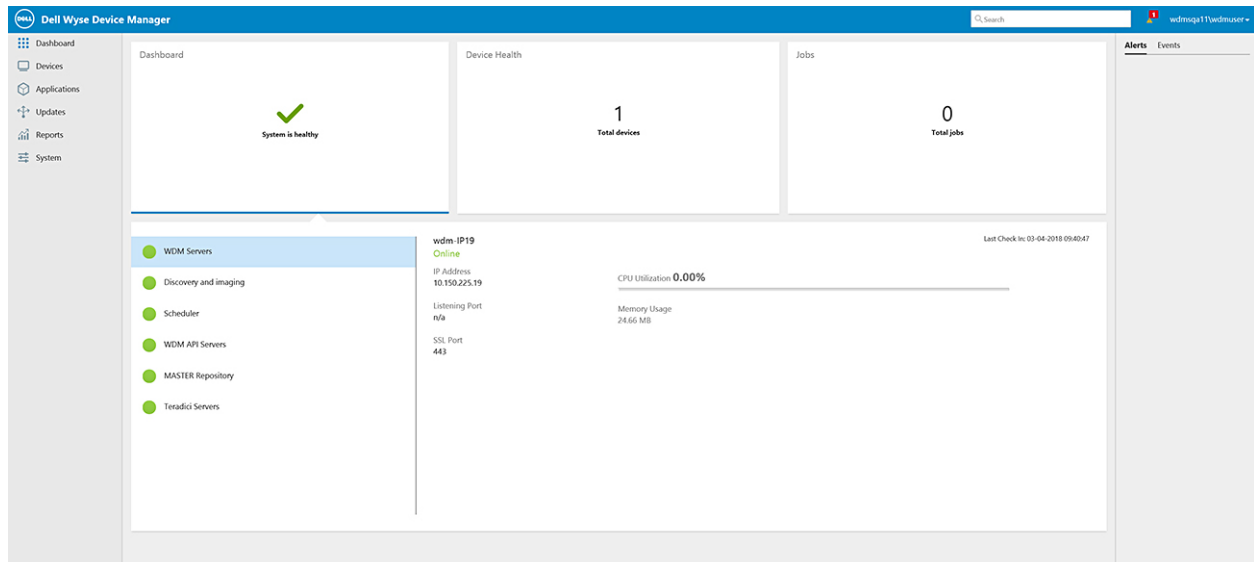


Abbildung 3. Unlizenzierte Geräte

**ANMERKUNG:**

- Um unlizenzierte Geräte zu den lizenzierten Geräte zu verschieben, muss der WDM-Administrator ausreichend Lizenzen bereitstellen.
- Wenn Sie nicht über genügend Lizenzen verfügen und versuchen, ein nicht lizenziertes Gerät zu den lizenzierten Geräten zu verschieben, wird die folgende Meldung angezeigt: `You have no license for the vendor` (Sie haben keine Lizenz für den Anbieter). Wenn Sie der Lizenzseite trotzdem ein Gerät hinzufügen möchten, dann fügen Sie eine Lizenz hinzu, die für mehrere Geräte gilt, oder löschen Sie die bereits vorhandenen Geräte auf der Lizenzseite.

## WDM-Utilities

WDM bietet viele Utilities, die zahlreiche zusätzliche Funktionen wie das Konfigurieren der Hochverfügbarkeit, Importieren von Daten in die Datenbank, Verwalten von Konten und die DNS-DHCP-Suche enthalten.

Führen Sie die folgenden Schritte durch, um auf das Utility zuzugreifen:

- 1 Klicken Sie auf die Drop-Down-Liste **Logged in Username (Angemeldeter Benutzername) > My Account (Mein Konto) > WDM Utilities (WDM-Dienstprogramme)** .  
Das Fenster **WDM Utilities** (WDM-Dienstprogramme) wird angezeigt. Es enthält Optionen zum Herunterladen und Konfigurieren der WDM-Dienstprogramme.
- 2 Klicken Sie auf **Configure WDM Utilities** (WDM-Dienstprogramme konfigurieren).
- 3 Speichern Sie die benutzerdefinierte Protokolldatei. Die Datei wird als **CustomProtocolforWDMUtilities.exe** heruntergeladen.
- 4 Führen Sie die Datei als Administrator aus.
- 5 Extrahieren Sie den Inhalt der heruntergeladenen Datei.

**ANMERKUNG:** Extrahieren Sie den Inhalt an denselben Speicherort, an dem die Datei **CustomProtocolforWDMUtilities.exe** heruntergeladen wird.

- 6 Folgende WDM-Utilities werden angezeigt:
  - **HA** (Utility für die HA-Konfiguration)
  - **Import** (Importieren von Daten in die Datenbank)
  - **Account** (Konto-Utility)
  - **DNS-DHCP** (Utility für DNS-DHCP-Suche)

## Importieren von Daten mit dem Import-Dienstprogramm

Im Abschnitt **Allgemeine WDM-Dienstprogramme** können Sie Daten aus **comma-delimited**- und **tab-delimited**-Dateien importieren. Dieses Dienstprogramm ermöglicht das Importieren von Geräten, Subnetzen, IP-Adressbereichen, Repositories oder Standardgruppen für Subnetze aus einer Datei in der WDM-Datenbank. Die Daten müssen aus Flatfiles importiert werden. Ein Flatfile mit Trennzeichen enthält einen oder mehrere Datensätze, getrennt durch ein bestimmtes Trennzeichen wie beispielsweise ein Komma oder ein Tabulatorzeichen.

Zum Importieren von Daten führen Sie folgende Schritte durch:

- 1 Wählen Sie aus dem Drop-Down-Menü die bevorzugte Kategorie aus.  
Die Drop-Down-Liste **Import Category** (Importkategorie) enthält die folgenden Optionen:
  - Gerät
  - Subnetze
  - IP-Bereiche
  - Repositories
  - Standardgruppen für Subnetze
- 2 Navigieren Sie zu dem Ordner und wählen Sie die Datei aus.  
Der Dateiname wird im Feld **Import File Name** (Name der Importdatei) angezeigt.
- 3 Klicken Sie auf **Import** (Importieren), um die Datendateien zu importieren.
- 4 Klicken Sie auf **Clear** (Löschen), um alle Einträge zu löschen.

## Format für den Import von Geräteeinstellungen aus Flatfiles

Das Format zur Bereitstellung von Daten in einem Flatfile für Geräteeinstellungen ist wie folgt:

```
Client-Name;MAC-Adresse;Plattform;Benutzerdefiniertes Feld 1 ;Benutzerdefiniertes Feld 2 ;Benutzerdefiniertes Feld 3 ;Kontakt;Standort;BS
```

- Client-Name ist der Name des Geräts. Beispiel: W1009341019
- MAC-Adresse des Geräts. Zum Beispiel: 0080646A1144
- Plattform des Geräts. Beispiel: VX0
- Benutzerdefiniertes Feld 1
- Benutzerdefiniertes Feld 2
- Benutzerdefiniertes Feld 3
- Kontakt sind die Ansprechpartner-Informationen für das Gerät. Beispiel: Administrator
- Standort des Geräts. Beispiel: Büro San Jose
- BS ist der Code des Betriebssystems des Geräts. Dieses Feld gilt nur für Geräte mit dem neuen Dell Namensschema.

Nachfolgend die Betriebssystemcodes:

- Wyse Xenith – XEN
- WTOS – BL
- WTOS PCoIP – BLP
- PCoIP (ThreadX) – TDC
- SUSE Linux – SLX

- Red Hat Linux 6.x, 7.x und 8.x – RLX
- Windows XP – XP
- Windows Embedded Standard – WES
- Windows Embedded Standard 7 – WES7
- Windows Embedded Standard 7 P – WES7P
- WE8Sx Windows Embedded 8 Standard 32 – WE8Sx
- Windows Embedded 8 Standard 64 – WE8SEmbedded 8 Standard 64 – WE8S
- Windows 10 IoT Enterprise – WIE10

Ein Beispiel für Geräteeinstellungsdaten ist wie folgt:

```
D90Q8;A02040401050;5020;XYZ;MN;OP;WE8S;W1009341019;0080646A1144;VX0;ABCD;EFGH;IJKL;Administrator;Büro San Jose;WES
```

## Format für den Import von Subnetzdaten aus Flatfiles

Das Format zur Bereitstellung von Daten in einem Flatfile für das Subnetz ist wie folgt:

Broadcast-Adresse, Beschreibung, SW-Repository, Überschreibung-Standardparameter, IP-Adresse, Subnetzmaske, Max. simultane Webdienst-Updates, Wake-On-LAN-Zeitlimit (Sek.), Wake-On-LAN-Versuche, TFTP-Zeitlimit (Sek.), TFTP-Wiederholungen, Netzwerkkartengeschwindigkeit

- Broadcast-Adresse für das Gerät. Beispiel: 10.10.10.255
- Beschreibung ist der in der GUI angezeigte Subnetzname.
- SW-Repository ist der Name eines Software-Repository. Beispiel: Master  
Es kann kein Subnetz ohne Software-Repository hinzugefügt werden.
- Überschreibung-Standardparameter – Globale Überschreibungseinstellungen (gilt nur für Enterprise-Lizenz)
- IP-Adresse ist die gültige IP-Adresse im Subnetz. Beispiel: 199.199.10.2
- Subnetzmaske des Geräts. Zum Beispiel: 255.255.255.0
- Max. simultane Webdienst-Updates ist der Grenzwert für die maximale Anzahl gleichzeitiger Aktualisierungen. Beispiel: 5
- Wake-On-LAN-Zeitlimit (in Sekunden) ist das Zeitlimit für Wake-On-LAN. Beispiel: 2
- Wake-On-LAN-Versuche ist der Grenzwert für WOL-Wiederholungen. Beispiel: 3
- TFTP-Zeitlimit (in Sekunden). Zum Beispiel 10
- TFTP-Wiederholungen ist der Grenzwert für TFTP-Wiederholungen. Beispiel: 3
- Netzwerkkartengeschwindigkeit des Geräts. Zum Beispiel 1 (für Auto), 2 (für 100M-F), 3 (für 100M-H)

Ein Beispiel für Subnetzdaten ist wie folgt:

```
10.10.10.255,Subnet1,MASTER,False,199.199.10.2,255.255.255.0,6,2,1,1,7,2.
```

In diesem Beispiel wird eine Subnetzdefinition hinzugefügt, die Geräte eines Subnetzes der Klasse C mit IP-Adresszuweisungen von 199.10.0.1 bis 199.10.0.254 erkennt und verwaltet. Der Spaltenkopf ist entweder nicht vorhanden oder besteht in der obigen korrekten Reihenfolge.

**ANMERKUNG:** Vor der Arbeit mit Subnetzen muss die WDM-Datenbank Informationen über mindestens ein Repository enthalten.

## Format für den Import von IP-Bereichsdaten aus Flatfiles

Das Format zur Bereitstellung von Daten in einem Flatfile für einen IP-Bereich ist wie folgt:

StartIP, EndIP, ExclusionStartIP, ExclusionEndIP, Beschreibung

- StartIP – IP-Anfangsadresse für den IP-Bereich

- EndIP – IP-Endadresse für den IP-Bereich
- ExclusionStartIP – IP-Anfangsadresse für den IP-Ausschlussbereich
- ExclusionEndIP – IP-Endadresse für den IP-Ausschlussbereich
- Beschreibung – Eingabe des Namens für den in der GUI angezeigten IP-Bereich

Ein Beispiel für IP-Bereichsdaten ist wie folgt:

Mein IP-Bereich 10.10.10.10 10.10.10.200 10.10.10.20 10.10.10.30

Die IP-Bereichsdefinition wird der Datenbank hinzugefügt, um alle Geräte zwischen den Bereichen 10.10.10.10 bis 10.10.10.19 und 10.10.10.31 bis 10.10.10.200 zu erkennen. Diese IP-Bereichsdefinition wird in der WDM-GUI als **My IP Range** (Mein IP-Bereich) angezeigt.

## Format für den Import von Software-Repository-Daten aus Flatfiles

Das Format zur Bereitstellung von Daten in einem Flatfile für ein Software-Repository ist wie folgt:

Repository-Name, Repository-IP-Adresse, Transfertyp, Relativer Pfad, Kontext, FTP-Portnummer, HTTP-Portnummer, FTP-Benutzername, FTP-Kennwort, HTTP-Benutzername, HTTP-Kennwort, IsHTTP Secure, HTTPSValidateWithCA, RemoteServerName, CIFSUsername, CIFSPassword

- Name des Software-Repository, wie er in der GUI angezeigt wird
- Standort ist die IP-Adresse des FTP-Servers
- Transfertyp ist der Typ des verwendeten Übertragungsprotokolls. Er kann FTP oder HTTP oder beides sein.
- Relativer Pfad ist der Pfad zum Software-Repository relativ zum Stammverzeichnis. Der Standardwert dafür ist /rapport.
- Kontext ist für HTTP-Kommunikation gültig und ist der Name des virtuellen Verzeichnisses. Standardmäßig ist der HTTP-Kontext MyWDM.
- FTP-Portnummer ist die Portnummer für FTP-Kommunikation. Standardwert ist 21.
- HTTP-Portnummer ist die Portnummer für HTTP/HTTPS-Kommunikation. Standardwert ist 80 für HTTP- und 443 für HTTPS-Kommunikation.
- FTP-Benutzername ist der Benutzername für das FTP-Konto wie mit IIS-FTP oder dem FTP-Dienst eingerichtet, den Sie für die Verbindung mit dem Repository verwenden.
- FTP-Kennwort ist das Kennwort für das FTP-Konto wie mit IIS-FTP oder dem FTP-Dienst eingerichtet, den Sie für die Verbindung mit dem Repository verwenden.
- HTTP-Benutzername ist der Benutzername für das HTTP-Konto wie mit IIS-HTTP oder dem HTTP-Dienst eingerichtet, den Sie für die Verbindung mit dem Repository verwenden.
- HTTP-Kennwort ist das Kennwort für das HTTP-Konto wie mit IIS-HTTP oder dem HTTP-Dienst eingerichtet, den Sie für die Verbindung mit dem Repository verwenden.
- Secure(HTTPS) – Geben Sie -1 ein, wenn **Secure** (Sicher) aktiviert ist (HTTPS unterstützt) und 0, wenn **Secure** (Sicher) nicht aktiviert ist (HTTP wird unterstützt, nicht HTTPS).
- HTTPSValidateWithCA – Ist -1 wenn **Validate Certificate with CA** (Zertifikat bei ZS überprüfen) aktiviert ist und 0, wenn das Kontrollkästchen deaktiviert ist.

Beispiele für Software-Repository-Daten sind wie folgt:

- Beispiel, bei dem der Transfertyp HTTP und FTP ist  
RemoteHTTPFTP, 10.10.11.9, HTTP and FTP, /rapport, MyWDM, 21, 80, FTPUserName, FTPPassword, HTTPUserName, HTTPPassword, 0, 0
- Beispiel, bei dem der Transfertyp HTTP ist  
RemoteHTTP, 10.10.11.9, HTTP, /rapport, MyWDM, , 80, , , HTTPUserName, HTTPPassword, 0, 0
- Beispiel, in dem der Transfertyp HTTP mit aktiviertem Secure-Flag ist  
RemoteHTTP, 10.10.11.9, HTTP, /rapport, MyWDM, , 443, , , HTTPUserName, HTTPPassword, -1, -1 or  
RemoteHTTP, 10.10.11.9, HTTP, /rapport, MyWDM, , 443, , , HTTPUserName, , -1, -1
- Beispiel, in dem der Transfertyp FTP ist  
RemoteFTP, 10.10.11.9, FTP, /rapport, , 21, , FTPUserName, FTPPassword, , , 0, 0
- Beispiel, in dem der Transfertyp CIFS ist

```
RemoteCIFS,10.150.112.3,SMB,/rapport,MyWDM,,,,,,,,,
0,0,RemoteServerName,CIFSUsername,CIFSPassword
```

- Beispiel, in dem der Transfertyp FTP, HTTP und CIFS ist

```
FTPHTTPandCIFS,10.150.112.3,HTTP and FTP and SMB,/Rapport,MyWDM,
21,80,FTPUsername,FTPpassword,Httpusername,Httppassword,
0,0,RemoteServerName,CIFSusername,CIFSpasword
```

- Beispiel, in dem der Transfertyp FTP, HTTPS und CIFS ist

```
FTPHTTPSandCIFS,10.150.112.7,HTTP and FTP and SMB,/Rapport,MYWDM,
21,443,FTPUsername,FTPPassword,HttpUsername,HttpPassword,-1,0,RemoteServerName,CIFSUserName,CIFSPassword
```

Die Software-Repository-Definition wird der Datenbank hinzugefügt, um ein Repository auf einem Server bei 10.10.11.9 zu definieren. Der Standardpfad für das Stammverzeichnis des FTP-Diensts ist **/rapport**. Auf dieses Repository wird mit dem Benutzernamen des Benutzers zugegriffen. FTP wird als Übertragungsprotokoll verwendet und in WDM als Remote angezeigt.

## Format für den Import von Standardgruppen für Subnetze aus Flatfiles

Das Format zur Bereitstellung von Daten in einem Flatfile für Standardgruppen für Subnetze ist wie folgt:

```
Broadcast-Adresse, Standardgruppe, Standardgruppenwert
```

- IP-Adresse des Geräts. Beispiel: 10.10.10.255
- Standardgruppe. Zum Beispiel Staat
- Standard-Gruppenwert. Zum Beispiel Kalifornien

```
Beispiel 1: 10.150.115.255;Staaten;Kalifornien
```

```
Beispiel 2: 10.150.115.255;Abteilung;Verkauf
```

```
Beispiel 3: 10.150.116.255;Staaten;Kalifornien
```

### ANMERKUNG: Die WDM-Datenbank muss das Subnetz, Gruppen und Gruppenwerte enthalten.

Ein Kontrollkästchen mit der Bezeichnung **Update Existing Default Groups for Subnets** (Bestehende Standardgruppen für Subnetze aktualisieren) wird am unteren Rand der Seite angezeigt, wenn **Default Groups for Subnets** (Standardgruppen für Subnetze) ausgewählt ist.

Wenn das Kontrollkästchen deaktiviert ist, schlägt der Import für jeden Gruppennamenwert fehl, wenn das Subnetz die zugewiesene Standardgruppe bereits enthält.

Wenn das Kontrollkästchen aktiviert ist, wird der Gruppenwert mit dem Gruppennamenwert der Importdatei aktualisiert.

## Utility für die HA-Konfiguration

Das Utility für die HA-Konfiguration wird beim Einrichten einer HA-Umgebung und beim Clustering der Datenbank verwendet. Mit diesem Utility kann WDM mit dem Cluster verbunden werden, um einen einwandfreien Betrieb innerhalb des Clusters zu ermöglichen, und sicherstellen, dass keine Ausfallzeiten auftreten. Dieses Utility ist verfügbar, nachdem Sie WDM installiert haben.

- 1 Geben Sie folgende Informationen ein:
  - **Database Name (Datenbankname)** – Dieser Wert wird standardmäßig angezeigt und kann nicht bearbeitet werden.
  - **Database Server (Datenbankserver)** – Geben Sie den Hostnamen des Datenbankclusters an.
  - **Database Port (Datenbankport)** – Geben Sie die Portnummer an.
  - **Database User Name (Name des Datenbankbenutzers)** – Geben Sie den Datenbankbenutzer an.
  - **Database Password (Datenbankkennwort)** – Geben Sie das Kennwort des Datenbankbenutzers an.
- 2 Klicken Sie auf **Provision** (Bereitstellung).

Die Verbindungsdaten werden im rechten Fensterbereich des Utilitys angezeigt.

 **ANMERKUNG:** Sie sollten die Lizenz erneut eingeben, da bei Bereitstellung die Lizenz geändert wird. Führen Sie das HA-Utility nicht in einer Nicht-HA-Umgebung.

## Konto-Utility

Das Konto-Utility ermöglicht das Anzeigen der Details der WDM-Datenbank und das Erstellen neuer Anmeldeinformationen für den Zugriff auf die Datenbank.

- 1 Das Konto-Utility zeigt die folgenden Informationen an:
  - **Server Port** – Die IP-Adresse des WDM-Datenbankservers und die Datenbankserver-Portnummer.
  - **Database Name** – Der Name der WDM-Datenbank.
  - **User Name** – Der Benutzername zum Zugreifen auf die WDM-Datenbank. Dies ist der Benutzername, den Sie bei der Installation von WDM angegeben haben.
- 2 So ändern Sie die Anmeldeinformationen für den Zugriff auf die Datenbank:
  - a Geben Sie im Feld **User Name** unter **New credentials for WDM database (Neue Anmeldeinformationen für die WDM-Datenbank)** den neuen Benutzernamen ein.
  - b Geben Sie unter **Password (Kennwort)** das Kennwort für den Zugriff auf die Datenbank ein.
  - c Geben Sie das Kennwort erneut in das Feld **Confirm Password (Kennwort bestätigen)** ein.
  - d Wenn Sie den Domänennamen und das -kennwort verwenden möchten, wählen Sie **Connect as domain user (Verbindung als Domänenbenutzer herstellen)**.
- 3 Klicken Sie auf **Update (Aktualisieren)**, wenn Sie neue Anmeldeinformationen eingegeben haben, oder klicken Sie auf **Clear (Löschen)**, um das Fenster zu schließen, wenn Sie keine neuen Anmeldeinformationen eingegeben haben.

## DNS-DHCP-Such-Utility

Mit diesem Utility können Sie nach der Methode suchen, die im Netzwerk zur Ermittlung von WDM durch den Client konfiguriert wurde.

Sie können die Ergebnisse der DNS- und DHCP-Suche für den WDM-Server prüfen.

# Geräte

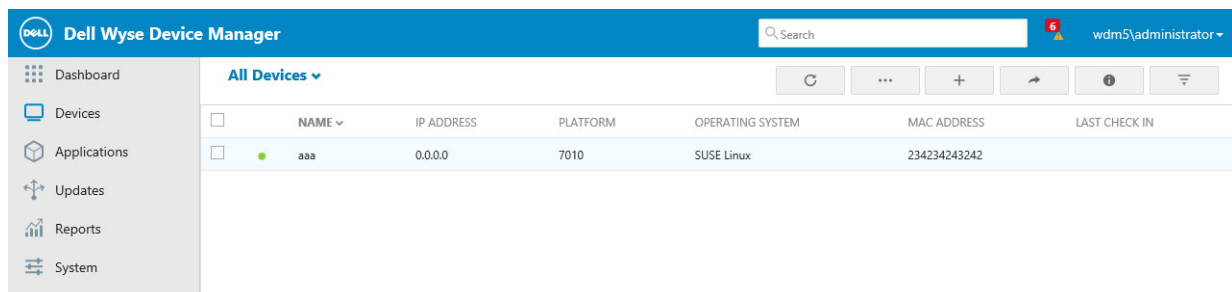
Auf der Seite „Devices“ (Geräte) werden alle Geräte angezeigt, die automatisch oder manuell ermittelt wurden. Es werden detaillierte Geräteinformationen angezeigt und Sie können Aufgaben wie das manuelle Hinzufügen neuer Geräte und Ausführen von Befehlen in Echtzeit durchführen.

**Tabelle 3. Geräte**

Parameter	Beschreibung
Name	Zeigt den Namen des Geräts an.
IP-Adresse	Zeigt die IP-Adresse des Geräts an.
Plattform	Zeigt die Plattform der Geräte an.
Betriebssystem	Zeigt das auf den Geräten ausgeführte Betriebssystem an.
MAC-Adresse	Zeigt die MAC-Adresse der Geräte an.
Last check in (Letztes Einchecken)	Zeigt den Zeitstempel an, wenn das Gerät mit dem WDM-Server kommuniziert.

**ANMERKUNG:** Für alle Geräte wird neben dem Namen der Gerätestatus angezeigt. Wenn Sie mit dem Mauszeiger über das Gerätestatussymbol fahren, wird der Status des jeweiligen Geräts angezeigt.

Eine ausführliche Zusammenfassung der Geräte wird oben links auf der Seite in der Registerkarte **All Devices** (Alle Geräte) angezeigt.

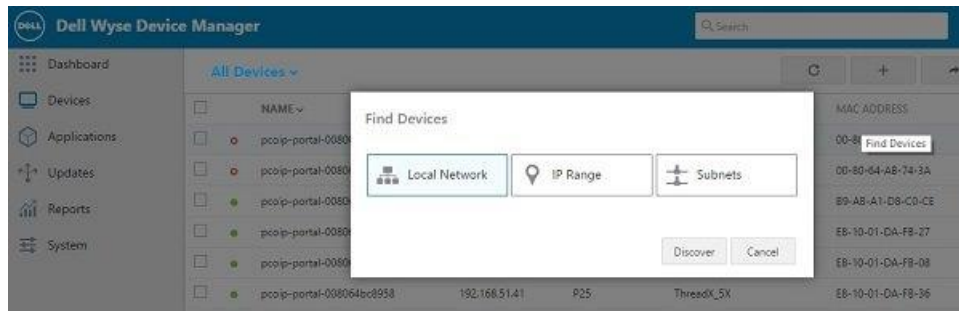


**Abbildung 4. Alle Geräte**

Um Echtzeitbefehle für die gesuchten Geräte auszuführen, führen Sie folgende Vorgänge durch:

Allgemeine Optionen für Echtzeitbefehle:

- 1 Die Echtzeitbefehle werden oben auf dem Bildschirm angezeigt.
  - a Um die Seite zu aktualisieren, klicken Sie auf **Refresh** (Aktualisieren).
  - b Klicken Sie auf **More** (Mehr), um das Gerät umzubenennen, und geben Sie den aktualisierten Namen in das Feld **Rename Device** (Gerät umbenennen) ein.
  - c Klicken Sie auf **Add or find Device** (Gerät hinzufügen oder suchen), um ein Gerät manuell hinzuzufügen oder durch die manuelle Suche nach weiteren Geräten zu suchen.

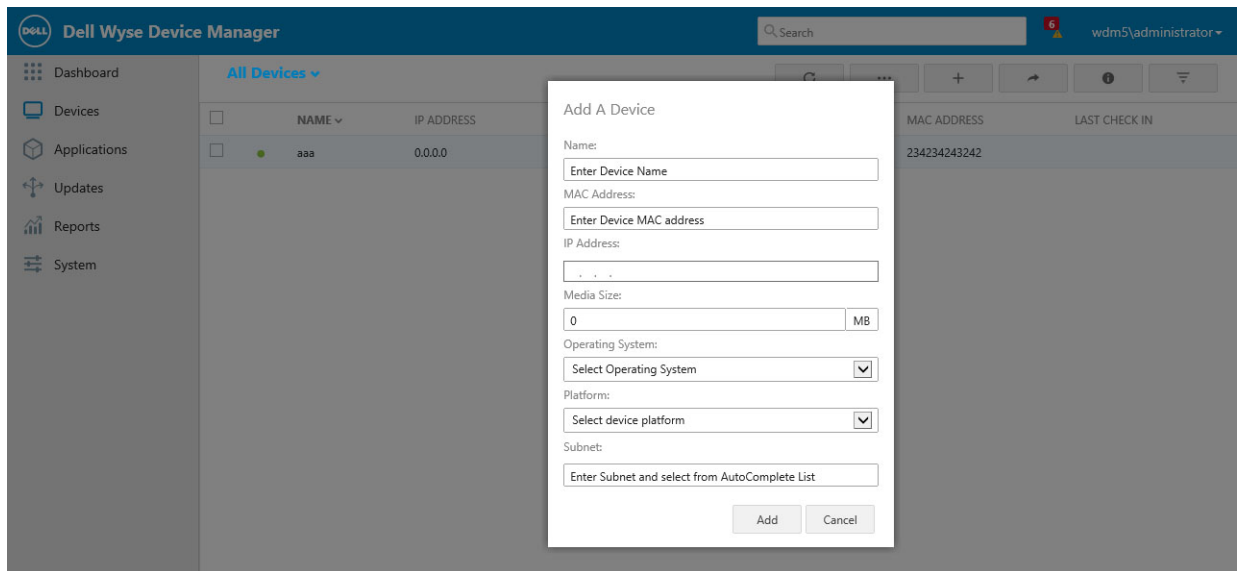


**Abbildung 5. Nach Geräten suchen**

Um nach einem Gerät zu suchen, führen Sie folgende Vorgänge durch:

- 1 Klicken Sie auf die Option **Find Devices** (Geräte suchen). Sie können ein Gerät mithilfe von **Local Network** (Lokales Netzwerk), **IP Range** (IP-Bereich) und **Subnet** (Subnetz) ermitteln.
- 2 Klicken Sie auf die Option **IP Range** (IP-Bereich), um anhand des IP-Bereichs nach einem Gerät zu suchen, und geben Sie einen IP-Adressbereich in das vorgesehene Feld ein.
- 3 Klicken Sie auf die Option **Subnets** (Subnetze), um ein Gerät mithilfe von Subnetzen zu ermitteln. Sie können in der Leiste für **Global Search** (Globale Suche) nach einem Subnetz suchen.
- 4 Klicken Sie auf die Option **Local Network** (Lokales Netzwerk), um über das lokale Netzwerk nach Geräten zu suchen.
- 5 Klicken Sie auf **Discover** (Ermitteln).

Um ein Gerät manuell hinzuzufügen, gehen Sie wie folgt vor:



**Abbildung 6. Gerät hinzufügen**

- 1 Klicken Sie auf die Option **Add A Device** (Gerät hinzufügen).
- 2 Geben Sie den Gerätenamen in das Feld **Name** ein.
- 3 Geben Sie die MAC-Adresse in das Feld **MAC address** (MAC-Adresse) ein.
- 4 Geben Sie die IP-Adresse in das Feld **IP Address** (IP-Adresse) ein.
- 5 Geben Sie die Mediengröße (in MB) des Geräts in das Feld **Media Size** (Mediengröße) ein.
- 6 Wählen Sie aus den Dropdown-Listen Ihre bevorzugten Optionen für **Operating System** (Betriebssystem) und **Platform** (Plattform) für das Gerät aus.
- 7 Geben Sie einen Wert für **Subnet** (Subnetz) ein und wählen Sie die IP-Adresse des Subnetzes aus der Autovervollständigen-Liste aus.

- 8 Klicken Sie auf **Add** (Hinzufügen).
- d Klicken Sie auf **Export** (Exportieren), um die Geräteliste im Format **.csv** oder **.txt** (mit Tabstopptrennzeichen) zu exportieren.
- e Klicken Sie auf **View Details** (Details anzeigen), um eine umfassende Übersicht sowie Status, Netzwerk, Hardware und Protokolle des ausgewählten Geräts anzuzeigen.
- **Overview** (Übersicht) – Stellt eine umfassende Übersicht über **System**, **Location** (Speicherort), **Capabilities** (Speicherort), **Network** (Netzwerk) und **Drives** (Laufwerke) des ausgewählten Geräts bereit.
  - **Status** – Zeigt Folgendes an:
    - Anwendungen, die installiert sind und auf dem System ausgeführt werden.
    - Prozessor- und Systemleistung.
    - Remote-Sitzung für die ausgewählten Geräte.
    - Angeschlossene USB-Geräte für ThinOS-Geräte.
  - **Network** (Netzwerk) – Stellt Details über **NIC card** (NIC-Karte) und **Network Details** (Netzwerkdetails) des ausgewählten Geräts bereit.
  - **Hardware** – Stellt Details über die folgenden Attribute bereit:
    - **Disks** (Festplatten): Zeigt die Anzahl der verfügbaren Partitionen auf dem Gerät und dessen Speichergröße an.
    - **Drives** (Laufwerke): Zeigt die Anzahl der Laufwerke und deren Speichergröße an.
    - **Systems** (Systeme): Zeigt die Hardware-bezogenen Details und angeschlossene Monitore für ThinOS-Geräte.
  - **Logs** (Protokolle) – Stellt Details über **Audit Trails** (Überwachungsprotokolle) und **Deployed Packages** (Bereitgestellte Pakete) des ausgewählten Geräts bereit.
- f Klicken Sie auf **Add/Modify Filter** (Filter hinzufügen/ändern), um die Seite „Devices“ (Geräte) nach Name, IP-Adresse, Betriebssystem, Plattform, letztem Einchecken und MAC-Adresse zu filtern. Verwenden Sie die folgenden Richtlinien:



**Abbildung 7. Filter hinzufügen/ändern**


- 1 Um die Seite „Devices“ (Geräte) nach dem Gerätenamen zu filtern, geben Sie den Gerätenamen in das Feld **Name** ein und klicken Sie dann auf **Update** (Aktualisieren).
 

**ANMERKUNG:** Verwenden Sie die Option **Partial Name of the device (Partieller Gerätename)**, wenn Sie nach einem Teil des Gerätenamens suchen möchten.
- 2 Um die Seite „Devices“ (Geräte) nach der IP-Adresse zu filtern, geben Sie die IP-Adresse des Geräts in das Feld **IP Address** (IP-Adresse) ein und klicken Sie dann auf **Update** (Aktualisieren).
- 3 Wählen Sie aus den Dropdown-Listen Ihre bevorzugten Optionen für **Operating System** (Betriebssystem) und **Platform** (Plattform) des Geräts aus, um die Seite „Devices“ (Geräte) nach dem Betriebssystem und der Plattform zu filtern.
- 4 Wählen Sie basierend auf Ihren Einstellungen entweder „After“ (Nach) oder „Between“ (Zwischen) aus der Dropdown-Liste **Last Check-in** (Letztes Einchecken) aus und geben Sie das Datum und die Uhrzeit, an dem das Gerät zuletzt eingetrickt war, im Format „MM/TT/JJJJ hh:mm“ an.
- 5 Geben Sie den Wert für **MAC address** (MAC-Adresse) des Geräts ein und klicken Sie auf **Update** (Aktualisieren), um die Seite „Devices“ (Geräte) nach der MAC-Adresse des Geräts zu filtern.
- 6 Geben Sie die **Number of Devices** (Anzahl der Geräte) ein, die auf einer Seite angezeigt werden sollen.
- 7 Klicken Sie auf **Reset** (Zurücksetzen), um den eingegebenen Wert zurückzusetzen.
- 8 Klicken Sie auf **Update** (Aktualisieren), um einen Filter zur Seite „Devices“ (Geräte) hinzuzufügen.
- 9 Fahren Sie mit dem Mauszeiger über das Filterattribut und klicken Sie dann auf das neben dem Filter angezeigte **x**-Symbol, um den angewendeten Filter zu entfernen.

Wählen Sie das bevorzugte Gerät aus, um folgende Echtzeitbefehle auszuführen:

- a Um ein Paket auf ein bestimmten Gerät zu übertragen, klicken Sie auf **Update** (Aktualisieren).
- b Um das ausgewählt Gerät neu zu starten, klicken Sie auf **Reboot Device** (Gerät neu starten).
- c Um das ausgewählte Gerät herunterzufahren oder anzuhalten, klicken Sie auf **Shutdown** (Herunterfahren).
- d Um eine Nachricht an das ausgewählte Gerät zu schicken, klicken Sie auf **Send Message** (Nachricht senden). Der Bildschirm **Send Message** (Nachricht senden) wird angezeigt.
  - 1 Wählen Sie die Optionsschaltfläche des bevorzugten Nachrichtentyps aus den angezeigten Optionen für den Nachrichtentyp aus. Es stehen folgende Nachrichtentypen zur Verfügung:
    - Informationen
    - Warnung
    - Kritisch
  - 2 Geben Sie den Titel der Nachricht in das Feld **Message Title** (Nachrichtentitel) ein.
  - 3 Geben Sie den Inhalt Ihrer Nachricht in das Feld **Message Body** (Nachrichtentext) ein.
  - 4 Klicken Sie auf die Schaltfläche **Send** (Senden), um Ihre Nachricht abzusenden.
- e Klicken Sie auf **More** (Mehr), um mehr Aufgaben ausführen. Sie können folgende Aufgaben ausführen:

**Table 4. Mehr**

Parameter	Beschreibung
Rename Device (Gerät umbenennen)	Geben Sie den aktualisierten Namen in das Feld <b>Rename Device</b> (Gerät umbenennen) ein.
Update Device Information (Geräteinformationen aktualisieren)	Geben Sie zum Aktualisieren der Geräteinformationen die entsprechenden Geräteinformationen ein. Geben Sie folgende Informationen ein, um die Geräteinformationen zu aktualisieren: <ul style="list-style-type: none"> <li>• Gerätestandort</li> <li>• Kontakt</li> <li>• Benutzerdefinierte Tags hinzufügen</li> </ul> Klicken Sie auf die Option <b>Update</b> (Aktualisieren), um die Geräteinformationen zu aktualisieren.
Execute Commands (Befehle ausführen)	Um die Befehle auszuführen, geben Sie den Befehl oder den Pfad in das Feld <b>Execute Commands</b> (Befehle ausführen) ein und klicken Sie zum Ausführen des eingegebenen Befehls auf die Option <b>Execute</b> (Ausführen).
Wake on LAN	Um die heruntergefahrenen Geräte über dasselbe Subnetz zu reaktivieren, in dem WDM installiert ist, klicken Sie auf <b>Wake on LAN</b> .
Relay Wake on LAN (Wake-On-LAN übertragen)	Um die Geräte über das Subnetz zu reaktivieren, klicken Sie auf <b>Relay Wake on LAN</b> (Wake-On-LAN übertragen).
Get Image (Image erstellen)	Geben Sie den Namen des Image und die zugehörigen Beschreibung in die entsprechenden Felder ein. Klicken Sie auf die <b>Compress Image</b> (Image komprimieren), um die Image-Komprimierung zu aktivieren. <div style="margin-top: 10px;"> <p> <b>ANMERKUNG: Durch die Komprimierung des Image wird die Verarbeitungszeit verlängert.</b></p> </div>
Protokolle ansehen	Verwenden Sie diese Option zum Anzeigen der Geräteprotokolle. Um ein eigenes Protokoll zu erstellen, klicken Sie auf die Schaltfläche <b>Create Log</b> (Protokoll erstellen), geben Sie den Namen für das Protokoll an und klicken Sie dann auf <b>Create</b> (Erstellen).
Include to PAD Repository (In PAD-Repository einbeziehen)	Um ein vom PAD-Repository ausgeschlossenes Gerät einzubeziehen, klicken Sie auf <b>Include</b> (Einbeziehen).

Parameter	Beschreibung
Exclude from PAD Repository (Von PAD-Repository ausschließen)	Um das Gerät vom PAD-Repository auszuschließen, klicken Sie auf <b>Exclude</b> (Ausschließen).
Löschen	Um ein Gerät aus der WDM-Datenbank zu löschen, klicken Sie auf <b>Force-delete</b> (Löschen erzwingen). Klicken Sie zum Löschen des Geräts durch Entfernen der Serverdetails aus dem Agent auf <b>Delete</b> (Löschen).
Remote Shadow (Remote-Spiegelung)	Verwenden Sie diese Option, um die Remote-Spiegelung Ihres Geräts zu aktivieren. Dies ermöglicht es, ein Gerät remote anzuzeigen und zu steuern (Shadowing eines Geräts).

Um die Gruppentypen zu verwalten, führen Sie den folgenden Vorgang durch:

## Manage Group Types

### Groups

G1	✎ 🗑

### Add value for G1

A1	✎ 🗑
A	✎ 🗑

Abbildung 8. Manage Group Types (Gruppentypen verwalten)

- 1 Klicken Sie auf die Option **All Devices** (Alle Geräte) und wählen Sie die Option **Manage Group Types** (Gruppentypen verwalten). Es wird die Seite **Manage Group Types** (Gruppentypen verwalten) angezeigt.
- 2 Geben Sie den Namen der benutzerdefinierten Gruppen in das Feld **Groups** (Gruppen) ein.
- 3 Klicken Sie auf die Option **Add** (Hinzufügen), um die ausgewählten benutzerdefinierten Gruppen hinzuzufügen.
- 4 Wählen Sie die hinzugefügte Gruppe aus der Liste aus und fügen Sie den Wert für die jeweilige Gruppe hinzu.
- 5 Klicken Sie auf die Option **Add** (Hinzufügen), um den Wert für die ausgewählte Gruppe hinzuzufügen.
- 6 Klicken Sie auf die Option **Save** (Speichern), um Ihre Änderungen zu speichern.

Um eine neue Ansicht zu erstellen, führen Sie folgenden Vorgang durch:

**Create View**

L1

Select group hierarchy

Search or add groups

- OS
- Image
- Subnet
- Platform
- VendorID
- Location
- Custom1
- Custom2
- Custom3
- TimeZone
- G1**

[ G1 ]

Private View

Off

Save Cancel

**Abbildung 9. Create View (Ansicht erstellen)**

- 1 Klicken Sie auf die Option **All Devices** (Alle Geräte) und wählen Sie die Option **Create View** (Ansicht erstellen). Es wird die Seite **Create View** (Ansicht erstellen) angezeigt.
- 2 Geben Sie den Namen der Ansicht in das Feld **New view** (Neue Ansicht) ein.
- 3 Wählen Sie die auf der linken Seite des Bildschirms angezeigten Gruppen in der Reihenfolge der bevorzugten Hierarchie aus.

**ANMERKUNG:** Klicken Sie zum Hinzufügen einer benutzerdefinierten Gruppe auf die Option **+ Add custom group** (Benutzerdefinierte Gruppe hinzufügen). Geben Sie den Namen der Gruppe an und aktivieren Sie das Kontrollkästchen, um die benutzerdefinierte Gruppe der Liste der Gruppenhierarchie hinzuzufügen. Sie können die Reihenfolge der ausgewählten Hierarchiegruppen anzeigen.

- 4 Klicken Sie auf die Schaltfläche **ON/OFF** (EIN/AUS), um die Option **Private View** (Private Ansicht) zu aktivieren oder zu deaktivieren.
- 5 Klicken Sie auf die Option **Save** (Speichern), um Ihre Änderungen zu speichern.

Um einer benutzerdefinierten Gruppe ein Gerät zuzuweisen, gehen Sie wie folgt vor:

- 1 Klicken Sie auf **All devices** (Alle Geräte) und wählen Sie die erstellte benutzerdefinierte Ansicht aus.
- 2 Klicken Sie auf **Unassigned** (Nicht zugewiesen).
- 3 Wählen Sie ein Gerät aus und klicken Sie dann auf **Assign Group** (Gruppe zuweisen).

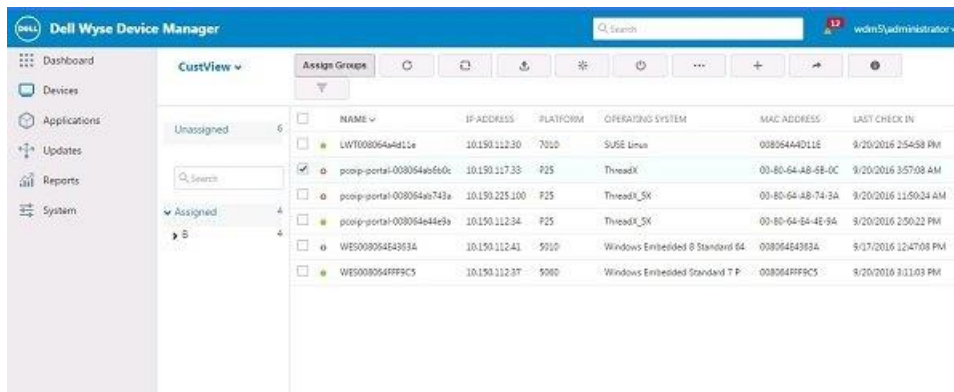


Abbildung 10. Assign Group (Gruppe zuweisen)

- 4 Wählen Sie den Gruppenwert aus, den Sie dem Gerät zuweisen möchten.

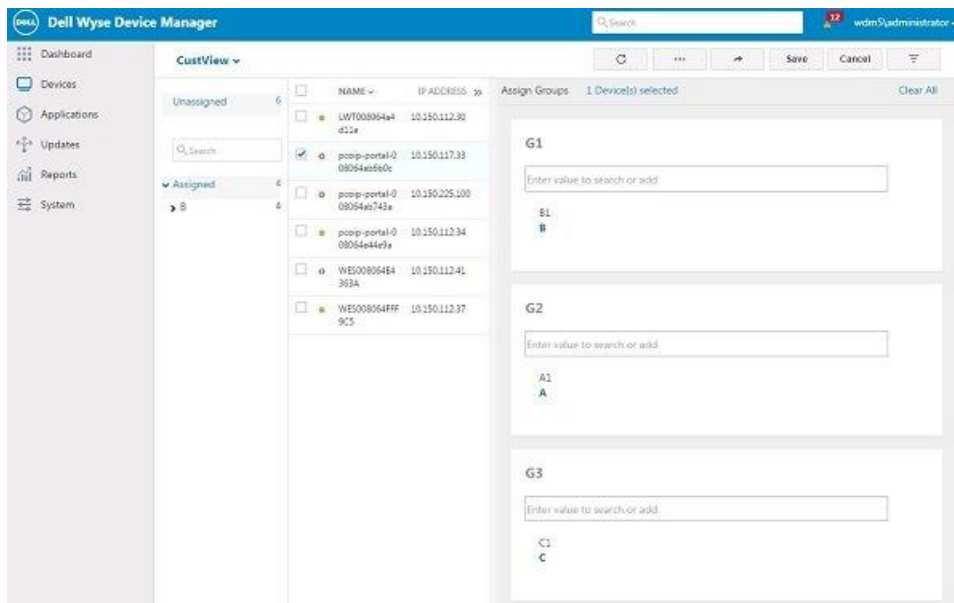


Abbildung 11. Assign Group (Gruppe zuweisen)

- 5 Klicken Sie auf **Save** (Speichern).

# Anwendungen

Auf der Seite „Applications“ (Anwendungen) können Sie folgende Aufgaben durchführen:

- Pakete im WDM-Master-Repository registrieren.
- Ein Paket für die Geräte bereitstellen.
- Die Paket-Images und/oder Konfigurationspakete, die Sie registrieren oder von den Geräten in Ihrem Netzwerk erstellen oder abrufen, manuell registrieren (zur Verteilung an andere Geräte).
- Vorregistrierte WDM Agent- und Boot Agent-Pakete aktualisieren.
- Pakete in funktionale Kategorien einteilen und Pakete an ausgewählte Geräte verteilen (sofort oder anhand eines Zeitplans).

Standardmäßig bietet WDM einige Standardpakete, die für die Geräte bereitgestellt werden können. Diese Pakete sind in fünf Kategorien unterteilt:

- Agent-Aktualisierung
- Gerätekonfiguration
- Images
- Other Packages (Andere Pakete)
- PCoIP Device Configuration (PCoIP-Gerätekonfiguration)
- **Agent Update** (Agent-Aktualisierung) – Die Seite „Agent Update“ (Agent-Aktualisierung) dient zum Anzeigen der Liste verfügbarer Agent-Pakete. Es werden die Beschreibungen der einzelnen Agent-Pakete sowie detaillierte Informationen zu den jeweiligen Betriebssystemen angezeigt, unter denen diese Pakete registriert werden können.

NAME	DESCRIPTION	OPERATING SYSTEM	CREATED AT
SUSELXHAgentUpgrade	SLETC HAgent Supported: SLED12(Ver-4.2.0), SLED11SP3(Ver-5.5.38), SLED11SP2(Ver-5.3.07)	SUSE Linux	2018-04-02 09:20:02.713
ThinLXHAgentUpgrade	SLETC HAgent Supported: SLED12 (Ver-5.4.47)	ThinLinux	2018-04-02 09:20:02.887
ThinLXHAgentUpgrade2	SLETC HAgent Supported: SLED12 (Ver-5.4.54)	Thin Linux 2.0	2018-04-02 09:20:08.190
UbuntuHAgentUpgrade	Ubuntu Linux HAgent Upgrade (Ver-5.0.39)	Wyse Enhanced Ubuntu Linux	2014-07-31 12:00:00.200
WES8WDAgentUpgrade	WES8 WDAgent Upgrade (Ver-14.1.1.3)	Windows Embedded 8 Standard 64	2018-04-02 09:20:09.663
WES7PWDAgentUpgrade	WES7P WDAgent Upgrade (Ver-14.1.1.3)	Windows Embedded Standard 7 P	2018-04-02 09:20:09.453
WES7WDAgentUpgrade	WES7 WDAgent Upgrade (Ver-14.1.1.3)	Windows Embedded Standard 7	2018-04-02 09:20:09.323
WIE10WDAgentUpgrade	WIE10 WDAgent Upgrade (Ver-14.1.1.3)	Windows 10 IoT Enterprise	2018-04-02 09:20:09.790

Abbildung 12. Agenten

- **SUSELXHAgentUpgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen ein SUSE Linux-BS ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent-Version auf die in WDM integrierte HAgent-Version zu aktualisieren.
- **ThinLXHAgentUpgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen ein Thin SE Linux-BS ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent-Version auf die in WDM integrierte HAgent-Version zu aktualisieren.

- **ThinLXHAgentUpgrade2** – Dieses Paket kann nur für Geräte geplant werden, auf denen ein Thin Linux-BS 2.0 ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent-Version auf die in WDM integrierte HAgent-Version zu aktualisieren.
- **UbuntuHAgent Upgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen das Wyse Enhanced Ubuntu Linux-BS ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent-Version auf die in WDM integrierte HAgent-Version zu aktualisieren.
- **WE8SWDAAgentUpgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen das Windows Embedded 8 Standard 64-Bit-Betriebssystem ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent- und WDA-Version auf die in WDM integrierte WDA-Version zu aktualisieren.
- **WES7WDAAgentUpgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen das WES7-BS ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent- und WDA-Version auf die in WDM integrierte WDA-Version zu aktualisieren.
- **WES7PWDAAgentUpgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen das WES7P-BS ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent- und WDA-Version auf die in WDM integrierte WDA-Version zu aktualisieren.
- **WESHAgentUpgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen das WES-BS ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent-Version auf die in WDM integrierte HAgent-Version zu aktualisieren.
- **WIE10WDAAgentUpgrade** – Dieses Paket kann nur für Geräte geplant werden, auf denen das WIE10-BS ausgeführt wird. Dieses Paket kann dazu verwendet werden, die vorhandene HAgent- und WDA-Version auf die in WDM integrierte WDA-Version zu aktualisieren.

**Tabelle 5. Agenten-Aktualisierung**

Parameter	Beschreibung
Name	Zeigt den Namen der Pakete an.
Beschreibung	Zeigt die Beschreibung des Pakets an.
Betriebssystem	Zeigt das Betriebssystem der registrierten Pakete an.
Created At (Erstellt am)	Zeigt das Datum und die Zeit der Paketerstellung an.

- **Device Configuration** (Agenten-Aktualisierung) – Die Seite „Device Configuration“ (Gerätekonfiguration) wird zum Erstellen und Registrieren von neuen Anwendungskonfigurationspaketen verwendet.

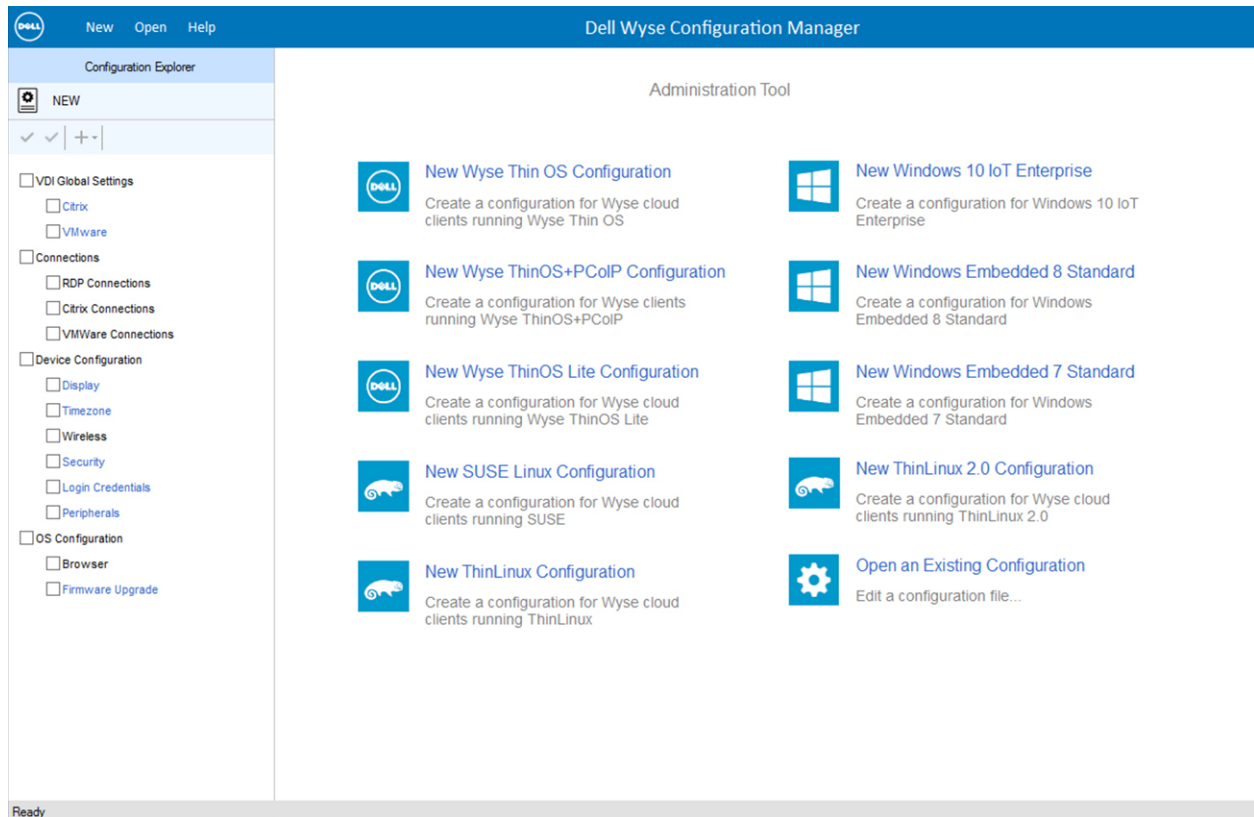


Abbildung 13. Gerätekonfiguration

- a Um die WCM-Anwendung zu starten, klicken Sie auf die Option **Create Package** (Paket erstellen) oder auf das Symbol **+**. Das Fenster **Register Configuration** (Konfiguration registrieren) wird angezeigt. Es enthält Optionen zum Herunterladen und Konfigurieren der Wyse Configuration Manager-Anwendungen.
- b Klicken Sie auf **Configure Wyse Configuration Manager** (Wyse Configuration Manager konfigurieren). Die WCM-Dienstprogramm-Datei wird heruntergeladen.
- c Speichern Sie die WCM-Datei. Die Datei wird als **CustomProtocolforWCM.exe** heruntergeladen.
- d Führen Sie die Datei als Administrator aus.
- e Klicken Sie auf **Create Package** (Paket erstellen). Das Fenster **Dell Wyse Configuration Manager** wird angezeigt.
- f Erstellen Sie die Gerätekonfigurationen mithilfe der GUI der WCM-Anwendung, indem Sie die erforderlichen Konfigurationen auswählen, aktualisieren und speichern. Die Konfigurationspakete werden im WDM-Repository gespeichert und im rechten Fensterbereich der WDM-Konsole angezeigt, wenn Sie den Knoten **Device Configuration** (Gerätekonfiguration) auswählen.

Weitere Informationen zum Erstellen von WCM-Konfigurationen finden Sie im *Administratorhandbuch für den Dell Wyse Configuration Manager*.

- **Images** – Die Seite „Images“ wird zum Anzeigen der Liste der registrierten Image-Pakete verwendet. Es werden Beschreibungen der einzelnen Image-Pakete sowie detaillierte Informationen zu dem jeweiligen Betriebssystem, Image-Typ und zur Größe des Pakets angezeigt. Die registrierten und importierten Image-Pakete werden auf der Seite „Images“ angezeigt.

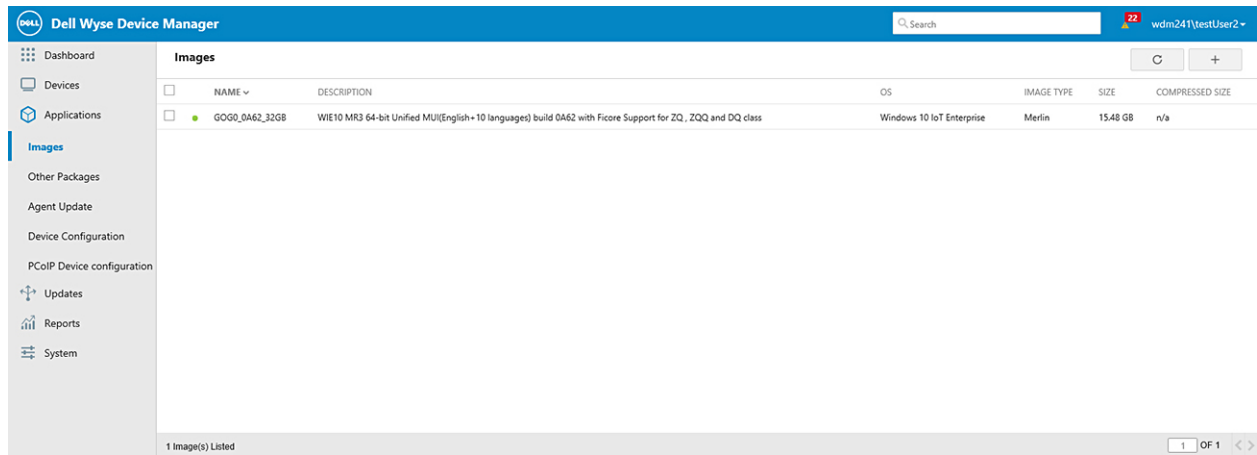


Abbildung 14. Images

Tabelle 6. Images

Parameter	Beschreibung
Name	Zeigt den Namen der Pakete an.
Beschreibung	Zeigt die Version der Pakete an.
Betriebssystem	Zeigt das Betriebssystem des registrierten Pakets an.
Image Type (Image-Typ)	Zeigt den Image-Typ für die Pakete an.
Größe	Zeigt die Größe des Images an.
Compressed Size (Komprimierte Größe)	Zeigt die komprimierte Image-Größe an.

• **Other Packages** (Andere Pakete) – Die Seite „Other Packages“ (Andere Pakete) wird zum Anzeigen der Liste von AgentUpgrade-Paketen und anderen Paketen verwendet. Es werden Beschreibungen für die einzelnen AgentUpgrade-Pakete sowie andere Pakete mit dem zugehörigen Betriebssystem angezeigt, unter dem diese Pakete registriert sind. Die Kategorie „Other Package“ (Anderes Paket) verfügt standardmäßig über Pakete für die Aktualisierung des Boot Agent für alle Betriebssysteme. Hier sind auch die standardmäßigen Pakete für das Neustarten, Herunterfahren sowie die Wake-On-LAN- und ResetOSsetting-Pakete enthalten.

NAME	DESCRIPTION	OPERATING SYSTEM	CREATED AT
BootAgentUpgradeLinux	Boot Agent Upgrade for SLETC SPL/SP2 (3.3.9)	SUSE Linux	2016-07-31 12:00:00.200
BootAgentUpgradeThinLinux	Boot Agent Upgrade for ThinLinux (3.3.9)	ThinLinux	2016-07-31 12:00:00.200
BootAgentUpgradeWE8S	Boot Agent Upgrade for WE8S (Ver-3.3.9)	Windows Embedded 8 Standard 64	2016-07-31 12:00:00.200
BootAgentUpgradeWE8Sx	Boot Agent Upgrade for WE8Sx (Ver-3.3.9)	Windows Embedded 8 Standard 32	2016-07-31 12:00:00.200
BootAgentUpgradeWE7	Boot Agent Upgrade for WE7 (Ver-3.3.9)	Windows Embedded Standard 7	2016-07-31 12:00:00.200
BootAgentUpgradeWE7P	Boot Agent Upgrade for WE7P (Ver-3.3.9)	Windows Embedded Standard 7 P	2016-07-31 12:00:00.200
BootAgentUpgradeWIE10	Boot Agent Upgrade for WIE10 (Ver-3.3.9)	Windows 10 IoT Enterprise	2016-07-31 12:00:00.200
PADService_SysprepScript_WE8S	PADService_SysprepScript_WE8S	Windows Embedded 8 Standard 64	2016-09-16 08:56:48.373
Reboot	Device Reboot	ALL	2011-12-19 12:50:16.970
ResetOSSettings	Resets OS configuration to factory default	ALL	2013-10-29 16:08:57.000
Shutdown	Device Shutdown	ALL	2011-12-19 12:50:17.093
WakeOnLAN	Device WOL	ALL	2011-12-19 12:50:17.017

Abbildung 15. Other Packages (Andere Pakete)

- **BootAgentUpgradeLinux** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein SUSE Linux Enterprise-BS ausgeführt wird.
- **BootAgentUpgradeThinLinux** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein ThinLinux-BS ausgeführt wird.
- **BootAgentUpgradeThinLinux2** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein ThinLinux 2.0-BS ausgeführt wird.
- **BootAgentUpgradeWE8S** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein Windows Embedded Standard 8-BS (64 Bit) ausgeführt wird.
- **BootAgentUpgradeWE8Sx** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein Windows Embedded Standard 8-BS (32 Bit) ausgeführt wird.
- **BootAgentUpgradeWE7** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein Windows Embedded Standard 7-BS ausgeführt wird.
- **BootAgentUpgradeWE7P** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein Windows Embedded Standard 7P-BS ausgeführt wird.
- **BootAgentUpgradeWIE10** – Zur Aktualisierung des Boot Agent für ein Gerät, auf dem ein Windows 10 IoT Enterprise-BS ausgeführt wird.
- **Reboot** (Neustart) – Wenn diese Option für ein Gerät geplant ist, wird das Gerät neu gestartet.
- **ResetOSSettings** – Damit wird die BS-Konfiguration des Geräts auf die Werkseinstellungen zurückgesetzt.
- **Shutdown** (Herunterfahren) – Wenn diese Option für ein Gerät geplant ist, wird das Gerät heruntergefahren.
- **WakeOnLAN** – Wenn diese Option für ein Gerät geplant ist, wird der WOL-Befehl an das Gerät gesendet.

Tabelle 7. Other Packages (Andere Pakete)

Parameter	Beschreibung
Name	Zeigt den Namen der Pakete an.
Beschreibung	Zeigt die Beschreibung des Pakets an.
Betriebssystem	Zeigt das Betriebssystem der registrierten Pakete an.
Created At (Erstellt am)	Zeigt das Datum und die Zeit der Paketerstellung an.

• **PCoIP Device Configuration** (PCoIP-Gerätekonfiguration) – Die Seite „PCoIP Device Configuration“ (PCoIP-Gerätekonfiguration) dient zum Anzeigen der Liste der PCoIP-Gerätepakete. Es werden Beschreibungen für die einzelnen PCoIP-Gerätepakete mit den zugehörigen Betriebssystemen angezeigt. Das registrierte PCoIP-Konfigurationspaket wird unter „PCoIP Device Configuration“ (PCoIP-Gerätekonfiguration) angezeigt.

Die als Standard verfügbaren Pakete gelten nur für die ThreadX 4.x-Firmware.

- ThreadX: Die Pakete gehören zur ThreadX 4.x-Firmware.
- ThreadX\_5x: Die Pakete gehören zur ThreadX 5.x-Firmware.

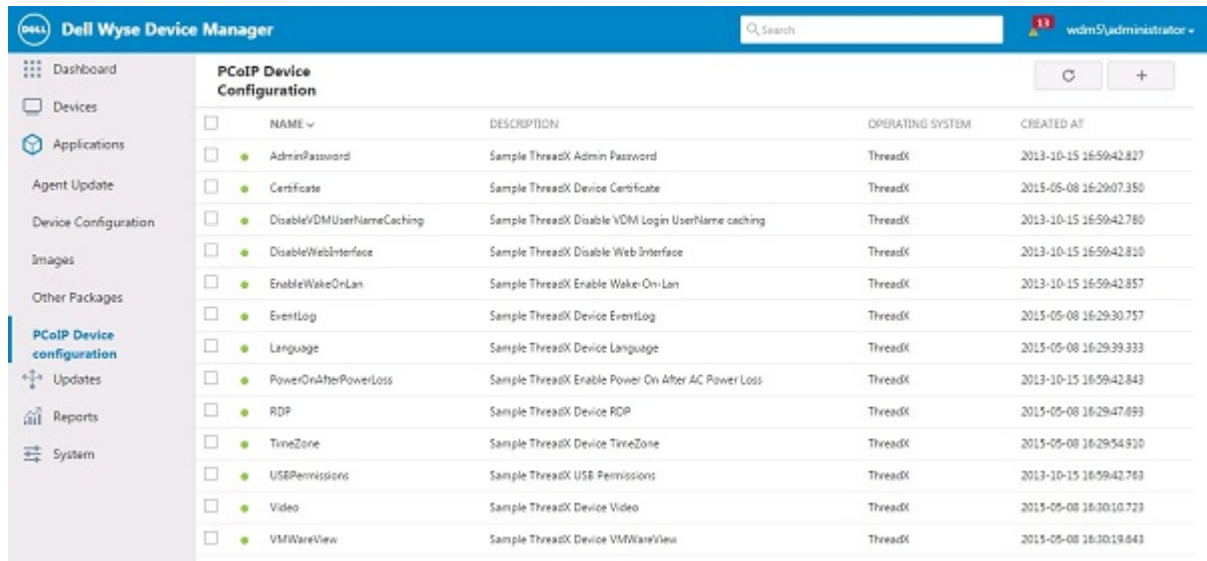


Abbildung 16. PCoIP Device Configuration (PCoIP-Gerätekonfiguration)

- **AdminPassword** – Sample-Paket zum Ändern des Administratorkennworts für ThreadX-Geräte.
- **Certification** – Sample-Paket zum Ändern des Gerätezertifikats für ThreadX-Geräte.
- **DisableVDMUserNameCaching** – Sample-Paket zum Deaktivieren des Zwischenspeicherns von VDM-Anmeldebenutzernamen für ThreadX-Geräte.
- **DisableWebInterface** – Sample-Paket zum Deaktivieren der Webschnittstelle für ThreadX-Geräte.
- **EnableWakeOnLAN** – Sample-Paket zum Aktivieren der WakeOnLAN-Funktion für ThreadX-Geräte.
- **EventLog** – Sample-Paket für die Ereignisprotokollierung für ThreadX-Geräte.
- **Language** – Sample-Paket zum Ändern der Sprachenkonfiguration für ThreadX-Geräte.
- **PowerOnAfterPowerLoss** – Sample-Paket zum Aktivieren des Einschaltvorgang nach einem Stromausfall auf ThreadX-Geräten.
- **RDP** – Sample-Paket zum Ändern des RDP-Konfiguration für ThreadX-Geräte.
- **TimeZone** – Sample-Paket zum Ändern der Zeitzonekonfiguration für ThreadX-Geräte.
- **USBPermissions** – Sample-Paket zum Konfigurieren der USB-Berechtigungen für ThreadX-Geräte.
- **Video** – Sample-Paket zum Ändern der Videokonfiguration für ThreadX-Geräte.
- **VMWareView** – Sample-Paket zum Ändern der VMware View-Konfiguration für ThreadX-Geräte.

Tabelle 8. PCoIP Device Configuration (PCoIP-Gerätekonfiguration)

Parameter	Beschreibung
Name	Zeigt den Namen der Pakete an.
Beschreibung	Zeigt die Version der Pakete an.
Betriebssystem	Zeigt das Betriebssystem der registrierten Pakete an.
Created At (Erstellt am)	Zeigt das Datum und die Zeit der Paketerstellung an.

#### Allgemeine Optionen für die Konfiguration von Paketen/Images

- 1 Wählen Sie ein beliebiges Paket/Image aus.

Die Optionen für die Ausführung der Aufgaben sind in der rechten oberen Ecke des Bildschirms aufgeführt.

- a Klicken Sie auf die Option **Update** (Aktualisierung), um das ausgewählte Paket/Image zu aktualisieren.
  - 1 Wählen Sie das bevorzugte Paket aus der Liste der Anwendungen.
  - 2 Klicken Sie auf die Aktualisierungsoption oben auf dem Bildschirm.
  - 3 Wählen Sie aus der Dropdown-Liste **Select View** (Ansicht auswählen) Ihre bevorzugte Ansicht aus.

**ANMERKUNG:** Die Paketverteilung ist der Massenbereitstellungsvorgang auf der Registerkarte „Application“ (Anwendung). Sie können kein einzelnes Gerät für die Bereitstellung eines Pakets auswählen. Das ausgewählte Paket wird für die ganze ausgewählte Ansicht bereitgestellt.

- 4 Planen Sie die Paketverteilung basierend auf Ihren Einstellungen. Sie können ein Paket auf folgende Arten verteilen:
  - Wenn Sie die Option **One time distribution** (Einmalige Verteilung) auswählen, geben Sie die entsprechenden Informationen zur Paketverteilung ein. Wählen Sie die Option **Now** (Jetzt), wenn Sie das Paket jetzt verteilen möchten, oder wählen Sie die Option **A specific date and time** (Bestimmtes Datum und Uhrzeit) und geben Sie das gewünschte Datum und die gewünschte Uhrzeit für die Paketverteilung ein. Klicken Sie auf die Option **On/Off** (Ein/Aus), um die Option **Retry failed updates** (Fehlgeschlagene Aktualisierungen wiederholen) zu aktivieren bzw. zu deaktivieren.
  - Wenn Sie die Option **Recurring distribution** (Wiederkehrende Verteilung) auswählen, geben Sie die folgenden Paketverteilungsdetails ein:
    - 1 Geben Sie den Namen für den Wiederholungsplaner ein.
    - 2 Wählen Sie in der Dropdown-Liste **Recur** (Wiederholen) den Tag für die Paketverteilung aus.
    - 3 Geben Sie das Start- und Enddatum der Paketverteilung ein.
    - 4 Geben Sie die Zeitdauer der Paketverteilung ein.
- 5 Klicken Sie auf die Option **Save** (Speichern) oben auf dem Bildschirm, um Ihre Änderungen zu speichern.
- b Klicken Sie auf die Option **Disable Distribution** (Verteilung deaktivieren), um die Verteilung des Pakets zu deaktivieren.
- c Klicken Sie auf die Option **Package Script** (Paket-Skript), um das Skript des ausgewählten Pakets anzuzeigen oder zu exportieren.

Weitere Informationen finden Sie unter [Exportieren des Paket-Skripts eines registrierten Pakets](#) und [Bearbeiten des Paket-Skripts eines registrierten Pakets](#).

- d Klicken Sie auf die Option **Refresh** (Aktualisieren), um die Seite zu aktualisieren.
- e Die Option **Register Package** (Paket registrieren) wird verwendet, um ein Paket zu registrieren.
  - 1 Klicken Sie auf die Option **Register Package** (Paket registrieren), um das Utility für die Paketregistrierung herunterzuladen. Das Dialogfeld „WDM Package Registration Utility“ (Utility für WDM-Paketregistrierung) wird angezeigt.
  - 2 Geben Sie die WDM-Serveradresse und Anmeldeinformationen in die Felder „WDM Server“ (WDM-Server) „Username“ (Benutzername) und Password (Kennwort) ein.
  - 3 Klicken Sie auf die Option **On/Off** (Ein/Aus), um die Option **Save credentials (encrypted)** (Anmeldeinformationen speichern (verschlüsselt)) zu aktivieren bzw. zu deaktivieren.
  - 4 Im Dialogfeld „Package Registration Utility“ (Utility für Paketregistrierung) können zwei Arten von Paketen registriert werden:
    - **Register RSP** (RSP registrieren): Ermöglicht die Auswahl eines .rsp-Pakets und das Hochladen des Pakets auf dem WDM-Server. Weitere Informationen finden Sie unter [Registrieren eines Pakets aus einer Skriptdatei \(.RSP\)](#).
    - **Register EXE** (EXE registrieren): Ermöglicht die Auswahl einer .exe-, .msi-, .msu- oder .bat-Datei und das Hochladen dieser auf dem WDM-Server. Weitere Informationen finden Sie unter [Registrieren eines Pakets zum Installieren einer Datei. \(nur .exe-, .msi-, .msu-, und .bat-Dateien\)](#).
- 5 Klicken Sie auf **Upload** (Hochladen).
- f **(Diese Option gilt nur für Images.)** Klicken Sie auf **Deploy via peers** (Verteilung über Peers), um ein Paket für ein Gerät bereitzustellen. Führen Sie zum Bereitstellen eines Pakets für ein Gerät die folgenden Aufgaben durch:
  - 1 Wählen Sie aus der Dropdown-Liste Ihre bevorzugte Plattform.
  - 2 Geben Sie das Startdatum, Enddatum und die Zeit im Format hh:mm:ss ein, um eine Verteilung zu planen.
  - 3 Geben Sie die Subnetz-IP-Adresse ein, um ein verfügbares Subnetz auszuwählen.

**ANMERKUNG:** Zum Erstellen eines PAD-Zeitplans muss mindestens ein Subnetz ausgewählt werden.

- 4 Klicken Sie auf **Deploy** (Bereitstellen).

Themen:

- Bearbeiten des Paket-Skripts eines registrierten Pakets
- Exportieren des Paket-Skripts eines registrierten Pakets
- Registrieren eines Pakets über eine Skriptdatei – .RSP
- Ein Paket registrieren – nur .exe-, .msi-, .msu- und .bat-Dateien
- PColP-Gerätekonfiguration

## Bearbeiten des Paket-Skripts eines registrierten Pakets

So zeigen Sie die Eigenschaften eines Softwarepakets an:

- 1 Klicken Sie auf die Option **Package Script (Paket-Skript)**.

Das Fenster „Package Script“ (Paket-Skript) wird angezeigt.

- 2 Klicken Sie auf die Option **Edit (Bearbeiten)**, um das Skript zu bearbeiten.
- 3 Klicken Sie auf **Save (Speichern)**.

**ⓘ ANMERKUNG:** Bei Standardpaketen können Sie das Skript nicht ändern. Dies gilt nur für benutzerdefinierte Pakete.

## Exportieren des Paket-Skripts eines registrierten Pakets

So exportieren Sie das Paket-Skript eines registrierten Softwarepakets:

- 1 Klicken Sie auf die Option **Package Script (Paket-Skript)**. Das Fenster „Package Script“ (Paket-Skript) wird angezeigt.
- 2 Wählen Sie die Option **Export (Exportieren)** aus, um das Paket-Skript zu exportieren.
- 3 Navigieren Sie zum Pfad, an dem das Skript gespeichert werden soll, und klicken Sie zum Speichern auf die Schaltfläche **OK**.
- 4 Das Bestätigungsfenster wird angezeigt. Klicken Sie auf **OK**, um das Skript unter dem angegebenen Speicherort zu speichern.

## Registrieren eines Pakets über eine Skriptdatei – .RSP

So registrieren Sie ein .rsp-Softwarepaket:

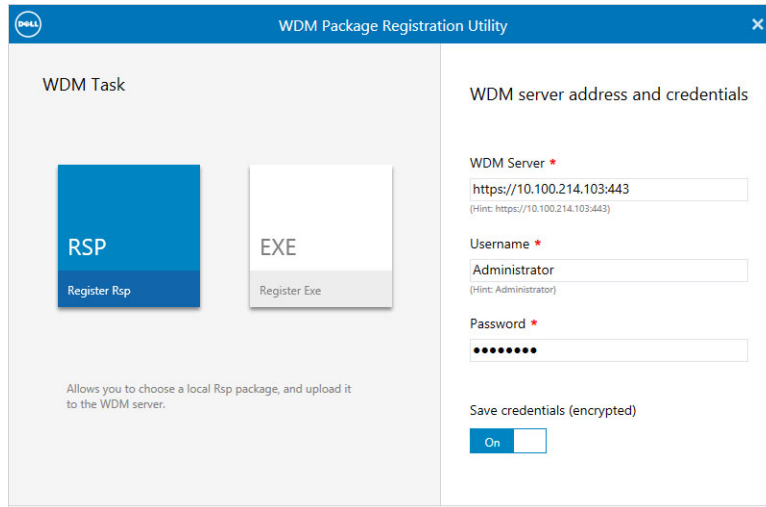


Abbildung 17. .rsp registrieren

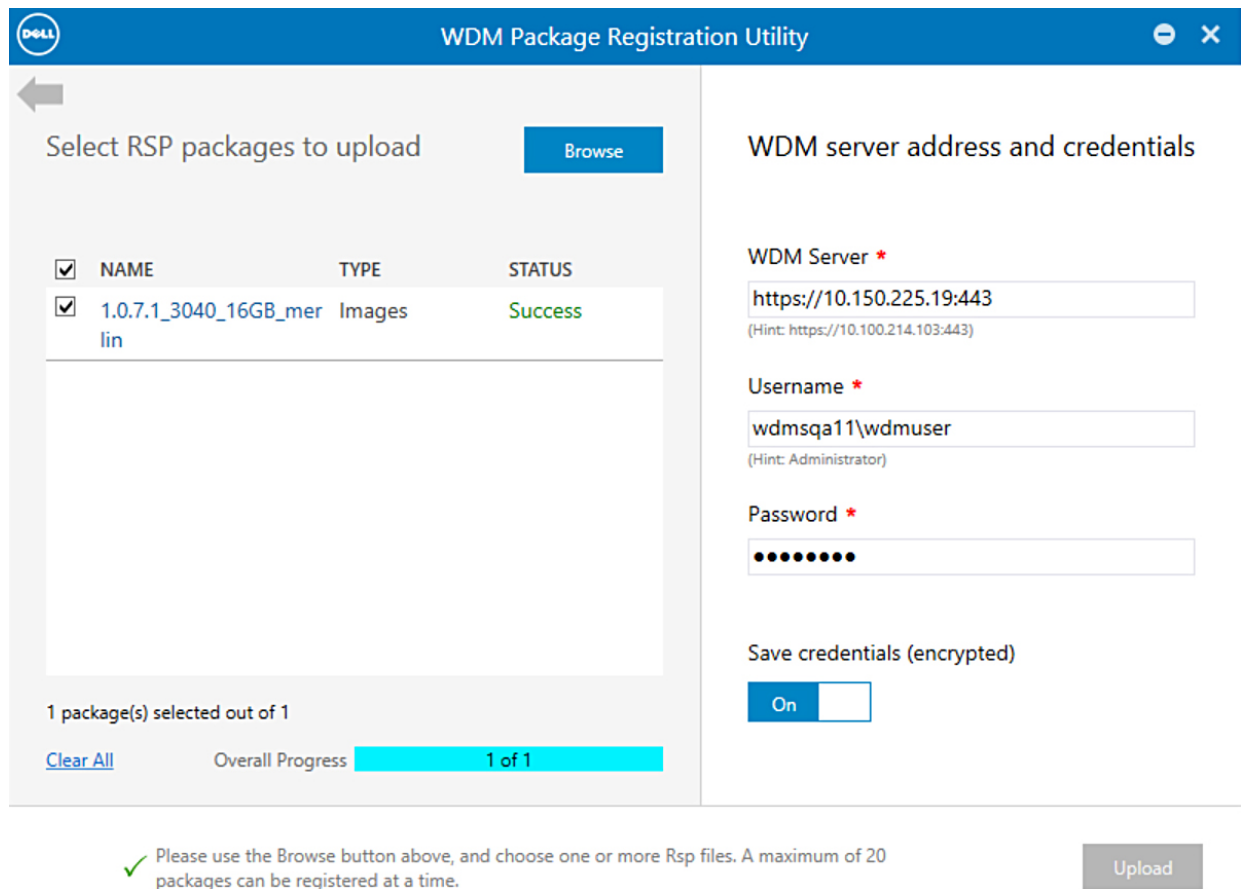


Abbildung 18. WDM-Paketregistrierung

1. Laden Sie es herunter und öffnen Sie das Dialogfeld „Package Registration Utility“ (Utility zur Paketregistrierung).
2. Klicken Sie auf die Kachel **RSP**, die im Dialogfeld „WDM Package Registration Utility“ (WDM-Utility zur Paketregistrierung) angezeigt wird.
3. Navigieren Sie zur hochzuladenden .rsp-Datei bzw. zum hochzuladenden Paket. Maximal 20 Pakete können auf einmal hochgeladen werden.

Die folgenden Details des .rsp-Pakets werden angezeigt.

- Name
- Typ
- Status

Wenn Sie den Mauszeiger auf den Namen des Pakets bewegen, wird eine Quickinfo mit den folgenden Informationen angezeigt:

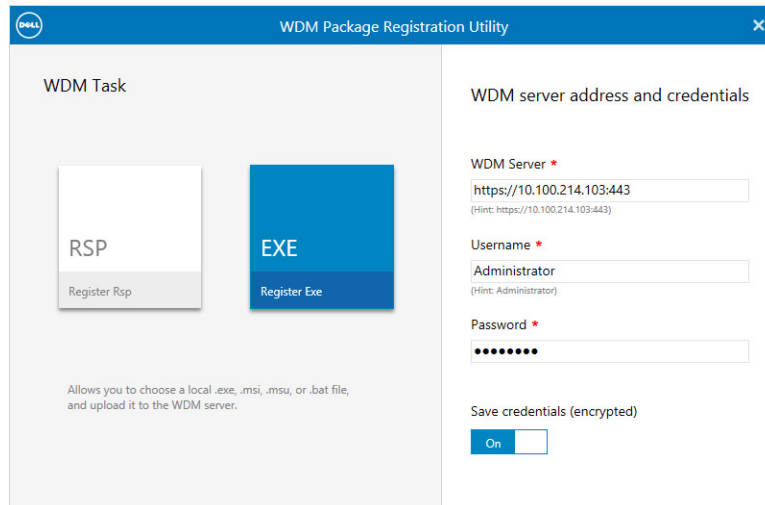
- Paketpfad
- OS
- Beschreibung
- Image-Größe

4 Klicken Sie auf **Upload** (Hochladen).

Nachdem der Hochladevorgang abgeschlossen ist, wird der Status in **Success** (Erfolg) geändert.

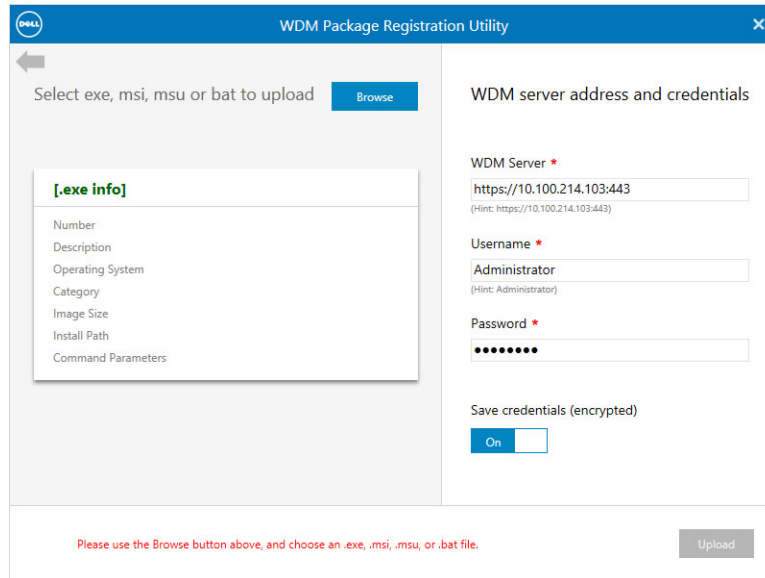
## Ein Paket registrieren – nur .exe-, .msi-, .msu- und .bat-Dateien

So registrieren Sie ein Paket:



The screenshot shows the 'WDM Package Registration Utility' window. It is divided into two main sections. The left section, titled 'WDM Task', contains two buttons: 'Register Rsp' (white) and 'Register Exe' (blue). Below these buttons is a note: 'Allows you to choose a local .exe, .msi, .msu, or .bat file, and upload it to the WDM server.' The right section, titled 'WDM server address and credentials', contains three input fields: 'WDM Server' with the value 'https://10.100.214.103:443' and a hint '(Hint: https://10.100.214.103:443)'; 'Username' with the value 'Administrator' and a hint '(Hint: Administrator)'; and 'Password' with a masked field of ten dots. At the bottom of this section is a checkbox labeled 'Save credentials (encrypted)' which is currently checked and labeled 'On'.

Abbildung 19. Utility für WDM-Paketregistrierung



**Abbildung 20. Utility für WDM-Paketregistrierung**

- 1 Laden Sie es herunter und öffnen Sie das Dialogfeld „Package Registration Utility“ (Utility zur Paketregistrierung).
- 2 Klicken Sie auf die Kachel **EXE**, die im Dialogfeld „WDM Package Registration Utility“ (WDM-Utility zur Paketregistrierung) angezeigt wird.
- 3 Navigieren Sie nur zu den .exe-, .msi-, .msu- und .bat-Dateien oder zum Paket, das Sie hochladen möchten. Die folgenden Details des ausgewählten Pakets werden angezeigt.
  - Name
  - Beschreibung
  - Betriebssystem
  - Kategorie
  - Image Size (Image-Größe)
  - Install Path (Installationspfad)
  - Befehlsparameter
- 4 Wählen Sie aus der Dropdown-Liste „Operating System“ (Betriebssystem) das Betriebssystem aus.
- 5 Geben Sie einen gültigen Thin Client-Pfad für die Installation des Pakets in das entsprechende Feld ein.
- 6 Geben Sie die Befehlsparameter in das entsprechende Feld ein.
- 7 Klicken Sie auf **Upload** (Hochladen).

## PCoIP-Gerätekonfiguration

Verwenden Sie die Seite **PCoIP device configuration** (PCoIP-Gerätekonfiguration), um neue PCoIP-Gerätekonfigurationspakete zu erstellen und bereitzustellen.

Um ein neues PCoIP-Gerätekonfigurationspaket zu erstellen, gehen Sie wie folgt vor:

- 1 Klicken Sie auf die Option **Register PCoIP Package** (PCoIP-Paket registrieren), um das Utility für die PCoIP-Gerätekonfiguration herunterzuladen.

Auf dem Bildschirm werden folgende Menüoptionen angezeigt:

- Klicken Sie oben rechts auf der Seite auf eine der folgenden ThreadX-Versionen, für den Sie eines PCoIP-Gerätekonfigurationspaket erstellen möchten:
  - Version 4.X

- Version 5.X
- Geben Sie den Paketnamen und Details zur Beschreibung in die Felder **Package Name** (Paketname) und **Description** (Beschreibung).
- **System**

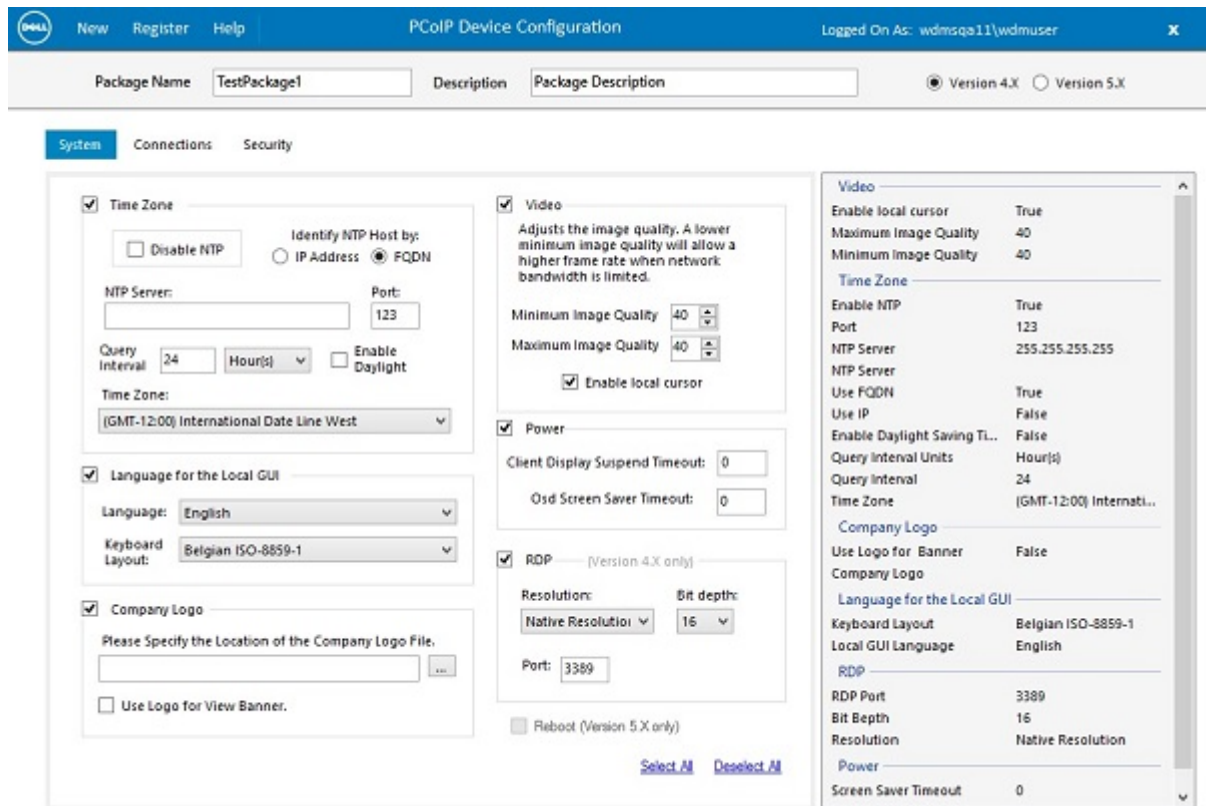


Abbildung 21. System Version 4.X

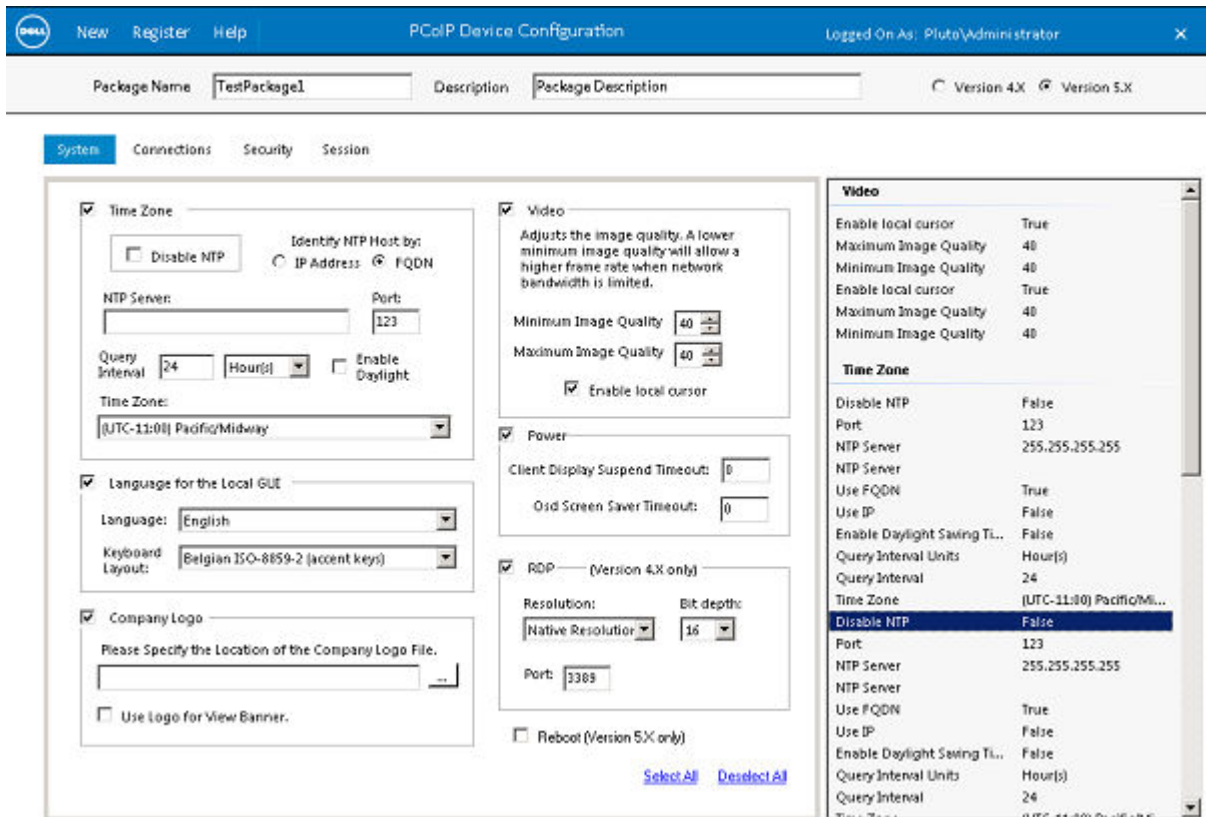


Abbildung 22. System Version 5.X

Tabelle 9. System

<p><b>Time Zone Configuration (Konfiguration der Zeitzone)</b></p>	<p>Geben Sie die folgenden Details ein:</p> <ul style="list-style-type: none"> <li>– Wählen Sie den Modus aus, über den der NTP-Host (Network Time Protocol) identifiziert werden soll.</li> <li>– Geben Sie die IP-Adresse oder den Hostnamen des NTP-Servers ein.</li> <li>– Geben Sie die Portnummer ein, das Abfrageintervall in Minuten und wählen Sie <b>Enable Daylight Saving Time</b> (Sommerzeit aktivieren) aus, sofern dies auf die von Ihnen ausgewählte Zeitzone zutrifft.</li> <li>– Wählen Sie die gewünschte Zeitzone aus der Dropdown-Liste aus.</li> </ul>
<p><b>Language for the Local GUI (Sprache für die lokale GUI)</b></p>	<p>Geben Sie Details zur lokalen Sprache und Tastatur für die lokalisierte GUI ein.</p>
<p><b>Company Logo (Firmenlogo)</b></p>	<p>Wählen Sie diese Option zum Hinzufügen des Firmenlogos. Navigieren Sie zum entsprechenden Speicherort, um die BMP-Datei auszuwählen.</p> <p>Das Firmenlogo muss eine 24-bmp-Bitmap-Datei sein, die nicht größer als 256 x 64 Pixel sein sollte.</p>
<p><b>Video</b></p>	<p>Geben Sie die entsprechenden Informationen zur minimalen und maximalen Bildqualität an. Aktivieren Sie das Kontrollkästchen, um die lokale Cursor-Funktion zu aktivieren bzw. zu deaktivieren.</p>

<p><b>Power (Stromverbrauch)</b></p>	<p>Wählen Sie die Option aus, um die Zeitüberschreitung für den Standby-Modus des Client-Bildschirms und den OSD-Bildschirmschoner einzustellen.</p> <p>Die Zeiteinheit sollte Sekunden sein.</p> <p>Geben Sie für die Zeitüberschreitung einen Wert zwischen 10 und 14400 Sekunden ein, um die Einstellung zu aktivieren, und 0, um diese zu deaktivieren.</p>
<p><b>RDP</b></p> <p>Diese Option gilt nur für ThreadX v4.X.</p>	<p>Geben Sie die RDP-Verbindungsdetails ein.</p>
<p><b>Reboot (Neustarten)</b></p> <p>Diese Option gilt nur für ThreadX v5.X.</p>	<p>Aktivieren Sie dieses Kontrollkästchen zusammen mit dem Kontrollkästchen <b>Company Logo</b> (Firmenlogo). Dies führt zum Neustart des ThreadX-Geräts nach der Bereitstellung des Pakets mit dem Firmenlogo.</p>

## Verbindungen

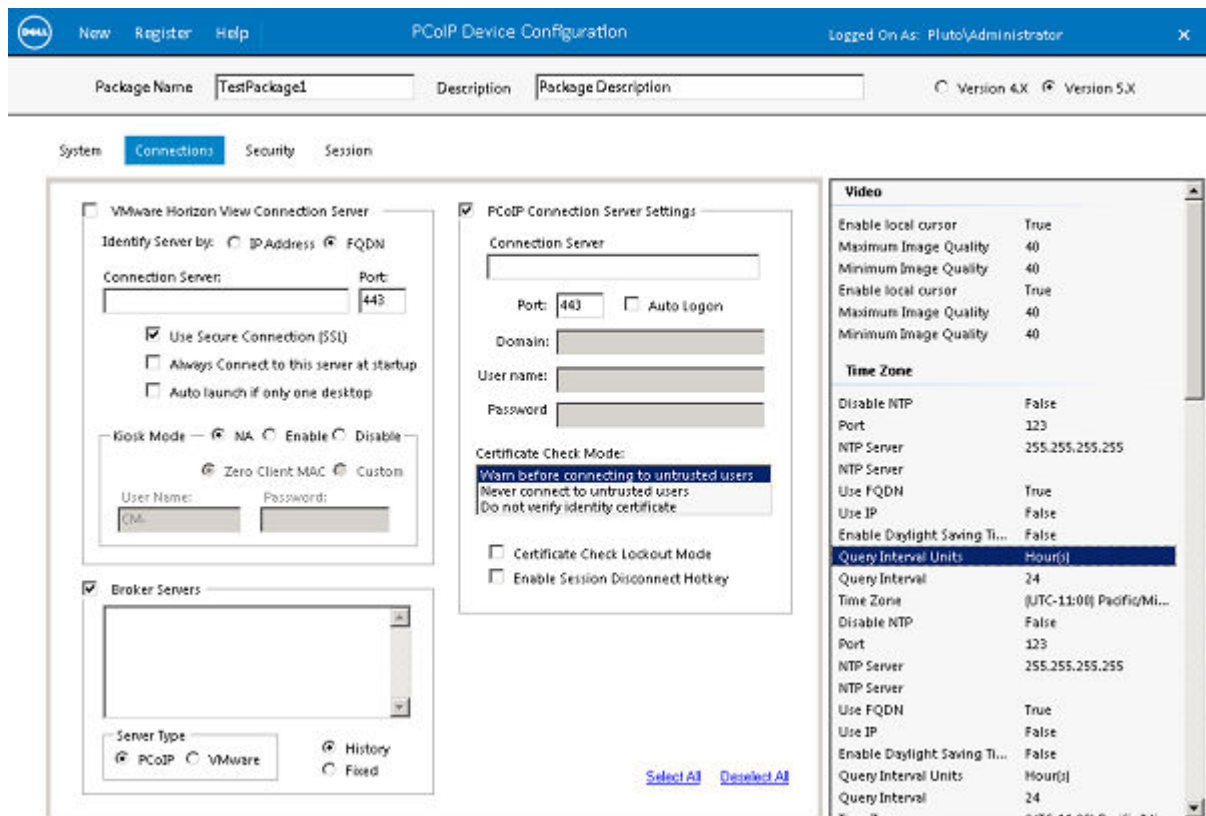


Abbildung 23. Verbindungen

Tabelle 10. Verbindungen

<p><b>Ansicht von VMware Horizon</b></p>	<p>Stellen Sie die folgenden Details für den VMware Horizon View Connection Server bereit:</p> <ul style="list-style-type: none"> <li>– Wählen Sie den Modus aus, über den der Verbindungsserver identifiziert werden soll.</li> <li>– Geben Sie die IP-Adresse oder den Hostnamen des Verbindungsservers ein.</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>– Geben Sie den Verbindungsportnummer ein und wählen Sie die Verbindungsoptionen entsprechend Ihren Anforderungen aus.</li> <li>– Klicken Sie auf <b>Kiosk Mode</b> (Kiosk-Modus), wenn das Gerät als Kiosk-Terminal fungieren soll.</li> </ul>
<b>PCoIP Connection Server Settings (Einstellungen für den PCoIP-Verbindungsserver)</b>	<p>Wählen Sie die Option aus, um folgende Details bereitzustellen:</p> <ul style="list-style-type: none"> <li>– Verbindungsserver</li> <li>– Portnummer</li> <li>– Domäne</li> <li>– Benutzername</li> <li>– Kennwort</li> <li>– Zertifikatsprüfmodus</li> </ul> <p>Aktivieren Sie basierend auf Ihren Anforderungen die folgenden Kontrollkästchen:</p> <ul style="list-style-type: none"> <li>– Certificate Check Lockout Mode (Sperrmodus für Zertifikatsprüfung)</li> <li>– Enable Session Disconnect Hotkey (Hotkey zum Trennen von Sitzungen aktivieren)</li> </ul>
<b>PCoIP oder VMware</b>	<p>Sie können dann den Servertyp PCoIP oder VMware auswählen. Es dürfen maximal 25 Server für PCoIP sowie VMware hinzugefügt werden.</p>

## Security (Sicherheit)

The screenshot shows the 'Security' tab in the PCoIP Device Configuration interface. The top navigation bar includes 'New', 'Register', 'Help', and 'Logged On As: Pluto\Administrator'. Below the navigation bar, there are input fields for 'Package Name' (containing 'TestPackage1') and 'Description' (containing 'Package Description').

The main content area is divided into several sections:

- Certificate:** A checkbox is checked. Below it is an empty text box with an 'Add' button. A note states: 'Enabling "Certificates" removes any existing certifications'.
- USB Device Authorization:** A checkbox is checked. Radio buttons for 'Authorized' (selected) and 'Unauthorized' are present. A 'Device Class' dropdown menu is set to 'Any'. Below are 'Add' and 'Remove' buttons and a table with columns 'Class' and 'Status'.
- Enable Advanced Configuration:** A checkbox is checked. It contains several sub-sections:
  - Web Interface of Device: Radio buttons for 'NA' (selected), 'Enable', and 'Disable'.
  - Wake-On-LAN: Radio buttons for 'NA' (selected), 'Enable', and 'Disable'.
  - Power On after Power Loss: Radio buttons for 'NA' (selected), 'Enable', and 'Disable'.
  - User Name Caching: Radio buttons for 'NA' (selected), 'Enable', and 'Disable'.
  - Enable Unified Communications: Radio buttons for 'NA' (selected), 'Enable', and 'Disable'.
  - Security Setting (Version 5X): Radio buttons for 'NA' (selected), 'Low', 'Med', and 'High'.
- Reset Administrator Password:** A checkbox is checked. It contains input fields for 'New Password' and 'Confirm Passwords'.

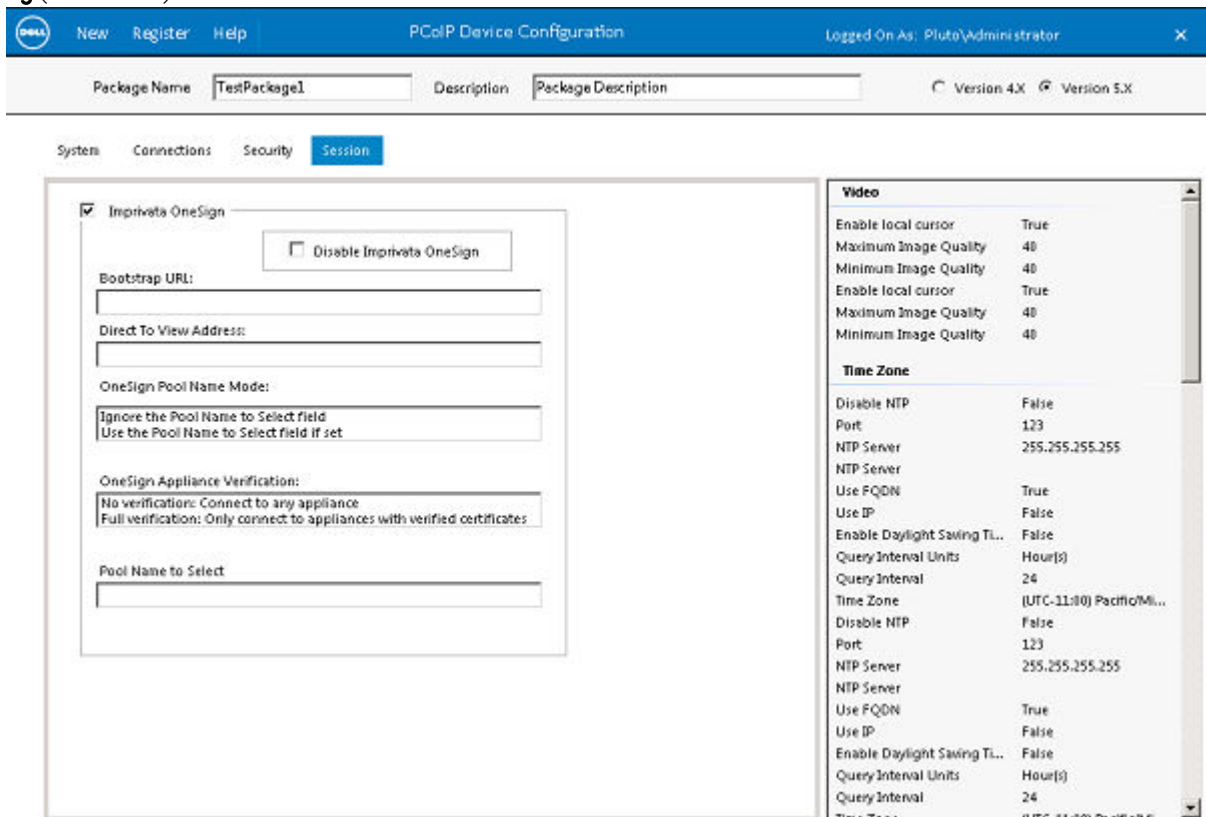
At the bottom right of the main content area, there are links for 'Select All' and 'Deselect All'.

Abbildung 24. Security (Sicherheit)

**Tabelle 11. Sicherheit**

<b>Certificate (Zertifikat)</b>	Wählen Sie die Option aus, um den Inhalt des Zertifikats einzugeben.
<b>USB Device Authorization (USB-Geräteautorisierung)</b>	Geben Sie Details zu USB-Berechtigungen (autorisiert und nicht autorisiert) für Geräte an.
<b>Enable Advanced Configuration (Erweiterte Konfiguration aktivieren)</b>	Wählen Sie die Optionen aus, wenn Sie die Weboberfläche des Geräts, Wake-on-LAN, Einschaltung nach Stromausfall, Zwischenspeicherung von Benutzernamen und Unified Communications aktivieren möchten.
<b>Reset Administrator Password (Administratorkennwort zurücksetzen)</b>	Wenn Sie das Kennwort des Geräteadministrators zurücksetzen möchten, wählen Sie diese Option aus und geben Sie das neue Kennwort ein.

**Sitzung (Version 5.X)**



**Abbildung 25. Sitzung**

**Tabelle 12. Sitzungen**

<b>Imprivata OneSign</b>	Wählen Sie diese Option, um Imprivata OneSign zu aktivieren.
<b>Disable Imprivata OneSign (Imprivata OneSign deaktivieren)</b>	Wählen Sie diese Option, um Imprivata OneSign zu deaktivieren.
<b>Bootstrap URL</b>	Geben Sie die Bootstrap-URL in das entsprechende Feld ein.
<b>OneSign Pool Name Mode (Modus für OneSign-Poolname)</b>	Wählen Sie die gewünschte Option aus. Die Optionen sind: <ul style="list-style-type: none"> <li>Ignore the Pool Name to Select field (Feld zum Auswählen des Poolnamens ignorieren)</li> </ul>

	<ul style="list-style-type: none"> <li>Use the Pool Name to Select field if set (Feld zum Auswählen des Poolnamens verwenden, wenn festgelegt)</li> </ul>
<b>OneSign Applicable Verification (Anwendbare OneSign-Überprüfung)</b>	<p>Wählen Sie die gewünschte Option aus. Die Optionen sind:</p> <ul style="list-style-type: none"> <li>No verification: Connect to any appliance (Keine Überprüfung: Verbindung mit jeder Appliance herstellen)</li> <li>Full verification: Only connect to appliance with verified certificates. (Vollständige Überprüfung: Verbindung nur mit Appliances mit geprüften Zertifikaten herstellen)</li> </ul>
<b>Pool Name to Select (Poolnamen auswählen)</b>	Geben Sie den Poolnamen in das entsprechende Feld ein.

- 2 Klicken Sie auf die Registerkarte **Register** (Registrieren), um die aktuelle Konfiguration zu speichern und den Vorgang abzuschließen.
- 3 Klicken Sie auf die Registerkarte **New** (Neu), um das neue PColP-Gerätekonfigurationspaket zu erstellen.

**ANMERKUNG:** Weitere Informationen zur Aktualisierung von ThreadX-Geräten von Version 4.X auf Version 5.X finden Sie unter [Aktualisieren der ThreadX 4.X-Geräte auf ThreadX 5.X über WDM](#).

# Updates

Die Seite „Update“ (Aktualisierung) bietet Ihnen eine Zusammenfassung der Details zu geplanten Jobs, zu wiederkehrenden Aktualisierungen, zu Jobs zur Repository-Synchronisierung und zur Peer-gestützten Verteilung. Sie können auch Profile und DDCs erstellen.

Themen:

- [Aufgaben](#)
- [Wiederkehrende Aktualisierungen](#)
- [Echtzeit Befehle](#)
- [Repository-Synchronisierung](#)
- [Peer-gestützte Verteilung](#)
- [Profile](#)
- [Identifizieren von vom Profile-Manager unterstützten Geräten](#)
- [Bereitstellen eines Konfigurationspakets mithilfe des Profil-Managers](#)
- [Löschen eines PM-Konfigurationspakets](#)

## Aufgaben

Mit diesem Parameter können Sie geplante Agent-Aktualisierungen, Images, Konfigurationen oder andere Pakete von Geräten oder Anwendungsseiten anzeigen. Sie können die Details zu geplanten Aufgaben wie folgt anzeigen:

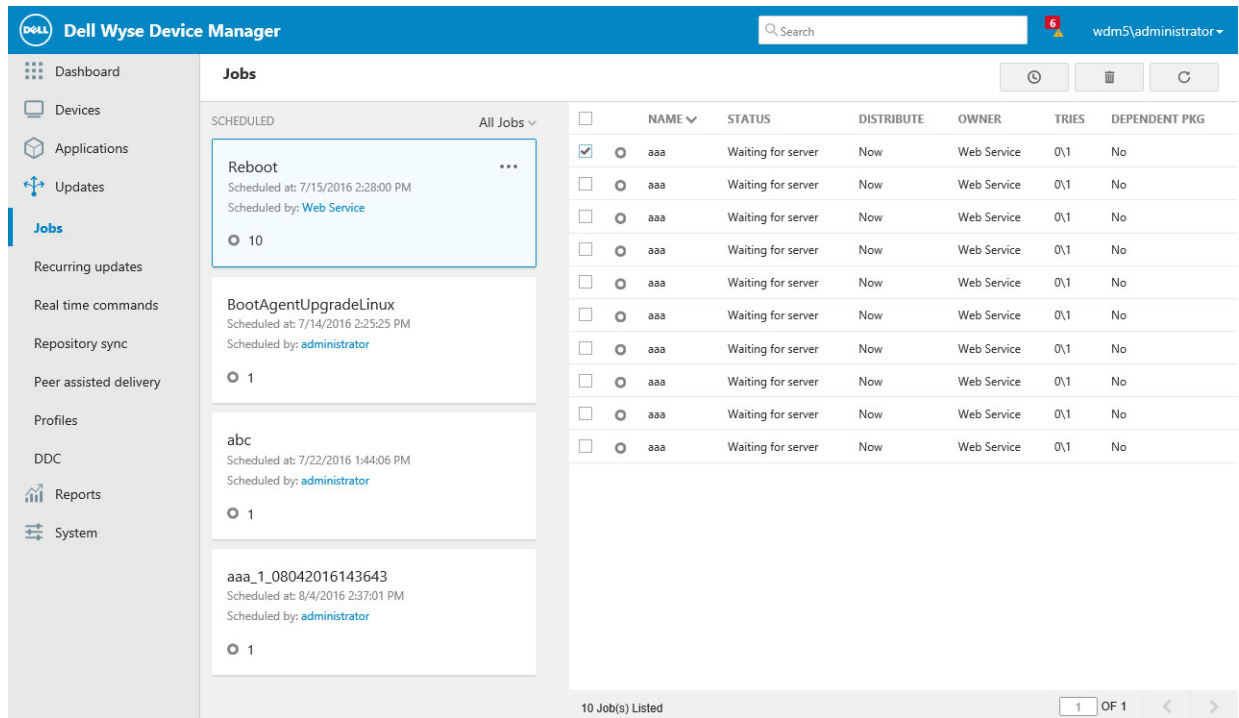
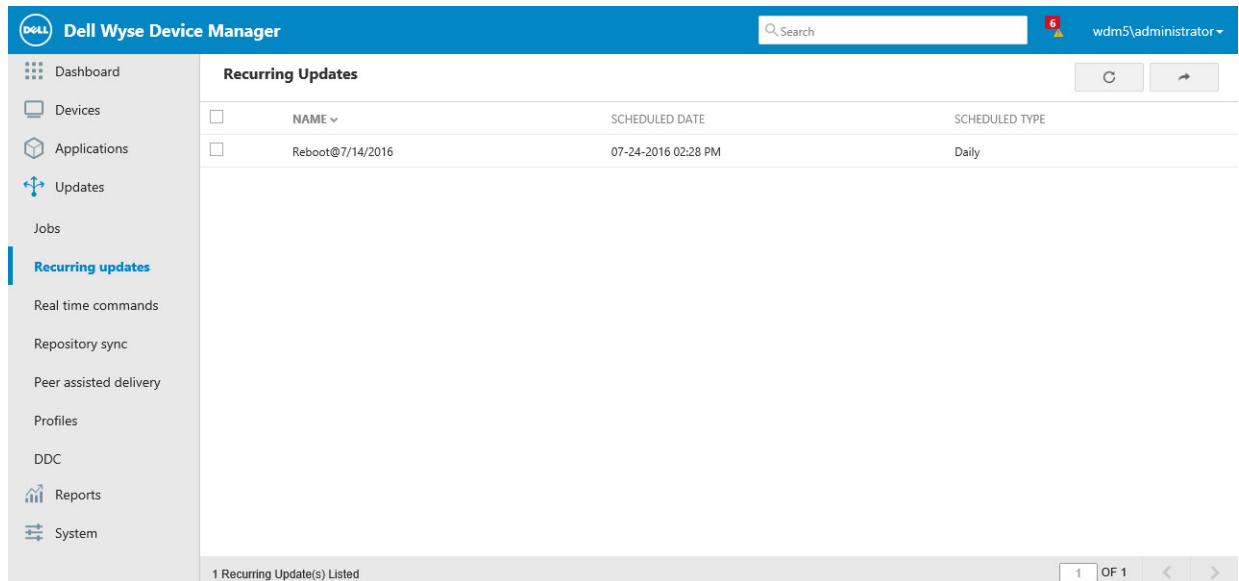


Abbildung 26. Aufgaben

- All jobs (Alle Aufgaben) – Wenn Sie „All jobs“ (Alle Aufgaben) auswählen, werden die geplanten Aufgaben für alle Benutzer aufgeführt.
  - My jobs (Meine Aufgaben) – Wenn Sie „My jobs“ (Meine Aufgaben) auswählen, werden nur die geplanten Aufgaben des angemeldeten Benutzers aufgeführt.
- 1 Um die Aufgabe neu zu planen, wählen Sie die Option **Now** (Jetzt), wenn Sie das Paket jetzt verteilen möchten, oder wählen Sie die Option **A specific date and time** (Bestimmtes Datum und Uhrzeit) und geben Sie das gewünschte Datum und die gewünschte Uhrzeit für die Paketverteilung ein. Klicken Sie auf die Option **On/Off** (Ein/Aus), um die Option **Retry failed updates** (Fehlgeschlagene Aktualisierungen wiederholen) zu aktivieren bzw. zu deaktivieren.
  - 2 Klicken Sie auf **Reschedule** (Erneut planen).
  - 3 Klicken Sie auf **Delete** (Löschen), um die Aufgabe zu löschen.

## Wiederkehrende Aktualisierungen

Mit diesem Parameter können Sie den Zeitplan des Agent für Aktualisierungen, Images, Konfigurationen oder anderen Pakete als wiederkehrende Aktualisierungen von Geräten oder Anwendungsseiten anzeigen.



**Abbildung 27. Wiederkehrende Aktualisierungen**

- 1 Klicken Sie auf die Option **Refresh** (Aktualisieren), um die Seite zu aktualisieren.
- 2 Klicken Sie auf die Option **Reschedule** (Erneut planen), um die Paketverteilung erneut zu planen.
  - a Geben Sie folgende Details zur Paketverteilung ein:
    - 1 Name der wiederkehrenden Aktualisierung.
    - 2 Wählen Sie in der Dropdown-Liste **Recur** (Wiederholen) den Tag für die Paketverteilung aus.
    - 3 Geben Sie das Start- und Enddatum der Paketverteilung ein.
    - 4 Geben Sie die Zeitdauer der Paketverteilung ein.
    - 5 Klicken Sie auf **Reschedule** (Erneut planen).
- 3 Klicken Sie auf die Option **Delete** (Löschen), um die Aufträge zu entfernen.
- 4 Klicken Sie auf die Option **Export** (Exportieren), um das Gerät im Format .cs- oder .txt (mit Tabstoppentrennzeichen) zu exportieren.

## Echtzeit Befehle

In dieser Kategorie können Sie Details zu den für die Geräte geplanten Echtzeitbefehlen anzeigen. Zudem können Sie folgende Vorgänge durchführen.

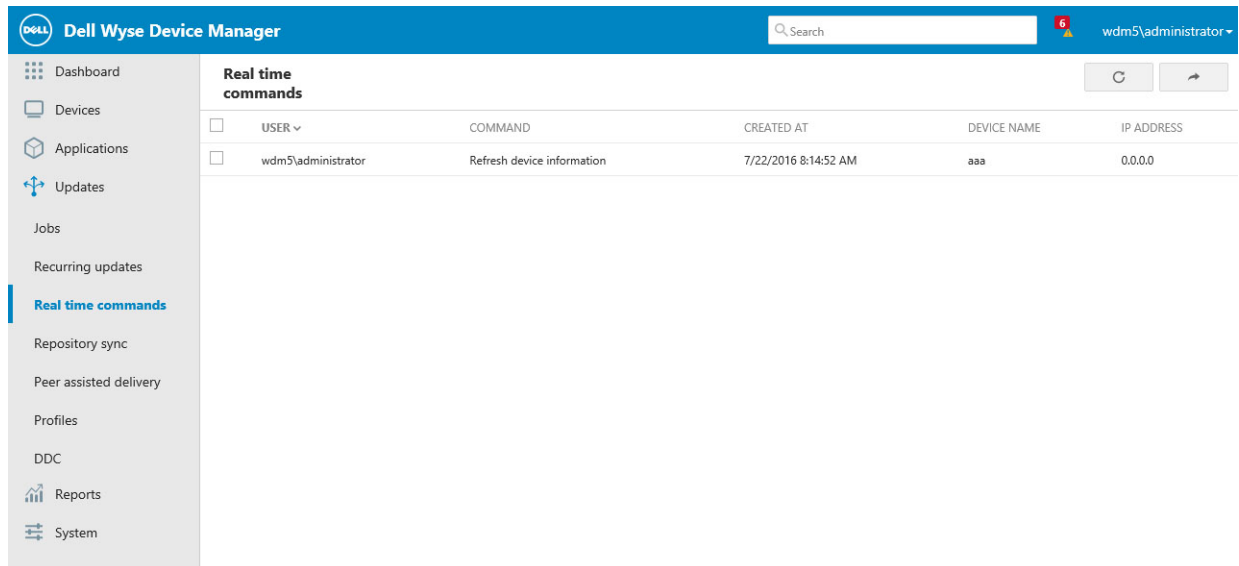


Abbildung 28. Echtzeit Befehle

- 1 Klicken Sie auf die Option **Refresh** (Aktualisieren), um die Seite zu aktualisieren.
- 2 Klicken Sie auf die Option **Delete** (Löschen), um den Befehl zu entfernen.
- 3 Klicken Sie auf die Option **Export** (Exportieren), um das Gerät im Format .cs- oder .txt (mit Tabstopptrennzeichen) zu exportieren.

## Repository-Synchronisierung

In dieser Kategorie können Sie die für das erstellte Remote-Repository geplanten Aufgaben für die Repository-Synchronisierung anzeigen.

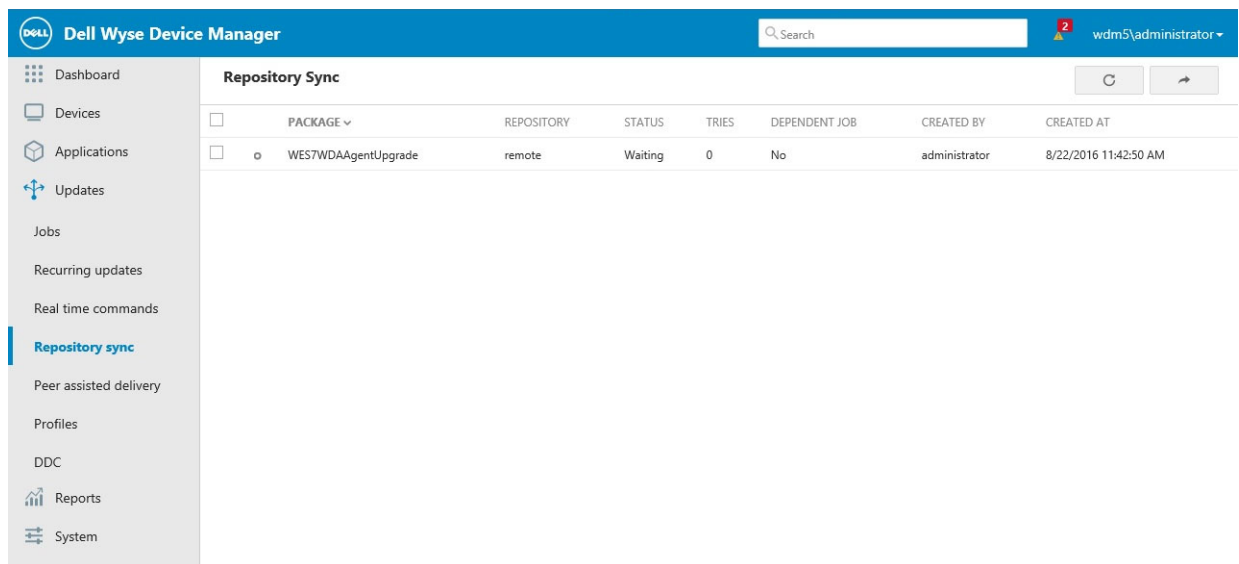


Abbildung 29. Repository-Synchronisierung

## Peer-gestützte Verteilung

In dieser Kategorie können Sie Details zum Plan für die Peer-gestützte Verteilung für Subnetze anzeigen. Weitere Informationen über die Peer-gestützte Verteilung finden Sie unter [Peer-gestützte Verteilung](#) und [Konfigurieren von PAD](#).

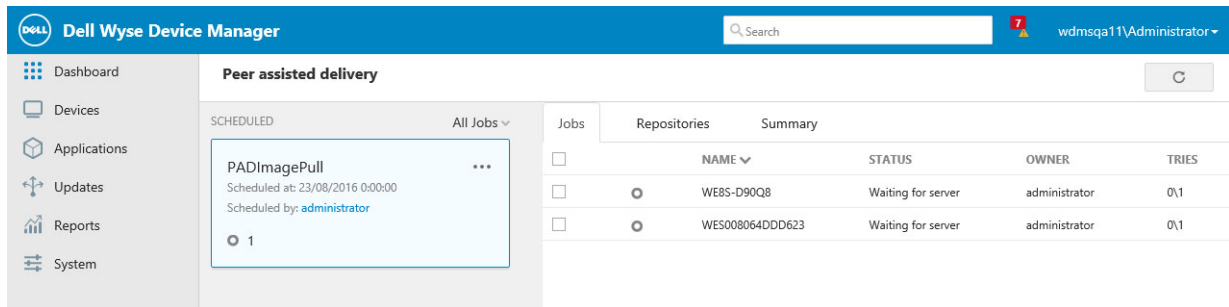


Abbildung 30. Peer-gestützte Verteilung

## Profile

Die Seite **Profiles** (Profile) ermöglicht die Bereitstellung einer vordefinierten Konfiguration auf einer bestimmten Gruppe von Geräten. Sie können die Konfigurationen mithilfe des Dell Wyse Configuration Manager (WCM) erstellen und sie in einem angegebenen Repository speichern. Ein Repository ist ein System, in dem die Konfigurationen gespeichert werden. Thin-Client-Geräte verbinden sich über HTTP(S), FTP oder CIFS mit diesen Repositories und laden die Konfigurationen herunter. Weitere Informationen finden Sie im *Dell Wyse Configuration Manager Administratorhandbuch* auf der Dell Wyse Support-Website. Profile sind eindeutig für ein Betriebssystem und Sie können immer nur eine Konfiguration gleichzeitig auf eine Gruppe von Geräten anwenden.

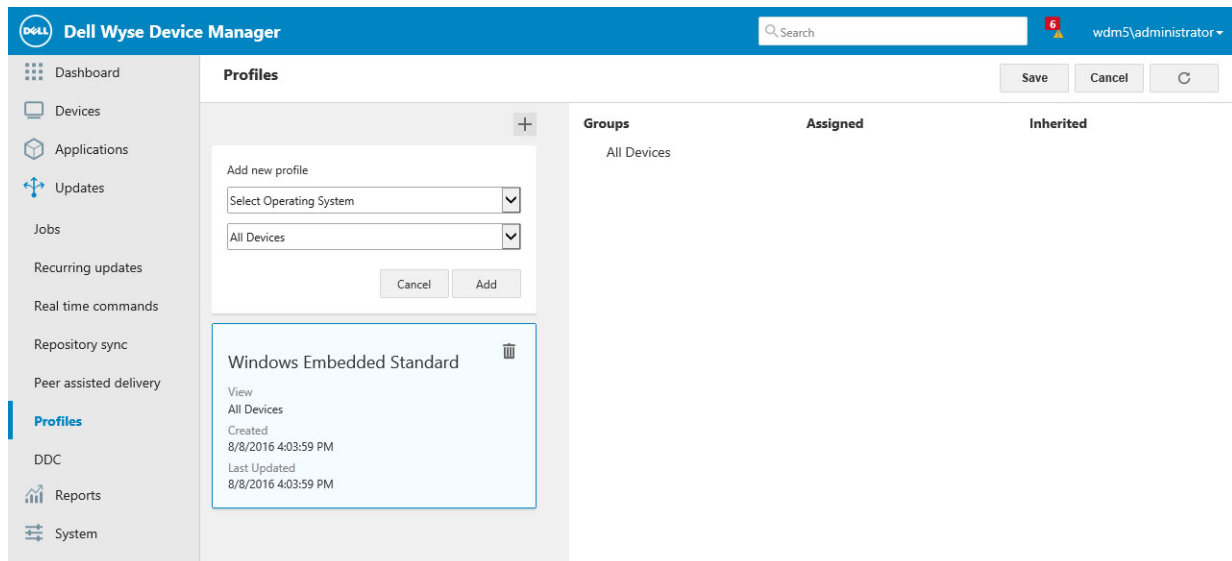


Abbildung 31. Profile

Mit diesem Parameter können Sie ein neues Profil hinzufügen und Details angeben, z. B. für **Groups** (Gruppen), **Assigned** (Zugewiesen) und **Inherited** (Geerbt).

Um ein neues Profil hinzuzufügen, führen Sie folgenden Vorgang durch:

- 1 Wählen Sie aus der Dropdown-Liste **Select Operating System** (Betriebssystem auswählen) Ihr bevorzugtes Betriebssystem aus.
- 2 Wählen Sie aus der Dropdown-Liste die bevorzugte Ansicht aus, die für ein bestimmtes Profil bereitgestellt werden soll.
- 3 Klicken Sie auf **Add** (Hinzufügen), um das neue Profil in den Gruppen einzubeziehen.

Weitere Informationen über die von PM unterstützten Geräte, Bereitstellung von Konfigurationspaketen und Löschung eines Profilkonfigurationspakets finden Sie unter [Identifizieren von vom PM unterstützten Geräten](#), [Bereitstellen eines Konfigurationspakets mithilfe des Profil-Managers](#), [Erstellen eines Gerätekonfigurationspakets](#), [Aktivieren des Profil-Managers im System](#) und [Löschen eines PM-Konfigurationspakets](#).

# Identifizieren von vom Profile-Manager unterstützten Geräten

- 1 Wählen Sie auf der Seite **Device** (Gerät) ein Gerät aus.
- 2 Klicken Sie auf die Option „View details“ (Details anzeigen) und schauen Sie sich den Abschnitt „Capabilities“ (Fähigkeiten) an.
- 3 Suchen Sie im Abschnitt „Capabilities“ (Fähigkeiten) nach „WCM Support“ (WCM-Unterstützung).
- 4 Das Gerät ist Profil-Manager-fähig, wenn folgende Bedingungen vorliegen:
  - Grün: Das Gerät ist Profil-Manager-fähig.
  - Rot: Das Gerät ist nicht Profil-Manager-fähig.
- 5 Um die Profil-Manager-Fähigkeit des Geräts herzustellen, müssen Sie in WDM den aktuell verfügbaren WDA-Agent bereitstellen.

**ANMERKUNG:** Registrieren Sie bei HAgent-unterstützten Geräten das WCM Client-Paket und übertragen Sie es auf Geräte mit HAgent.

Wenn sich diese Geräte beim WDM-Server anmelden, erkennt der Hserver-Service diese Geräte basierend auf dem Wert, den sie an den WCMSUPP-Tag senden.

# Bereitstellen eines Konfigurationspakets mithilfe des Profil-Managers

Zum Erstellen eines Konfigurationspakets mithilfe des Profilmanagers führen Sie die folgenden Schritte aus:

- 1 Klicken Sie in der WDM-Web-UI auf **Updates > Profiles (Profile)**.  
Die Seite **Profiles** (Profile) wird angezeigt.
- 2 Wählen Sie aus der Drop-Down-Liste **Select Operating System** (Betriebssystem auswählen) Ihr bevorzugtes Betriebssystem aus.  
Im Drop-Down-Feld werden nur die Betriebssysteme aufgeführt, für die Sie noch keine Konfigurationspakete erstellt haben. Sie können nur ein Profil pro Betriebssystem erstellen. Die Leaf-Konfiguration hat Vorrang vor der übergeordneten Konfiguration, aber WTOS ist eine Ausnahme.
- 3 Wählen Sie aus der Dropdown-Liste die bevorzugte Ansicht aus, in der das jeweilige Profil bereitgestellt werden muss.
- 4 Klicken Sie auf **Add** (Hinzufügen), um das neue Profil in den Gruppen einzubeziehen.
- 5 Wählen Sie eine WCM-Konfiguration aus der Dropdown-Liste **Assigned** (Zugewiesen) aus.  
Diese Liste zeigt alle Konfigurationspakete an, die Sie für das ausgewählte Betriebssystem mithilfe der WCM-Anwendung erstellt haben.
- 6 Klicken Sie auf **Save** (Speichern).

Wenn sich Konfigurationsänderungen zu der vorhandenen Konfiguration auf dem Client ergeben, wendet PM die aktualisierte Konfiguration an, wenn der Client angemeldet wird. Das Fenster **Update Now** (Jetzt aktualisieren) wird auf dem Client angezeigt und wenn Sie auf **OK** klicken, wendet PM die aktualisierte Konfiguration an.

**ANMERKUNG:** Bitte beachten Sie die Unterschiede zwischen den XML-Konfigurationen und den JSON-Konfigurationen.

**Tabelle 13. Unterschiede zwischen XML- und JSON-Konfigurationen**

XML-Konfigurationen	JSON-Konfigurationen
Sie können nur von der MMC-UI erstellt werden.	Sie können von der Web-UI und der MMC-UI erstellt werden.
Sie können nur für Windows-Betriebssysteme erstellt werden.	Sie können für Windows-, WTOS- und Linux-Betriebssysteme erstellt werden.
Sie können nur für Geräte mit HAgents bereitgestellt werden.	Sie können für Geräte mit WDA bereitgestellt werden.
Sie werden nicht in der zugewiesenen Drop-Down-Liste in der Web-UI angezeigt.	

# Löschen eines PM-Konfigurationspakets

So löschen Sie ein Konfigurationspaket:

- 1 Klicken Sie in der Web-UI von WDM auf **Updates (Aktualisierungen) > Profiles (Profile)**.

Die vorhandenen Profile werden auf der Seite aufgeführt.

- 2 Wählen Sie ein Profil aus und klicken Sie auf das Symbol zum **Löschen**.

Sie werden aufgefordert, mit dem Löschvorgang fortzufahren oder ihn abzubrechen.

- 3 Klicken Sie auf **Delete (Löschen)**, um das Konfigurationspaket zu löschen.

**ANMERKUNG:** Sie können immer nur ein Profil für ein bestimmtes Betriebssystem erstellen. Wenn Sie ein weiteres Profil für dasselbe Betriebssystem erstellen möchten, müssen Sie das vorhandene Paket löschen und ein neues erstellen.

## Default Device Configuration – DDC

Mit WDM können Sie auf einfache Weise DDCs erstellen und verwalten. Sie können Images oder mehrere Softwarepakete oder beides mithilfe von DDC auf die Geräte anwenden. Mit DDC wird sichergestellt, dass alle Geräte in der Gruppe, der DDC zugewiesen ist, über dieselben Images oder Konfigurationen verfügen.

Mit diesem Parameter können Sie eine neue Default Device Configuration (DDC) hinzufügen und Details wie z. B. **Groups** (Gruppen), **Image**, **Packages** (Pakete) und **Execute DDC** (DDC ausführen) angeben.

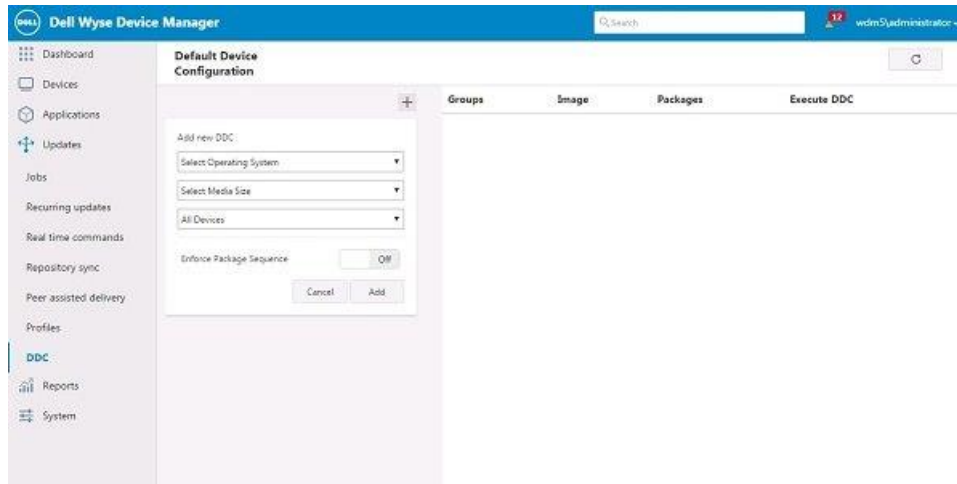


Abbildung 32. DDC

So fügen Sie eine neue DDC hinzu:

- 1 Wählen Sie aus der Dropdown-Liste **Select Operating System** (Betriebssystem auswählen) Ihr bevorzugtes Betriebssystem aus.
- 2 Wählen Sie aus der Dropdown-Liste **Select Media Size** (Mediengröße auswählen) Ihre bevorzugte Mediengröße aus.
- 3 Wählen Sie aus der Dropdown-Liste die bevorzugte Ansicht aus, die für ein bestimmtes Profil bereitgestellt werden soll.
- 4 Klicken Sie auf die Option **On/Off** (Ein/Aus), um die Option **Enforce Sequence** (Sequenz durchsetzen) zu aktivieren bzw. zu deaktivieren. Je nachdem, ob Sie möchten, dass die Pakete, die Teil der DDC sind, die einzigen, für das Gerät zulässigen Pakete sein sollen (kein anderes Paket kann an die Geräte gesendet werden), aktivieren oder deaktivieren Sie „Enforce Sequence“ (Sequenz durchsetzen).

**ANMERKUNG:** Die Auswahl von „Enforce Sequence“ (Sequenz durchsetzen) könnte Pakete beeinträchtigen, die außerhalb des DDC-Prozesses für ein Gerät gesendet oder geplant wurden.

- 5 Klicken Sie auf **Add** (Hinzufügen), um die neue DDC in die Gruppen zu integrieren.
- 6 Wählen Sie ein Image aus der Dropdown-Liste „Image“.

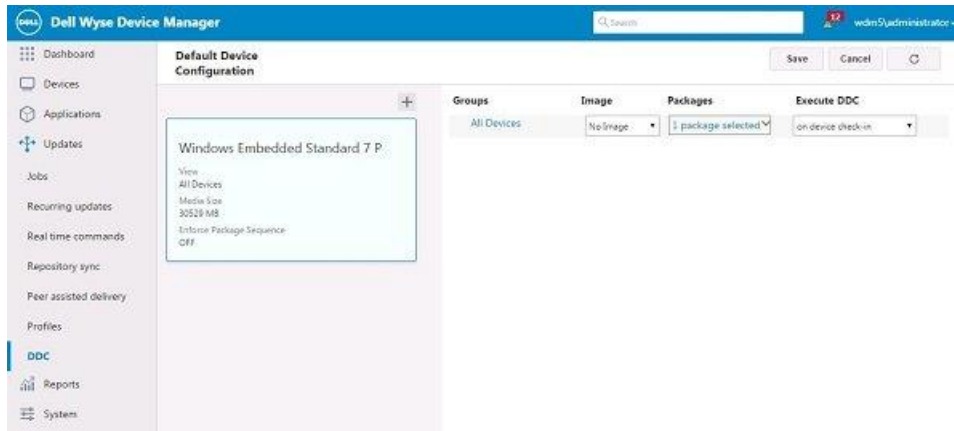


Abbildung 33. DDC

- 7 Wählen Sie ein Softwarepaket aus der Dropdown-Liste „Packages“ (Pakete).
- 8 Legen Sie für „Execute DDC“ (DDC ausführen) entweder „Device Checks in“ (Gerät meldet sich an) oder „Every Day at Specific Time“ (Jeden Tag zu einer bestimmten Zeit) fest.
- 9 Klicken Sie auf **Save** (Speichern).

# Berichte

In der Web-UI können Sie Protokollberichte täglich, wöchentlich oder monatlich erstellen. Die erstellten Berichte können eingesehen, bearbeitet und gespeichert werden.

Themen:

- Erstellen eines Protokollberichts
- Erstellen eines Anwendungsberichts
- Erstellen eines Berichts zu einer Remote-Sitzung

## Erstellen eines Protokollberichts

Protokollberichte enthalten wichtige Informationen über Ereignisse oder Aktivitäten, die hinsichtlich WDM-Komponenten auf dem WDM-Server stattgefunden haben. Sie ermöglichen es Ihnen, ganz einfach und jederzeit die von Ihnen gewünschten Informationen anzuzeigen. Nach dem Erstellen eines Berichts speichert WDM diesen automatisch unter der Registerkarte „Reports“ (Berichte), sodass Sie ihn jederzeit erneut nutzen können. Sie müssen bereits erstellte Berichte nicht noch einmal erstellen. Jedes Mal, wenn Sie den Bericht anzeigen, erhalten Sie die neuesten Informationen zu den von Ihnen festgelegten Kriterien.

**ANMERKUNG: Berichte sind nicht statisch. Wenn sich Informationen ändern (zum Beispiel werden neue Geräte erkannt oder es werden neue protokollierte Informationen generiert), zeigt der Bericht die neuen Informationen an (vorausgesetzt, diese Informationen entsprechen den Kriterien des Berichts).**

Verwenden Sie die folgenden Richtlinien, um einen Protokollbericht zu erstellen, anzuzeigen und zu speichern:

The screenshot shows the Dell Wyse Device Manager web interface. The left sidebar contains navigation options: Dashboard, Devices, Applications, Updates, Reports, Log Report, Application, Remote Session, and System. The main area is titled 'Log Report' and includes a 'Saved Reports' section with a dropdown menu. Below this, there is a 'Time Range' section with a 'Today' dropdown, 'From' and 'To' date pickers, and checkboxes for 'No Start Date' and 'No End Date'. A 'Users' section has a dropdown menu set to 'All' and an 'Apply' button. The right side of the interface displays a table of log entries with columns for DATE, USER, DEVICE, MAC, IP, SW PKG, and DESCRIPTION.

DATE	USER	DEVICE	MAC	IP	SW PKG	DESCRIPTION
August 25th 2016, 11:02:53 am	Web Service					[WorkerThread]UpdateAllClientBroker: success
August 25th 2016, 11:02:53 am	Web Service					[WorkerThread]AddUpdateClientBroker: success
August 25th 2016, 11:02:53 am	Web Service					[WorkerThread]AddUpdateClientBroker: success
August 25th 2016, 11:02:53 am	Web Service					[WorkerThread]UpdateAllClientBroker: success
August 25th 2016, 11:02:53 am	Web Service					[WorkerThread]AddUpdateClientBroker: success
August 25th 2016, 11:02:53 am	Web Service					[WorkerThread]AddUpdateClientBroker: success
August 25th 2016, 11:02:53 am	administrator	WT00806	4c1a057	008064	10.150.112.30	Refresh Device Information for device WT008064c1a057 By: administrator
August 25th 2016, 11:02:53 am	administrator	WT00806	4c1a057	008064	10.150.112.30	Send real time command 'Refresh Device Info' for ClientID 2 by: administrator
August 25th 2016, 10:47:05 am	Web Service					[WorkerThread]UpdateAllClientBroker: success

Abbildung 34. Protokollbericht

- 1 Klicken Sie auf **Reports (Berichte) > Log Report (Protokollbericht)**.
- 2 Wählen Sie die gewünschten Bereiche aus und wählen Sie die Anzahl der Benutzer aus, deren Aktivitäten Ihr Bericht enthalten soll. Wenn Sie den Bericht auf die Aktivitäten eines bestimmten Benutzers beschränken möchten, wählen Sie den Benutzer unten aus. Wenn Sie die Aktivitäten aller Benutzer anzeigen möchten, wählen Sie **All (Alle)** aus der Drop-down-Liste aus.
- 3 Klicken Sie auf **Apply (Anwenden)**.

Wenn Ihr Protokollbericht zusammengestellt wurde, wird er im rechten Fensterbereich der Seite angezeigt.

- Um den Bericht zu speichern, klicken Sie auf den Link **Save Report** (Bericht speichern) im Bereich **Time Range** (Zeitraum).
- Geben Sie den Berichtsnamen im Dialogfeld **Save Report** (Bericht speichern) ein und klicken Sie auf **Save** (Speichern).

Der gespeicherte Bericht wird in der Dropdown-Liste **Saved Reports** (Gespeicherte Berichte) aufgeführt.

- ANMERKUNG:** Um einen Protokollbericht als .txt-Datei oder .csv-Datei zu speichern, klicken Sie auf das Symbol für den Export in der oberen rechten Ecke der Seite und wählen Sie je nach Präferenz .csv oder .txt (tab delimited) (txt [tabulatorgetrennt]) aus. Für die zukünftige Verwendung des Berichts wählen Sie ihn unter Saved Reports (Gespeicherte Berichte) aus. Die gespeicherten Berichte können je nach Bedarf bearbeitet oder gelöscht werden.

## Erstellen eines Anwendungsberichts

Dies ermöglicht dem Benutzer die Erstellung eines Berichts, der die Geräte, auf denen bestimmte Software installiert ist, sowie die vom Benutzer ausgewählte Version aufführt.

- Klicken Sie auf **Reports (Berichte) > Application (Anwendung)**.  
Daraufhin wird die Seite **Application Report** (Anwendungsbericht) angezeigt.

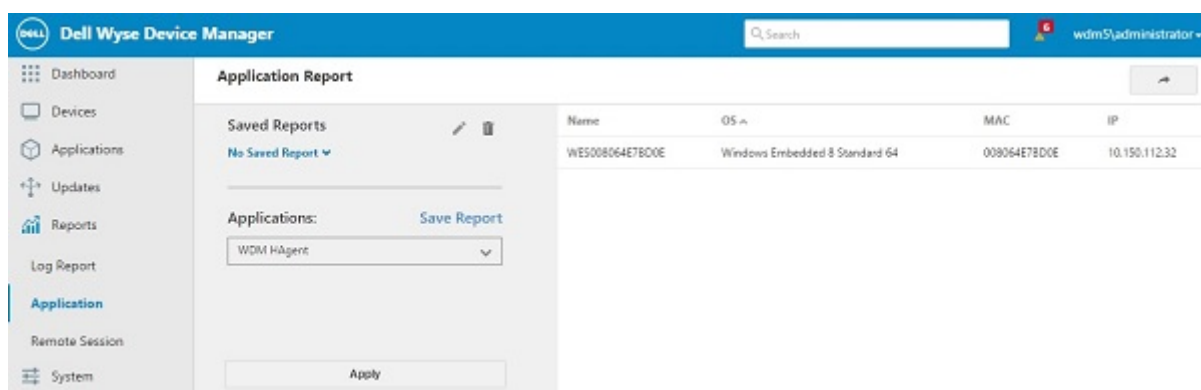


Abbildung 35. Anwendungsbericht

- Wählen Sie in der Dropdown-Liste **Applications** (Anwendungen) Ihre bevorzugte Anwendung aus, für die Sie den Bericht anzeigen möchten, und klicken Sie dann auf **Apply** (Anwenden).  
Wenn Ihr Anwendungsbericht zusammengestellt wurde, wird er im rechten Fensterbereich der Seite angezeigt.
- Um den Bericht zu speichern, klicken Sie auf den Link **Save Report** (Bericht speichern) im Bereich **Applications** (Anwendungen).
- Geben Sie den Berichtsnamen im Dialogfeld **Save Report** (Bericht speichern) ein und klicken Sie auf **Save** (Speichern).  
Der gespeicherte Bericht wird in der Dropdown-Liste **Saved Reports** (Gespeicherte Berichte) aufgeführt.

- ANMERKUNG:** Um einen Anwendungsbericht als .txt-Datei oder .csv-Datei zu speichern, klicken Sie auf das Symbol für den Export in der oberen rechten Ecke der Seite und wählen Sie je nach Präferenz .csv oder .txt (tab delimited) (txt [tabulatorgetrennt]) aus. Für die zukünftige Verwendung des Berichts wählen Sie ihn unter Saved Reports (Gespeicherte Berichte) aus. Die gespeicherten Berichte können je nach Bedarf bearbeitet oder gelöscht werden.

## Erstellen eines Berichts zu einer Remote-Sitzung

Berichte zu Remote-Sitzungen enthalten Verbindungsinformationen zu allen Geräten in WDM basierend auf den Filterkriterien, die während der Berichterstellung definiert werden. Sie ermöglichen es Ihnen, festzustellen, welcher Benutzer wie lange mit welcher Art von Broker-Verbindung verbunden war. Nach dem Erstellen eines Berichts wird er im rechten Fensterbereich der Seite angezeigt. Sie können den Bericht exportieren und später verwenden.

Verwenden Sie die folgenden Richtlinien, um einen Bericht zu Remote-Sitzungen zu erstellen, anzuzeigen und zu speichern:

- Klicken Sie auf **Reports (Berichte) > Remote Session (Remote-Sitzung)**.  
Daraufhin wird die Seite **Remote Session Report** (Bericht zu einer Remote-Sitzung) angezeigt.

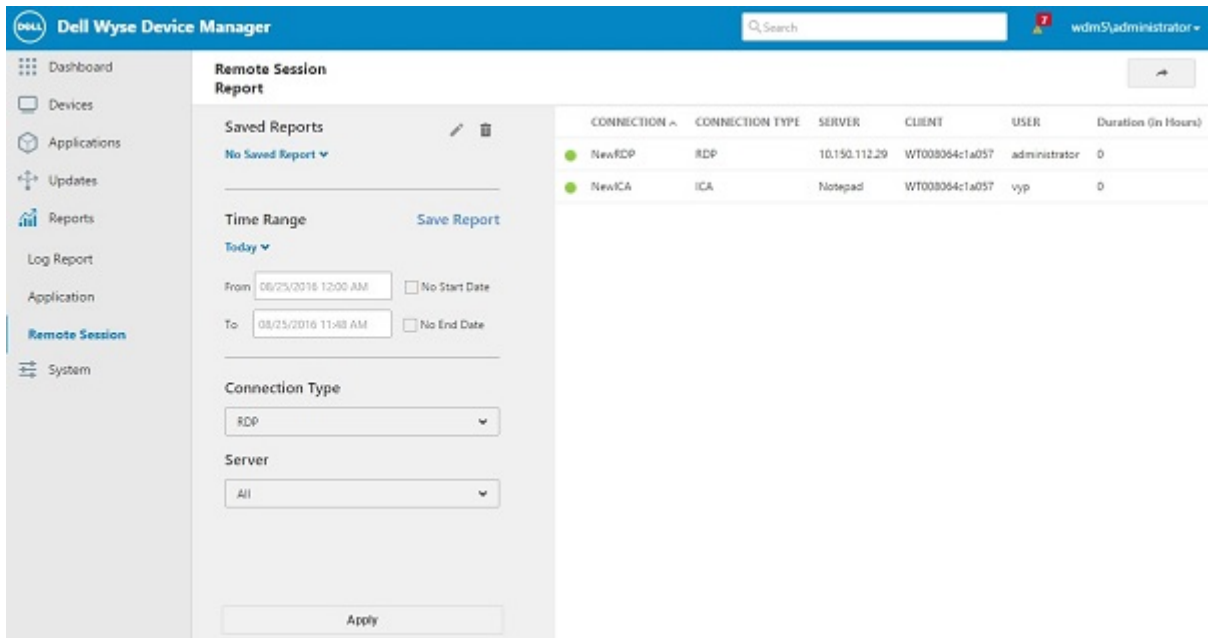


Abbildung 36. Remote-Sitzung

- 2 Wählen Sie aus der Drop-down-Liste **Time Range** (Zeitraum) den gewünschten Zeitraum oder die Dauer aus, für die Sie den Bericht erstellen möchten. Berichte können für den aktuellen Tag, den vorherigen Tag, die letzten 7 Tage, die letzten 30 Tage oder immer erstellt werden. Um Ihren eigenen Zeitraum festzulegen, klicken Sie auf **Custom** (Benutzerdefiniert) und geben Sie das Anfangs- und Enddatum an.
- 3 Sie können den Bericht auf der Grundlage der folgenden Suchkriterien generieren:
  - Wählen Sie aus der Dropdown-Liste **Connection Type** (Verbindungstyp) den gewünschten Verbindungstyp.
  - Wählen Sie aus der Dropdown-Liste **Server** den gewünschten Servernamen oder die IP.
- 4 Klicken Sie auf **Apply** (Anwenden).  
Wenn Ihr Anwendungsbericht zusammengestellt wurde, wird er im rechten Fensterbereich der Seite angezeigt.
- 5 Um den Bericht zu speichern, klicken Sie auf den Link **Save Report** (Bericht speichern) im Bereich **Time Range** (Zeitraum).
- 6 Geben Sie den Berichtsnamen im Dialogfeld **Save Report** (Bericht speichern) ein und klicken Sie auf **Save** (Speichern).  
Der gespeicherte Bericht wird in der Dropdown-Liste **Saved Reports** (Gespeicherte Berichte) aufgeführt.

**ANMERKUNG:** Um einen Bericht zu Remote-Sitzungen als .txt-Datei oder .csv-Datei zu speichern, klicken Sie auf das Symbol für den Export in der oberen rechten Ecke der Seite und wählen Sie je nach Präferenz .csv oder .txt (tab delimited) (txt [tabulatorgetrennt]) aus. Für die zukünftige Verwendung des Berichts wählen Sie ihn unter Saved Reports (Gespeicherte Berichte) aus. Die gespeicherten Berichte können je nach Bedarf bearbeitet oder gelöscht werden.

# System

Auf der Seite **System** der Web-UI können Sie die folgenden Optionen konfigurieren:

- **Subnets** (Subnetze): Über die Seite „Subnets“ (Subnetze) können Sie die System-Broadcast-IP, die aktive IP, die Subnetzmaske und eine Beschreibung anzeigen. Subnetze werden automatisch erstellt, wenn das Gerät in den WDM-Server eingecheckt wird. Sie können Subnetze auch manuell konfigurieren. Informationen zum manuellen Konfigurieren von Subnetzen finden Sie unter [Manuelles Erstellen von Subnetzen](#).
- **Repositories** (Repositoryys): Die Seite „Repository“ enthält die Einzelheiten zum Master-Repository und zum Remote-Repository. Informationen zum Erstellen von Remote-Repositoryys finden Sie unter [Registrieren von Remote-Repositoryys](#).
- **Accounts** (Konten): Über die Seite „Accounts“ (Konten) können Sie Benutzerdetails anzeigen. Sie können außerdem folgende Aufgaben ausführen:
  - [Hinzufügen von Benutzern und Gruppen aus dem Active Directory](#).
  - [Hinzufügen von Benutzern aus lokalen Computerkonten](#).
  - [Bearbeiten von Benutzerberechtigungen](#).
  - [Löschen von Benutzern](#).
- **Console** (Konsole) – Auf der Seite **Console** (Konsole) finden Sie die folgenden Details:
  - Gerätestatus
  - Benutzerdefinierte Gruppenordner
  - Remote-Sitzungen
  - Default Device Configuration (DDC)
  - Profil-Manager
  - Alias-Name für Verwaltungsserver

Weitere Informationen finden Sie unter [Konsole](#).
- **Device Discovery** (Geräteerkennung): Auf der Seite „Device Discovery“ (Geräteerkennung) finden Sie Informationen zum Agent-Erkennungsverhalten nach der ersten Anmeldung beim Verwaltungsserver und DHCP-Erkennungsdetails. Weitere Informationen finden Sie unter [Konfigurieren der Geräteerkennung](#).
- **Services**: Auf der Seite „Services“ werden Ihnen die Details zum TFTP-Server und zu Wake On LAN angezeigt. Weitere Informationen finden Sie unter [Über die Services](#).
- **Logging** (Protokollierung): Dieser Parameter hilft Ihnen bei der Konfiguration der Protokollierungsebenen für verschiedene WDM-Komponenten. Bei einer höheren Protokollierungsebene werden mehr Daten in der Datenbank gespeichert. Dies kann dazu führen, dass der Server verlangsamt wird. Weitere Informationen finden Sie unter [Konfigurieren der Protokollierungsebenen](#).
- **Scheduling** (Planung): Auf der Seite „Scheduling“ (Planung) können Sie Details anzeigen, wie z. B. die maximale Anzahl gleichzeitiger Aktualisierungen, die Zeitzone von geplanten Aktualisierungen, die maximale Anzahl an Wiederholungsversuchen für die erneute Planung fehlgeschlagener Aktualisierungen und die automatische Synchronisierung von Remote-Software-Repositoryys. Weitere Informationen finden Sie unter [Planung](#).
- **Peer Assisted Deployment** (Peer-gestützte Verteilung): Die Seite „Peer Assisted Deployment“ (Peer-gestützte Verteilung) unterstützt Sie bei folgenden Vorgängen:
  - [Voraussetzungen für PAD](#).
  - [Konfigurieren von PAD](#).
- **Wyse ThinOS**: Mit diesem Parameter können Sie den WTOS INI-Stammpfad und den Anmeldepfad anzeigen. Weitere Informationen finden Sie unter [Wyse ThinOS](#).

Themen:

- Manuelles Erstellen von Subnetzen
- Registrieren von Remote-Repositorys
- Hinzufügen von Benutzern aus lokalen Konten
- Hinzufügen von Benutzern und Gruppen von Domänencontroller und globalem Katalog
- Bearbeiten von Benutzerberechtigungen
- Löschen von Benutzern
- Konsole
- Konfigurieren der Geräteerkennung
- Über die Services
- Konfigurieren der Protokollierungsebenen
- Planung
- Peer-gestützte Verteilung
- Wyse ThinOS

## Manuelles Erstellen von Subnetzen

Mit WDM können Sie Subnetze manuell hinzufügen und konfigurieren.

**Dell Wyse Device Manager** | Search | wdm5administrator

Dashboard | Devices | Applications | Updates | Reports | System | **Subnets** | Repositories | Accounts | Console | Device Discovery | Services | Logging | Scheduling | Peer Assisted Deployment | Wyse ThinOS

**Subnets**

BROADCAST IP	ACTIVE IP	SUBNET MASK	DESCRIPTION
<input type="checkbox"/>	10.150.112.255	10.150.112.12	255.255.255.0

1 Subnet(s) Listed | 1 OF 1

**Add subnet**

Broadcast address:

Manually Create

Active IP address:

Subnet mask:

Software repository: MASTER FTP HTTPS CIFS [Edit](#)

Default groups: [Edit](#)

Contiguous bits

If your network uses Classless Inter-Domain Routing or supernetting, type the number of contiguous bits to configure your subnet mask.

Description

Override global preferences

For WDM Enterprise Edition customers if you want to override the global preferences for this subnet

On

Maximum Simultaneous Updates

The maximum number of device updates you can perform at the same time in subnet

[Reset](#)

Wake on LAN time out

**Dell Wyse Device Manager** | Search | wdm5administrator

Dashboard | Devices | Applications | Updates | Reports | System | **Subnets** | Repositories | Accounts | Console | Device Discovery | Services | Logging | Scheduling | Peer Assisted Deployment | Wyse ThinOS

**Subnets**

BROADCAST IP	ACTIVE IP	SUBNET MASK	DESCRIPTION
<input type="checkbox"/>	10.150.112.255	10.150.112.12	255.255.255.0

1 Subnet(s) Listed | 1 OF 1

**Add subnet**

If your network uses Classless Inter-Domain Routing or supernetting, type the number of contiguous bits to configure your subnet mask.

Description

Override global preferences

For WDM Enterprise Edition customers if you want to override the global preferences for this subnet

On

Maximum Simultaneous Updates

The maximum number of device updates you can perform at the same time in subnet

[Reset](#)

Wake on LAN time out

The length of time WDM attempts to wake a device on the subnet before stopping

[Reset](#)

Network Card Speed

This field is valid only in case of Merlin. It defines the network card speed.

Auto  100M-H  100M-F

[Reset](#)

[Hide advance settings](#)

Abbildung 37. Subnetz hinzufügen

So fügen Sie ein Subnetz hinzu und konfigurieren es:

- 1 Erweitern Sie im Strukturbereich der WDM-Konsole **System** und klicken Sie auf die Option **Subnet** (Subnetz).
- 2 Klicken Sie auf die Option **Add Subnet** (Subnetz hinzufügen).
- 3 Führen Sie einen der folgenden Aufgaben aus:
  - Wenn Sie eine Broadcast-Adresse für das Subnetz manuell eingeben möchten, wählen Sie **Manually create** (Manuell erstellen) und geben Sie die **Broadcast Address** (Broadcast-Adresse) ein.
  - Wenn Sie die Broadcast-Adresse für das Subnetz nicht manuell eingeben möchten, geben Sie die **IP Address** (IP-Adresse) ein (eine gültige IP-Adresse mit dem Subnetz), eine **Subnet Mask** (Subnetzmaske; Subnetzmaske für das Subnetz) und die **Contiguous Bits** (Angrenzende Bits) ein (wenn Ihr Netzwerk klassenloses domänenübergreifendes Routing oder Supernetting verwendet, geben Sie die Anzahl der angrenzenden Bits für die Konfiguration der Subnetzmaske ein).
- 4 Geben Sie eine **Description** (Beschreibung) zur Identifizierung des Subnetzes in der WDM--Datenbank ein.
- 5 Führen Sie einen der folgenden Aufgaben aus:
  - Wenn Sie die globalen Einstellungen für dieses Subnetz nicht überschreiben möchten, klicken Sie auf **OK**.
  - **(WDM Enterprise Edition only)** (Nur WDM Enterprise Edition) – Wenn Sie die globalen Einstellungen für dieses Subnetz überschreiben möchten, wählen Sie **Override Global Preferences** (Globale Einstellungen überschreiben) und füllen Sie die Felder für die Subnetz-Einstellungen mithilfe der folgenden Richtlinien aus und klicken Sie auf **OK**:
    - **Maximum Simultaneous Updates** (Maximale Anzahl gleichzeitiger Aktualisierungen) – Die maximale Anzahl an Geräteaktualisierungen, die gleichzeitig im Subnetz ausgeführt werden können.
    - **Wake On LAN Time Out (Secs.)** (Zeitüberschreitung Wake On LAN [Sek.]) – Die Zeitspanne, in der WDM versucht, ein Gerät im Subnetz zu reaktivieren.
    - **Network Card Speed** (Geschwindigkeit der Netzwerkkarte) – Dieses Feld gilt nur bei Merlin. Hier wird die Geschwindigkeit der Netzwerkkarte definiert. Zulässige Werte sind Auto (Automatisch), 100M-F, 100M-H.

Informationen über die Subnetz und dessen Einstellungen sind jetzt in der WDM--Datenbank gespeichert und WDM kann die Geräte im Subnetz erkennen.

 **ANMERKUNG:** Das Subnetz sollte mit den angegebenen angrenzenden Bits übereinstimmen.

## Registrieren von Remote-Repositorys

WDM Enterprise Edition ermöglicht die Installation mehrerer Repositorys in Ihrem Netzwerk. Mithilfe von Remote-Repositorys können Sie Netzwerkbandbreite sparen, da Softwareaktualisierungen lokal gespeichert und an Geräte verteilt werden, die sich im selben Subnetz wie jedes Repository befinden.

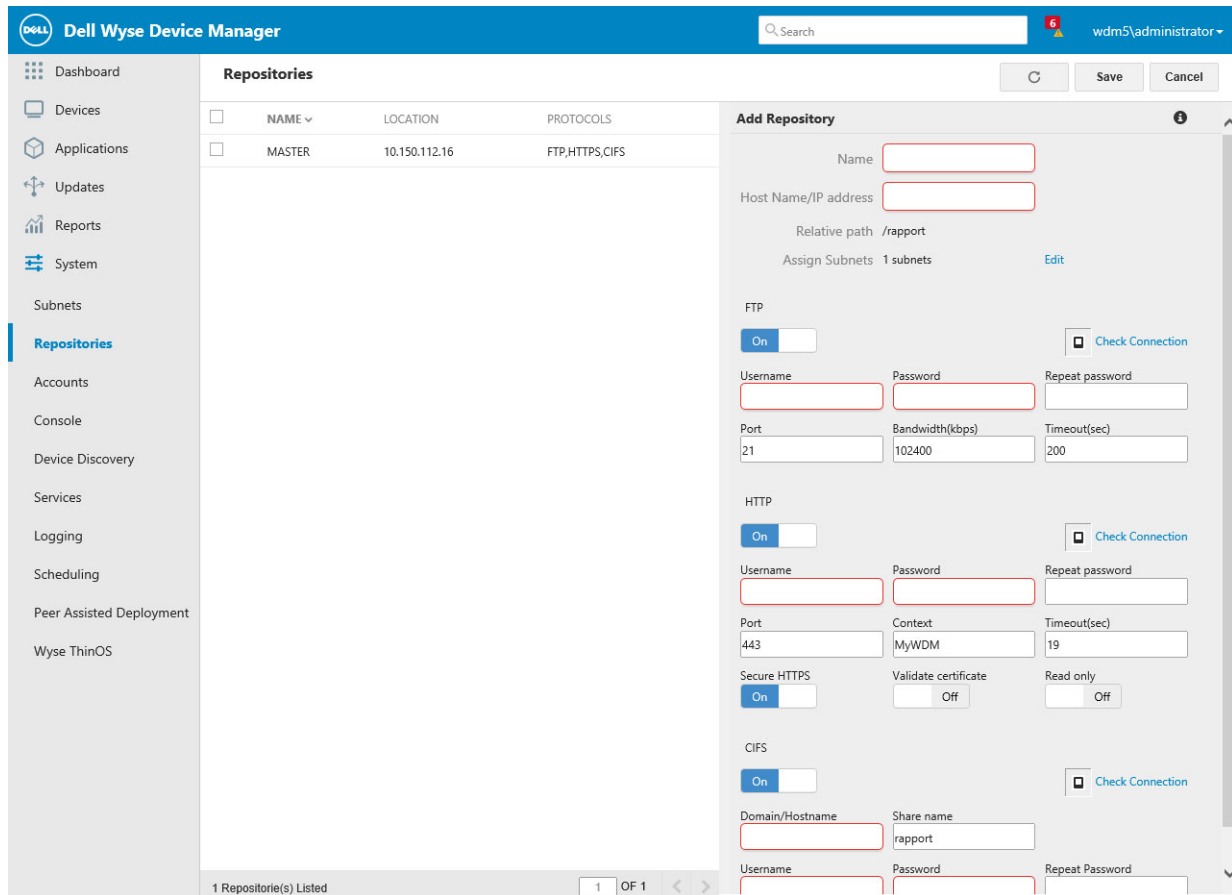


Abbildung 38. Registrieren von Remote-Repositories

Sie müssen folgende Punkte konfigurieren, bevor Sie Remote-Repositorys registrieren:

- WDM nennt das erste Repository immer *Master*. Etwaige zusätzliche Remote-Repositorys, die Sie installieren, können einen anderen Namen als Master haben.
- Wenn Sie keine weiteren Remote-Repositorys installieren, verwendet WDM das Master-Repository für alle Subnetze.
- Wenn Sie WDM-Komponenten getrennt bereitgestellt haben, wird empfohlen, das Master-Repository auf einem Rechner im selben Subnetz zu installieren, in dem Sie die anderen WDM-Komponenten installiert haben.

Stellen Sie vor der Registrierung sicher, dass Sie folgende Komponenten erfolgreich installiert haben:

- WDM Enterprise Edition in Ihrem Netzwerk
- Alle Remote-Repositorys zur Herstellung einer Verbindung mit diesen.

So registrieren Sie ein Remote-Repository:

- 1 Erweitern Sie in der WDM-Konsole den Abschnitt **System**.
- 2 Klicken Sie auf die Option **Repositories** (Repositorys). Um ein neues Repository zu konfigurieren, klicken Sie auf die Option **Add Repository** (Repository hinzufügen) und führen Sie die Konfigurationen mithilfe der folgenden Richtlinien durch:
  - **Bereich mit Informationen über das Repository:**
    - **Name** – Geben Sie den Namen zur Identifizierung des Software-Repository an.
    - **Host Name/IP address** (Host-Name/IP-Adresse) – Geben Sie **Host-Namen** oder die **IP-Adresse** des Servers an, auf dem das Repository konfiguriert werden soll.
    - **Relative Path** (Relativer Pfad) – Enthält den Stammpfad des WDM-Software-Repository.

- **Assign Subnets** (Subnetze zuweisen) – Ermöglicht die Zuweisung eines Subnetzes zu einem Repository.

• **FTP-Bereich:**

- **Username** (Benutzername) – Benutzername für den Zugriff auf das FTP-Repository.
- **Password** (Kennwort) – Kennwort für den Zugriff auf das FTP-Repository.
- **Repeat Password** (Kennwort wiederholen) – Geben Sie das Kennwort für den Zugriff auf das FTP-Repository zur Bestätigung erneut ein.
- **Bandwidth** (Bandbreite) – Menge der Bandbreite in Kbit/s, die für die Datenübertragung zum und vom Software-Repository verwendet wird.
- **Timeout (sec)** (Zeitüberschreitung (Sek.)) – Zeit in Sekunden, in der die Verbindung für jede Sitzung offen bleiben soll.

• **HTTP-Bereich:**

- **Username** (Benutzername) – Benutzername für den Zugriff auf das HTTP-Repository.
- **Password** (Kennwort) – Kennwort für den Zugriff auf das HTTP-Repository.
- **Repeat Password** (Kennwort wiederholen) – Geben Sie das Kennwort für den Zugriff auf das HTTP-Repository zur Bestätigung erneut ein.
- **Port Number** (Portnummer) – Zeigt die Portnummer für die HTTP-Kommunikation an. Die Standardportnummer für HTTP ist 80 und für HTTPS lautet sie 443.
- **Context** (Kontext) – Zeigt den Pfad des virtuellen Verzeichnisses für die HTTP-Kommunikation an.
- **Timeout (sec)** (Zeitüberschreitung (Sek.)) – Zeit in Sekunden, in der die Verbindung für jede Sitzung offen bleiben soll.
- **Secure HTTPS** (Sicheres HTTPS) – Wenn aktiviert, ist die HTTP-Kommunikation für das Repository sicher.
- **Validate Certificate** (Zertifikat validieren) – Wenn aktiviert, ist die Zertifikatüberprüfung für die HTTPS-Kommunikation aktiviert.
- **Read Only** (Schreibgeschützt) – Wenn aktiviert, ist das Repository schreibgeschützt.

• **CIFS-Bereich:**

- **Domain/Host Name** (Domänen-/Hostname) – Geben Sie den Domänen- oder Hostnamen des Repository-Servers an.
- **Share Name** (Freigabename) – Geben Sie den Namen des freigegebenen Ordners an, in dem das Paket bereitgestellt werden muss.
- **Username** (Benutzername) – Geben Sie den Benutzernamen des Benutzers an, der Zugriff auf den freigegebenen Ordner hat.
- **Password** (Kennwort) – Kennwort des CIFS-Benutzers, der Zugriff auf den freigegebenen Ordner hat.
- **Repeat Password** (Kennwort wiederholen) – Bestätigen Sie das Kennwort des CIFS-Benutzers, der Zugriff auf den freigegebenen Ordner hat.

3 Klicken Sie auf **Save** (Speichern).

**ⓘ ANMERKUNG:** WDM testet die Verbindung zum Remote-Repository, das Sie hinzugefügt haben, um sicherzustellen, dass es ordnungsgemäß eingerichtet wurde. Sie können die Verbindung mit einem Remote-Repository jederzeit durch Klicken auf **Check Connection (Verbindung überprüfen)** prüfen.

Das neue Remote-Repository ist nun fertig eingerichtet und in der WDM-Datenbank registriert. Sie können das Remote-Repository nun einem Subnetz zuweisen.

**ⓘ ANMERKUNG:** WDM speichert alle Pakete, das Sie registrieren, in seinem Master-Repository. Wenn Sie eine Aktualisierung für ein Gerät in einem Subnetz mit Zugriff auf ein lokales Repository durchführen, können Sie Remote-Repositorys synchronisieren.

## Hinzufügen von Benutzern aus lokalen Konten

Sie können WDM--Benutzer aus lokalen Computerkonten hinzufügen.

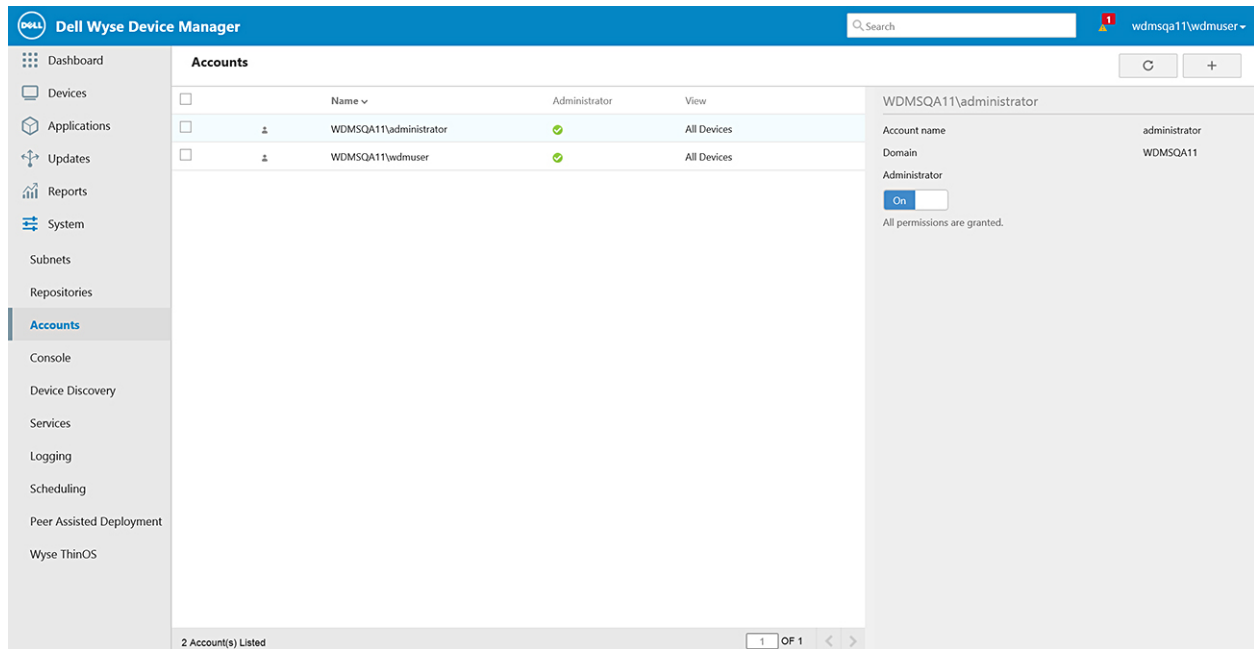


Abbildung 39. Konten

**ANMERKUNG:** Bevor Sie einen WDM--Benutzer hinzufügen können, muss der Benutzer bereits in Liste der Benutzer für die Windows-Domänen aufgeführt sein, in der Sie WDM installiert haben.

So fügen Sie einen Benutzer aus einem lokalen Computerkonto hinzu:

- 1 Erweitern Sie in der WDM-Konsole den Abschnitt **System**.
- 2 Wählen Sie den Namen des Benutzer, den Sie hinzufügen möchten, als WDM--Benutzer aus und klicken Sie auf **Add** (Hinzufügen).
- 3 Klicken Sie auf **OK**, um den neuen Benutzer zur Liste der WDM--Benutzer hinzuzufügen.

**ANMERKUNG:** Neue Benutzer haben keine Berechtigung. Dafür müssen Sie die Benutzerberechtigungen bearbeiten.

## Hinzufügen von Benutzern und Gruppen von Domänencontroller und globalem Katalog

Als Administrator können Sie WDM--Benutzer und -Gruppen aus dem Active Directory hinzufügen.

**ANMERKUNG:** Bevor Sie eine WDM--Gruppe hinzufügen können, muss die Gruppe bereits im Active Directory vorhanden sein.

So fügen Sie einen Benutzer oder eine Gruppe aus dem Active Directory hinzu:

- 1 Erweitern Sie in der WDM-Konsole den Abschnitt **System**.
- 2 Wählen Sie die Option **Domain Controller** (Domänen-Controller), wenn Sie Benutzer aus der Domäne auswählen möchten.
- 3 Geben Sie eine IP-Adresse bzw. einen Namen ein oder wählen Sie einen Domänen-Controller aus der Liste aus. Der Server, auf dem Sie WDM installiert haben, muss Teil der Domäne sein.
- 4 Wählen Sie die gewünschte Suchkriterienoption.

**ANMERKUNG:** Wenn Sie die Option **Show user only** (Nur Benutzer anzeigen), müssen Sie den genauen Namen des Benutzers in das Textfeld eingeben, die angezeigt wird.

- 5 Klicken Sie auf **Search** (Suche), um die Benutzer und Gruppen anzuzeigen, die Ihren Kriterien entsprechen.
- 6 Klicken Sie auf **Add** (Hinzufügen), um Benutzer und Gruppen in WDM zu integrieren.

## Bearbeiten von Benutzerberechtigungen

Als Administrator können Sie die Berechtigungen von WDM-Benutzern bearbeiten.

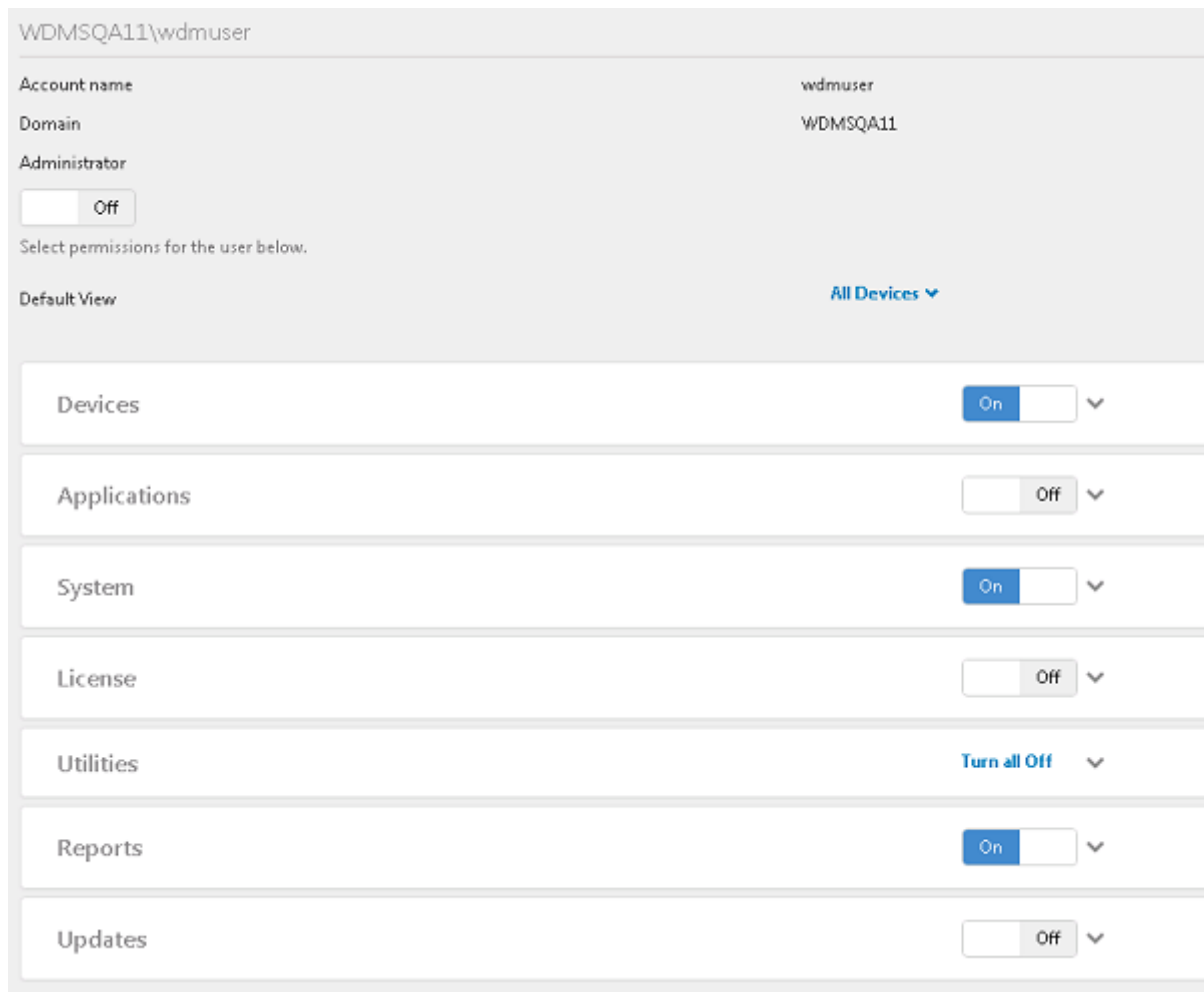


Abbildung 40. Konten

**ANMERKUNG:** Als Administrator können Sie die Berechtigungen bearbeiten, allerdings besitzt der Standard-Administrator alle Berechtigungen, die Sie nicht ändern können.

So bearbeiten Sie Benutzerberechtigungen:

- 1 Erweitern Sie im Strukturbereich der WDM-Konsole **System** und klicken Sie auf die Option **Accounts** (Konten).
- 2 Klicken Sie auf die Option **Add** (Hinzufügen), um Benutzer oder Benutzergruppen hinzuzufügen.
- 3 Klicken Sie auf die Registerkarte **Local** (Lokal), um die Liste der WDM-Benutzer anzuzeigen.
- 4 Wählen Sie den gewünschten Benutzer aus der Liste der Benutzer aus und klicken Sie auf **Add** (Hinzufügen), um das Dialogfeld „User Permissions“ (Benutzerberechtigungen) zu öffnen.
- 5 Klicken Sie auf die Option „On/Off“ (Ein/Aus), um die Option **Administrator** zu aktivieren oder zu deaktivieren.

**ANMERKUNG:** Wenn Sie die Option **Administrator** aktivieren, werden alle Berechtigungen ausgewählt.

- 6 Klicken Sie auf die Option „On/Off“ (Ein/Aus), um die folgenden Benutzerberechtigungen zu aktivieren bzw. zu deaktivieren:

**ANMERKUNG:**

Die Einstellung „On/Off“ (Ein/Aus) einer Gruppe wird auf Grundlage der Änderungen an bestimmten Berechtigungen innerhalb einer Gruppe geändert.

Gruppenberechtigung ist auf „Turn off all“ (Alle Aus) festgelegt, wenn die Einstellung für mindestens eine Berechtigung von „ON“ (Ein) zu „OFF“ (Aus) geändert wird.

Gruppenberechtigung ist auf „OFF“ (Aus) festgelegt, wenn alle Berechtigungen auf „OFF“ (Aus) festgelegt sind.

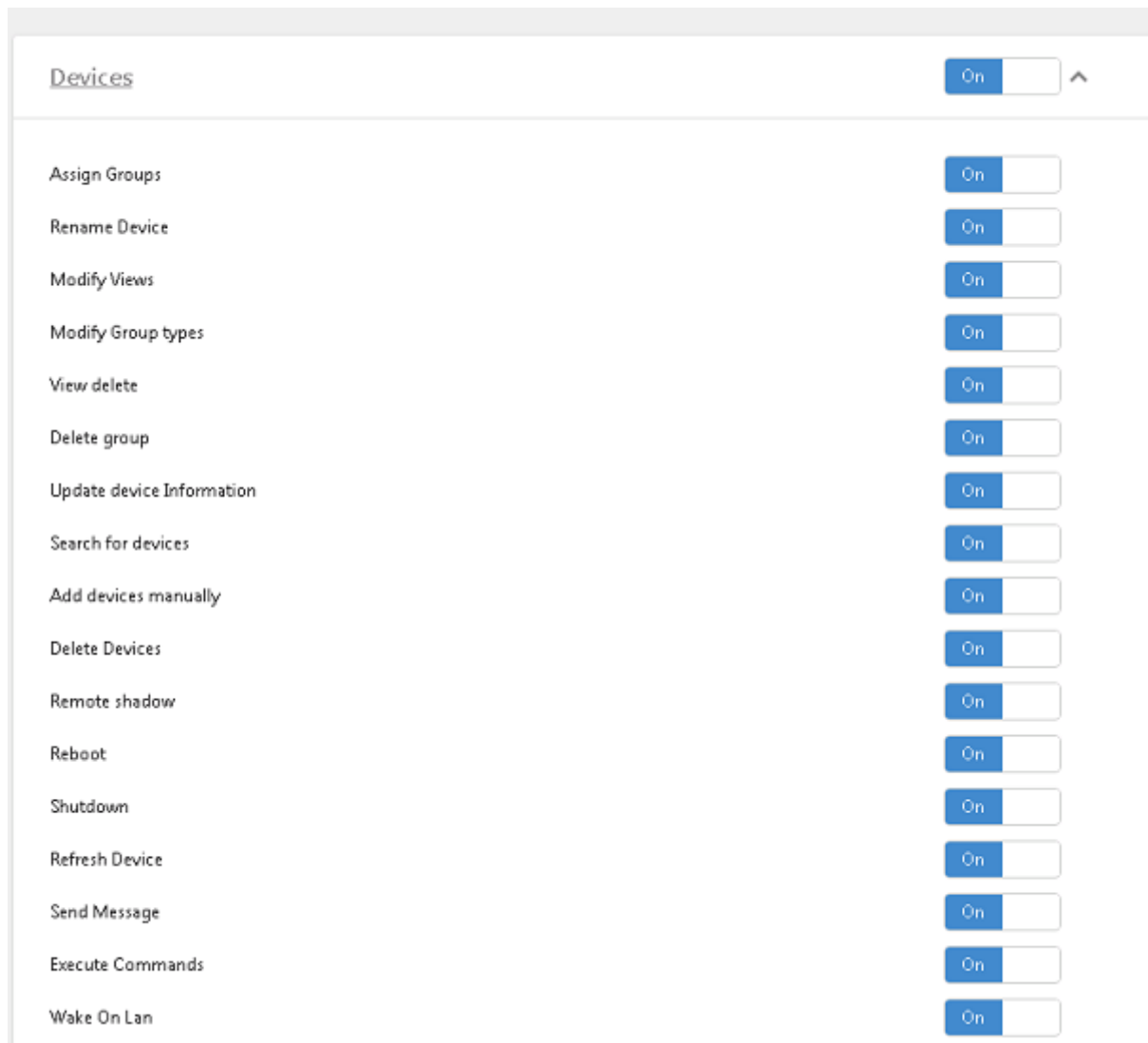


Abbildung 41. Geräte

Tabelle 14. Geräte

Geräte
Assign Group (Gruppe zuweisen)
Modify Views (Ansichten ändern)
Modify Groups types (Gruppentypen ändern)
View Delete (Ansicht löschen)
Update Device Information (Geräteinformationen aktualisieren)
Search for devices (Geräte suchen)
Aktualisierung
Add devices manually (Geräte manuell hinzufügen)
Delete Packages (Pakete löschen)
Delete Devices (Geräte löschen)

Geräte
Remote Shadow (Remote-Spiegelung)
Neustart
Herunterfahren
Refresh Device (Gerät aktualisieren)
Send Message (Nachricht senden)
Execute Commands (Befehle ausführen)
Wake on LAN
Relay Wake on LAN (Wake-On-LAN übertragen)
Exclude from PAD Repository (Von PAD-Repository ausschließen)
Include in PAD Repository (In PAD-Repository einbeziehen)
Create and View Log (Protokoll erstellen und anzeigen)
Get Device Log (Geräteprotokoll abrufen)
Get Image (Image erstellen)

Applications  Off ^

---

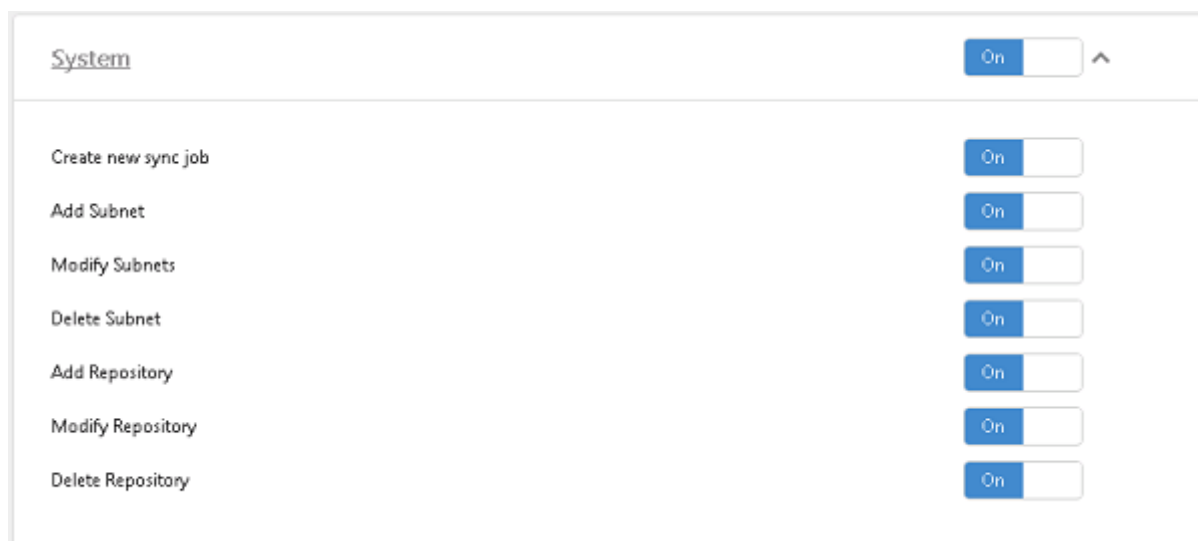
Modify Packages	<input type="checkbox"/> Off
Delete Packages	<input type="checkbox"/> Off
Distribute packages	<input type="checkbox"/> Off
Create Package	<input type="checkbox"/> Off
View package script	<input type="checkbox"/> Off
Export package	<input type="checkbox"/> Off
Enable distribution	<input type="checkbox"/> Off
Disable distribution	<input type="checkbox"/> Off
Deploy via peers	<input type="checkbox"/> Off
Create device configuration	<input type="checkbox"/> Off
Save script	<input type="checkbox"/> Off
Edit Config	<input type="checkbox"/> Off

---

Abbildung 42. Anwendungen

**Tabelle 15. Anwendungen**

Anwendungen
Create Packages (Pakete erstellen)
Modify Packages (Pakete ändern)
Distribute Packages (Pakete verteilen)
Configure Packages (Pakete konfigurieren)
Register Packages (Pakete registrieren)
View Packages Script (Paket-Skripts anzeigen)
Export Packages (Pakete exportieren)
Disable distribution (Verteilung deaktivieren)
Deploy via peers in subnet (Verteilung über Peers im Subnetz)
Create new configuration (Neue Konfiguration erstellen)
Save script (Skript speichern)
Edit Config (Konfiguration bearbeiten)



**Abbildung 43. System**

**Tabelle 16. System**

System
Create new sync Job (Neue Synchronisierungsaufgabe erstellen)
Subnetz hinzufügen
Modify Subnets (Subnetze ändern)
Delete Subnet (Subnetz löschen)
Add repository (Repository hinzufügen)
Modify Repository (Repository ändern)
Delete Repository (Repository löschen)



Abbildung 44. Lizenz

Tabelle 17. Lizenz

Lizenz
Add License (Lizenz hinzufügen)
Entfernen Sie Lizenzinstanzen

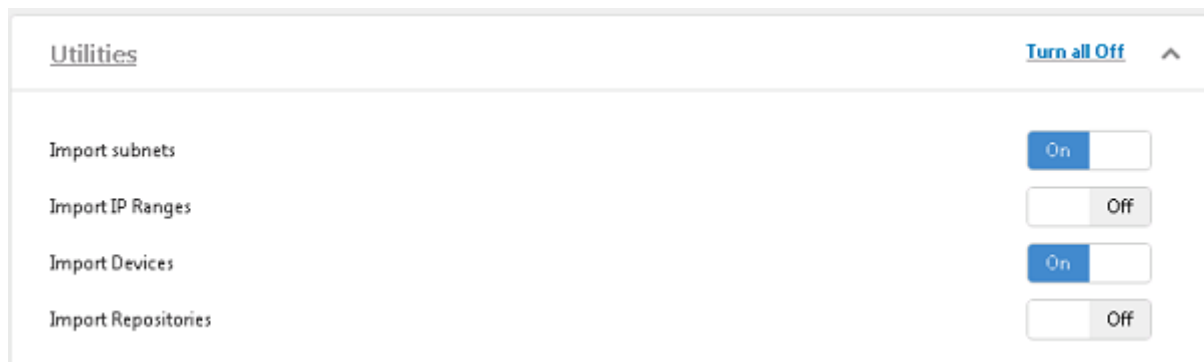


Abbildung 45. Utilitys

Tabelle 18. Dienstprogramme

Dienstprogramme
Import Subnets (Subnetze importieren)
Import IP Ranges (IP-Bereiche importieren)
Import Devices (Geräte importieren)
Import Repositories (Repositorys importieren)

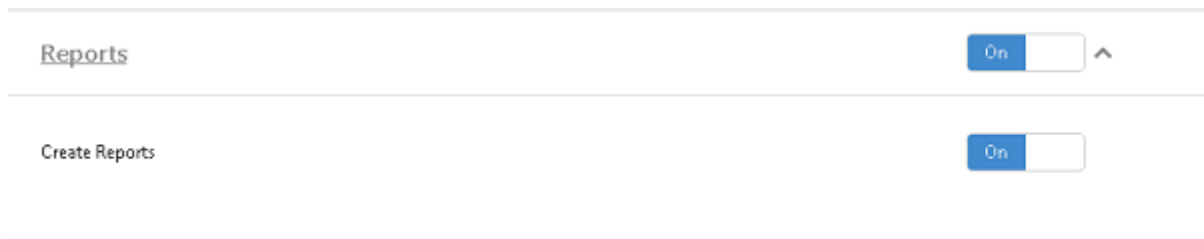


Abbildung 46. Berichte

Tabelle 19. Berichte

Berichte
Create Reports (Berichte erstellen)

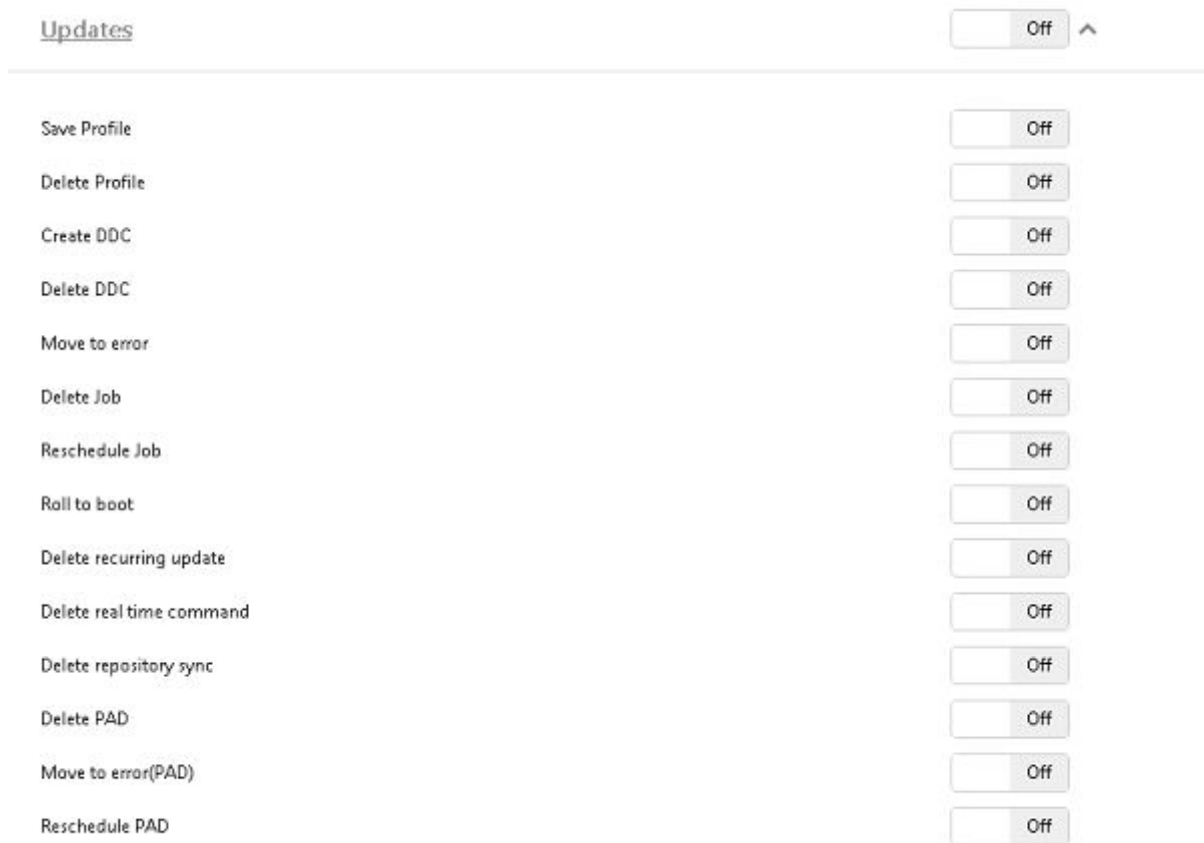


Abbildung 47. Aktualisierungen

Tabelle 20. Aktualisierungen

Aktualisierungen
Save Profile (Profil speichern)
Delete Profile (Profil löschen)
Create DDC (DDC erstellen)
Delete DDC (DDC löschen)

Aktualisierungen
Move to error (Zum Fehler wechseln)
Delete job (Aufgabe löschen)
Reschedule Job (Aufgabe neu planen)
Roll to boot (Roll zum Start)
Delete recurring update (Wiederkehrendes Update löschen)
Delete real time command (Befehl in Echtzeit löschen)
Delete repository sync (Repository-Synchronisierung löschen)
Delete PAD (PAD löschen)
Move to Error(PAD) (Zum Fehler wechseln [PAD])
Deploy via peers (Verteilung über Peers)
Reschedule PAD (PAD neu planen)

## Löschen von Benutzern

Als Administrator können Sie WDM-Benutzer löschen.

**ⓘ | ANMERKUNG: Sie können sich nicht selbst als Benutzer löschen.**

So löschen Sie einen Benutzer:

- 1 Erweitern Sie in der WDM-Konsole den Abschnitt **System** und klicken Sie auf **Accounts (Konten)**, um eine Liste der WDM-Benutzer anzuzeigen.
- 2 Aktivieren Sie das Kontrollkästchen des Benutzers, der aus der Liste der Benutzer entfernt werden soll, und wählen Sie **Delete (Löschen)** aus.
- 3 Klicken Sie auf **Delete (Löschen)**, um die Löschung zu bestätigen.

**ⓘ | ANMERKUNG: Wenn Sie einen Benutzer löschen, werden die privaten Geräteansichten des Benutzers ebenfalls gelöscht.**

## Konsole

Klicken Sie auf **Console** (Konsole) in der Systemliste, um den Gerätestatus anzuzeigen.

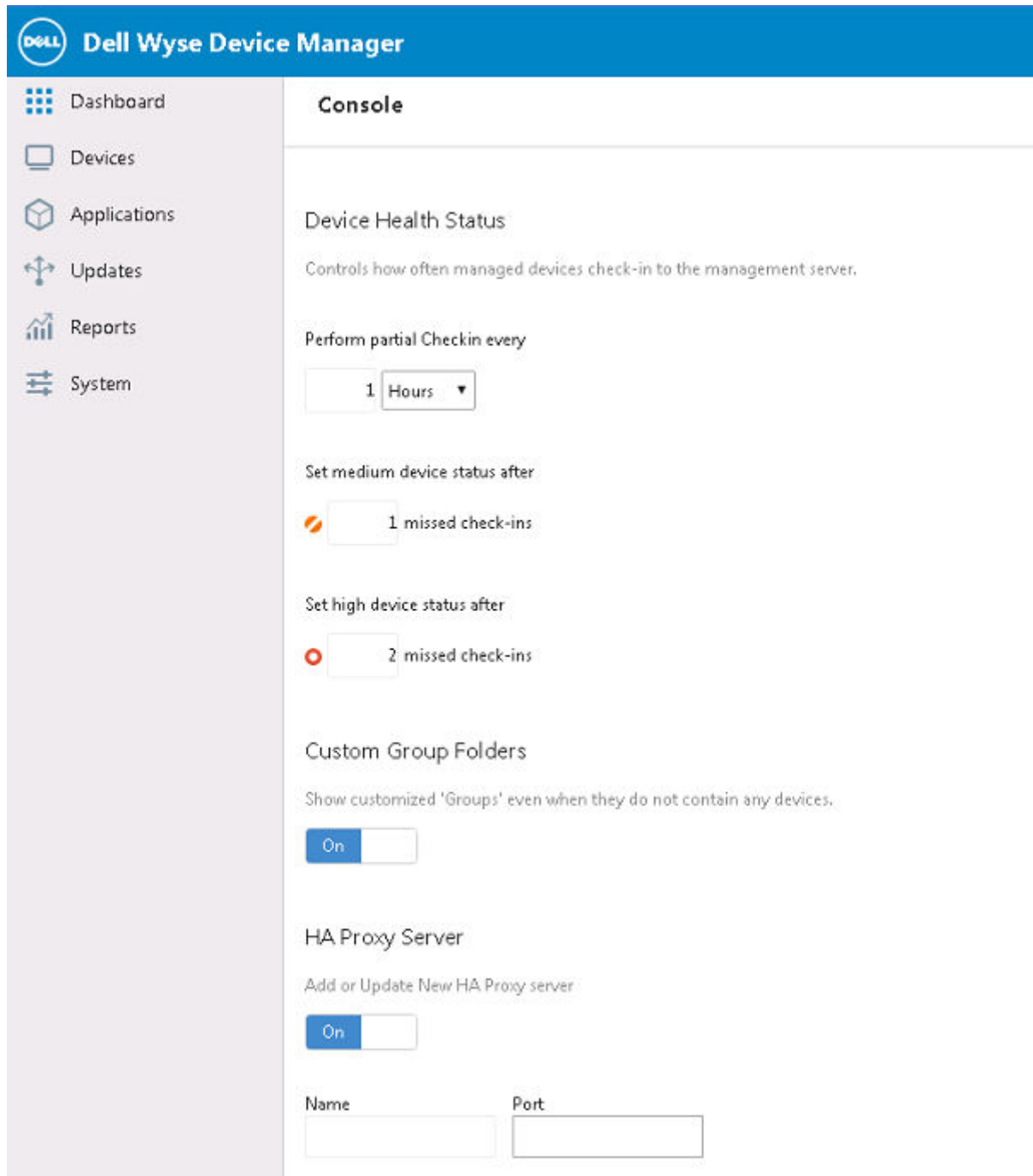


Abbildung 48. Konsole

- 1 Geben Sie folgende Informationen ein:
  - **Device Health Status** (Gerätestatus):
    - **Perform a partial check-in every** (Teilweises Einchecken durchführen alle) – Legen Sie die Häufigkeit für partielles Einchecken für alle Geräte fest, indem Sie eine Zahl und eine Zeiteinheit (Minuten, Stunden, Tage) auswählen. Die Standardeinstellung ist **1 Hour** (1 Stunde). Teilweises Einchecken wird regelmäßig im angegebenen Zeitabstand durchgeführt, um den Gerätestatus (rot, gelb, grün) zu ermitteln. Teilweises Einchecken erfordert weniger Netzwerkbandbreite als vollständiges Einchecken. Dies ist wichtig, wenn die WDM-Installation tausende Geräte enthält. Änderungen an der Häufigkeit für das Einchecken werden erst wirksam, wenn die festgelegte Zeit für das Einchecken oder das Gerät aktualisiert werden.
    - **Medium Device Status** (Mittlerer Gerätestatus) – Wählen Sie die Anzahl der verpassten Anmeldungen, um den mittleren Gerätestatus festzulegen.
    - **High Device Status** (Hoher Gerätestatus) – Wählen Sie die Anzahl der verpassten Anmeldungen, um den hohen Gerätestatus festzulegen.

- **Custom Group Folders** (Benutzerdefinierte Gruppenordner) – Wählen Sie diese Option aus, wenn Sie leere Ordner im Geräte-Manager anzeigen möchten, wenn Sie benutzerdefinierte Gruppen für Ihre Gerätansichten erstellen.
- **HA Proxy Server** (HA-Proxy-Server) – Wählen Sie diese Option aus, wenn Sie einen neuen HA-Proxy-Server hinzufügen oder aktualisieren möchten. Geben Sie den Namen und den Port in das entsprechende Feld ein, um einen neuen HA-Proxy-Server hinzuzufügen oder zu aktualisieren.
- **Remote Sessions** (Remote-Sitzungen) – Diese Option gilt für Windows-, Linux- und Thin OS (WTOS)-Geräte, für die Sie Remote-Sitzungen konfiguriert haben. Wenn Sie diese Option auswählen, werden die Details der Remote-Sitzungen für dieses Gerät in der Registerkarte **Remote Sessions** (Remote-Sitzungen) auf der Seite **Devices** (Geräte) gelistet. Diese Daten sind für die Abrechnung der Endbenutzer für die Remote-Sitzungen hilfreich.

Klicken Sie für Windows- und Linux-Geräte auf die Schaltfläche **+** zum Hinzufügen eines Servers, um Remote-Sitzungsserver für VMware und Citrix hinzuzufügen.

Geben Sie die folgenden Details zum Hinzufügen eines VMware Remote-Sitzungsservers ein:

- Host oder IP
- Database Name (Name der Datenbank)
- Benutzername der Datenbank
- Kennwort der Datenbank
- Authentifizierung
- Präfix

Geben Sie die folgenden Details zum Hinzufügen eines Citrix Remote-Sitzungsservers ein:

- Host oder IP
- Domain
- Version
- Benutzername
- Kennwort

Klicken Sie auf das Häkchen, um die Informationen zu bestätigen.

Sie können auch die Anzahl der Tage zum Löschen älterer Daten angeben. Die Standardeinstellung ist 45 Tage.

- 2 Mit der Standardgerätekonfiguration können Sie Firmware- oder SW-Paketen oder beide Varianten auf Ihre Thin Client-Geräte automatisch übertragen. Mit dem Zuweisen von DDCs zu Gerätegruppen wird die Konformität gewährleistet und Sie können maßgeschneiderte Images und Konfigurationen zielgerichtet für Funktionsbereiche in Ihrem Unternehmen bereitstellen.
- 3 Geben Sie die folgenden Einzelheiten an:

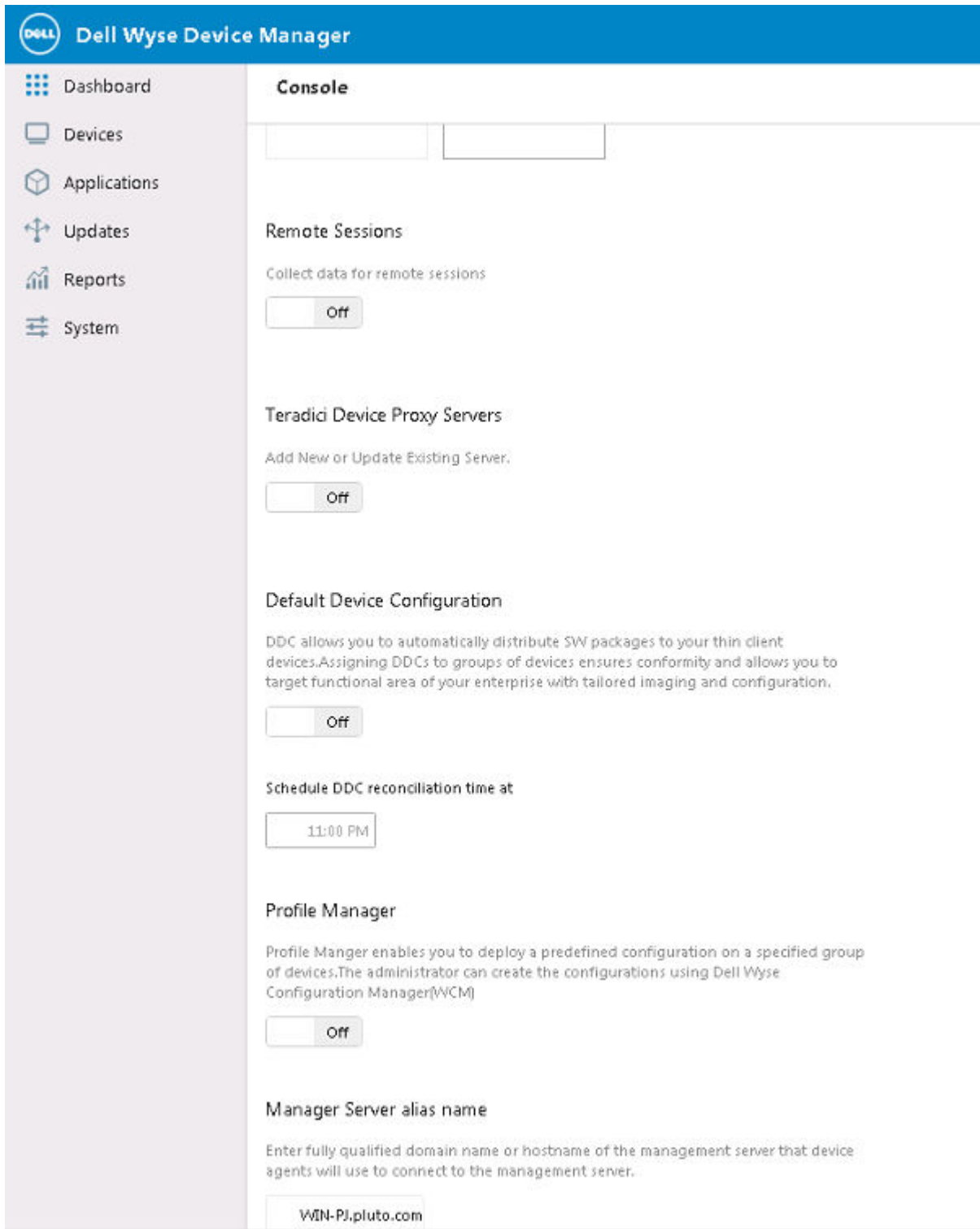


Abbildung 49. Konsole

- **Teradici Device Proxy Server** – Wählen Sie diese Option aus, um einen neuen Server hinzuzufügen oder den vorhandenen Server zu aktualisieren.

**Default Device Configuration** (Standardgerätekonfiguration) – Nur WDM Enterprise Edition) Diese Option ermöglicht die automatische Verteilung von Softwarepaketen auf Ihre Thin Client-Geräte. Durch die Zuweisung von DDCs zur Gruppe von

Geräten wird Konformität gewährleistet und das Abzielen auf den Funktionsbereich des Unternehmens mit zugeschnittener Image-Erstellung und Konfiguration ermöglicht.

- **Schedule DDC Reconciliation at** (DDC-Abstimmung planen um) – Gegen Sie die Zeit ein.

4 Klicken Sie auf **Profil Manager** (Profil-Manager).

in der Device Manager-Struktur, um das Fenster **Profile Manager Preferences** (Einstellungen für den Profil-Manager) zu öffnen. Profile Manager ermöglicht die Bereitstellung einer vordefinierten Konfiguration für eine bestimmte Gruppe von Geräten. Sie können die Konfigurationen mithilfe von Dell Wyse Configuration Manager (WCM) erstellen.

5 Geben Sie die folgenden Einzelheiten an:

- a Wählen Sie **Enable Profile Manager** (Profil-Manager aktivieren) im Fensterbereich der Voreinstellungen für den Profil-Manager.
- b Klicken Sie auf **OK**, um die Einstellungen zu speichern.

6 Klicken Sie auf die Option **Management Server alias name** (Alias-Name für Verwaltungsserver), um einen vollqualifizierten Domännennamen oder Hostnamen des Verwaltungsservers einzugeben, den die Geräte-Agents zur Verbindung mit dem Verwaltungsserver verwenden.

7 Klicken Sie auf **Save** (Speichern).

## Konfigurieren der Geräteerkennung

Die Geräteerkennung konfiguriert das Agent-Erkennungsverhalten nach der ersten Anmeldung beim Verwaltungsserver.

**Dell Wyse Device Manager** Search 6 wdm5\administrator

- Dashboard
- Devices
- Applications
- Updates
- Reports
- System
- Subnets
- Repositories
- Accounts
- Console
- Device Discovery**
- Services
- Logging
- Scheduling
- Peer Assisted Deployment
- Wyse ThinOS

### Device Discovery

Device agent discovery

Configure agents discovery behaviour after first check-in to management server. For automatic discovery of devices using DHCP or DNS. Please refer to documentation.

DNS Hostname  Off

DNS SRV record lookup  Off

DHCP Option tags  Off

Manual discovery from Device Manager  Off

Device autodiscover management server after  missed check-ins.

Device discovery timeout  seconds

DHCP discovery

Enables discovery of devices in the local subnet of the management server.

On

DHCP options tags used by agents

**Dell Wyse Device Manager** Search 6 wdm5\administrator

- Dashboard
- Devices
- Applications
- Updates
- Reports
- System
- Subnets
- Repositories
- Accounts
- Console
- Device Discovery**
- Services
- Logging
- Scheduling
- Peer Assisted Deployment
- Wyse ThinOS

### Device Discovery

DNS Hostname  Off

DNS SRV record lookup  Off

DHCP Option tags  Off

Manual discovery from Device Manager  Off

Device autodiscover management server after  missed check-ins.

Device discovery timeout  seconds

DHCP discovery

Enables discovery of devices in the local subnet of the management server.

On

DHCP options tags used by agents

Management server IP	186
Management server hostname	194
Management server port	192
Secure port	190

Abbildung 50. Geräteerkennung

- **DNS Hostname** (DNS-Hostname) – Wählen Sie diese Option, wenn Sie zulassen möchten, dass Geräte für die Erkennung des WDM-Servers die DNS Hostname-Suchmethode verwenden.
- **DNS SRV record lookup** (DNS SRV-Datensatzsuche) – Wählen Sie diese Option, wenn Sie zulassen möchten, dass Geräte für die Erkennung des WDM-Servers die DNS SRV-Datensatzsuche verwenden.
- **DHCP option tags** (DHCP-Option-Tag) – Wählen Sie diese Option, wenn Sie zulassen möchten, dass Geräte für die Erkennung des WDM-Servers DHCP-Option-Tags verwenden.
- **Manual discovery from Device Manager** (Manuelle Erkennung aus Geräte-Manager) – Wählen Sie diese Option, wenn Sie das Gerät anhand von IP-Bereichs- oder die Subnetzerkennungsmethoden im Fenster „Find Device“ (Gerät suchen) erkennen möchten.
- **Device autodiscover management server after** (Gerät für automatische Neuerkennung vom Verwaltungsserver nach): Wählen Sie die Anzahl der verpassten Anmeldungen aus, nach der die Optionen für die automatische Erkennung aktiviert werden. Das Gerät aktiviert die automatische Erkennung, wenn die Anzahl der verpassten Anmeldungen den angegebenen Wert überschreitet.
- **Device discovery timeout** (Zeitüberschreitung für Geräteerkennung) – Geben Sie den maximalen Zeitraum für WDM ein, um alle Geräte in Ihrem Netzwerk zu erkennen.
- **DHCP discovery** (DHCP-Erkennung) – Diese Option aktiviert die Erkennung von Geräten im lokalen Subnetz des Verwaltungsservers.

## Über die Services

Auf der Seite mit den Services werden Ihnen die Details zum TFTP-Server und zu Wake On LAN angezeigt.

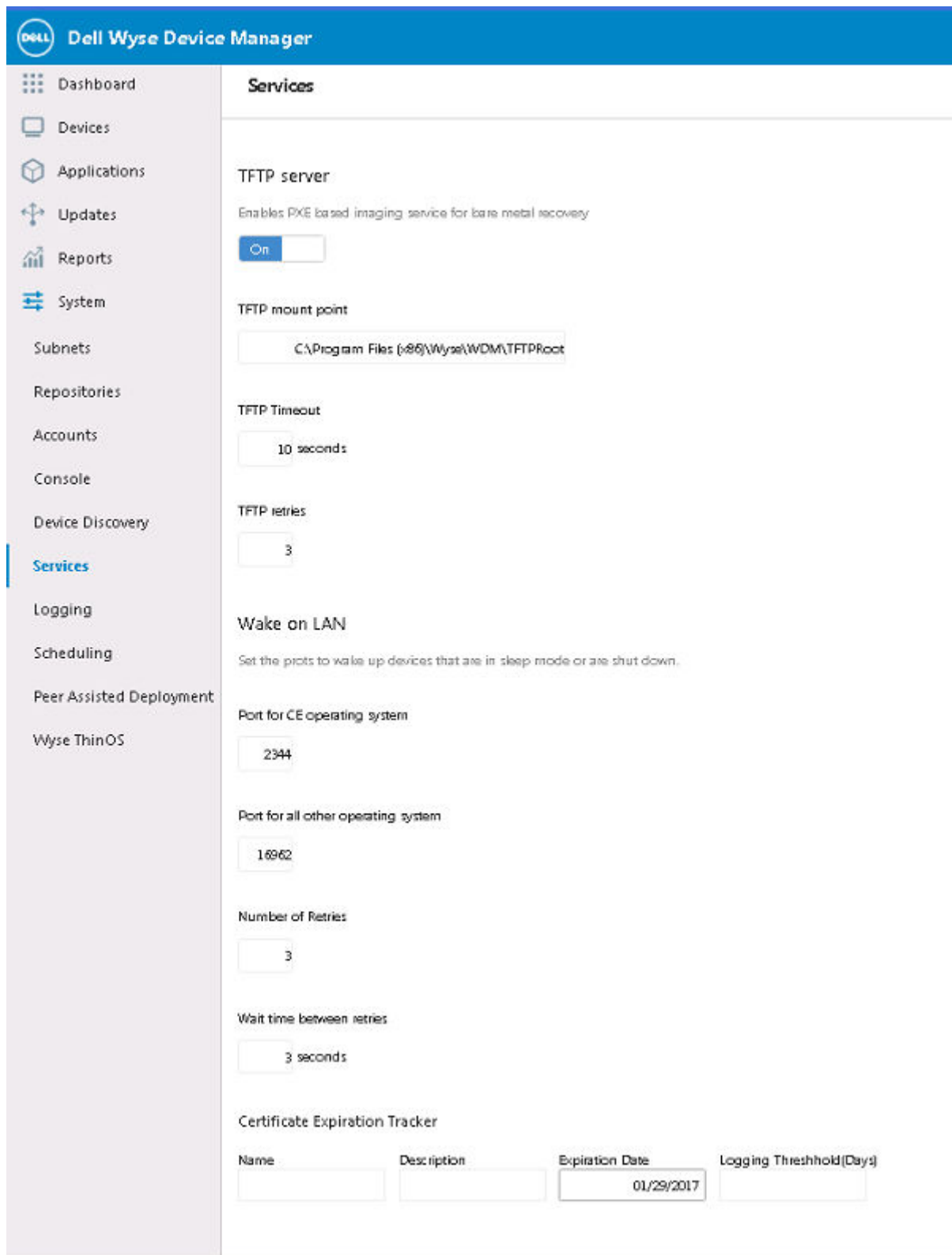


Abbildung 51. Dienste

- **TFTP Server** (TFTP-Server): Aktivieren Sie diese Option, damit WDM bei der Aktualisierung des Geräts das Trivial File Transfer Protocol (TFTP) verwenden kann.

- **TFTP Mount Point** (TFTP-Bereitstellungspunkt): Zeigt den TFTP-Bereitstellungspunkt, der von WDM während der Installation festgelegt wurde. Normalerweise ist dies das TFTP-Stammverzeichnis (WDM) unter dem FTP-Stammverzeichnis, das von dem Master-Repository verwendet wird.
- **TFT time out** (TFTP-Zeitlimit): Gibt das Zeitintervall (in Sekunden) an, während dessen das Gerät auf eine Verbindung mit dem TFTP-Service wartet, bevor es erneut versucht, eine Verbindung herzustellen.
- **TFT retries** (TFTP-Wiederholungsversuche): Gibt die Anzahl der Wiederholungsversuche an, die das Gerät bei der Verbindung mit dem TFTP-Service durchführt, bevor es fehlschlägt.
- **Wake On Lan:** Ermöglicht es Ihnen, Geräte zu aktivieren, die sich im Ruhemodus befinden oder heruntergefahren wurden.
  - Set the Wake On Lan tries (Anzahl der Wake On LAN-Versuche festlegen) Anzahl der WOL-Versuche, die der Dienst unternimmt, und die Verzögerung zwischen WOL-Wiederholungen (Sekunden). Die Dauer der Pause, die WDM zwischen den WOL-Versuchen für dasselbe Gerät einhält.

Für CE-Geräte lautet der standardmäßige WOL-Port 2344, für alle übrigen Geräte ist dies 16962. Sie können stattdessen einen benutzerdefinierten Port verwenden, legen Sie jedoch für den Firewall-Port eine Ausnahme fest, wenn die Firewall aktiviert ist.

- **Certificate Expiration Tracker:** WDM bietet ein Utility, der den Ablauf von Zertifizierungsstellen-Zertifikaten überwacht. Der WDM-Administrator muss manuell grundlegende Informationen über Zertifizierungsstellenzertifikate einschließlich Name, Beschreibung, Ablaufdatum und Protokollierungsschwellenwert eingeben. WDM überwacht diese Informationen und warnt den Administrator bei Ablauf des Zertifikats. Diese Informationen werden im Windows Event Viewer protokolliert.
  - **Name** – Geben Sie den Namen für den Certificate Expiration Tracker.
  - **Description** (Beschreibung) – Geben Sie eine Beschreibung für diesen ein.
  - **Expiration Date** (Ablaufdatum) – Wählen Sie das Ablaufdatum für Certificate Expiration Tracker aus.
  - **Logging Threshold(Days)** (Protokollierungsschwellenwert (Tage)) – Dies ist der Zeitraum, zu dem Sie die Warnmeldung bei Ablauf des Zertifikats erhalten möchten. Wenn Ihr Zertifikat beispielsweise am Datum x abläuft und Sie als Wert für **Logging Threshold(Days)** (Protokollierungsschwellenwert (Tage)) 30 Tage angegeben haben, erhalten Sie im Event Viewer ab dem Zeitpunkt x-30 einmal täglich eine Warnmeldung. Sie wird im Event Viewer als Fehlermeldung wie unten dargestellt angezeigt:

## Konfigurieren der Protokollierungsebenen

Mit diesem Parameter können Sie die folgenden verschiedenen Konfigurationsprotokollierungsebenen anzeigen. Bei einer höheren Protokollierungsebene werden mehr Daten in der Datenbank gespeichert. Dies kann dazu führen, dass der Server verlangsamt wird. Die Debug- und Informationsebenen sollte daher nur beim Debuggen verwendet werden.

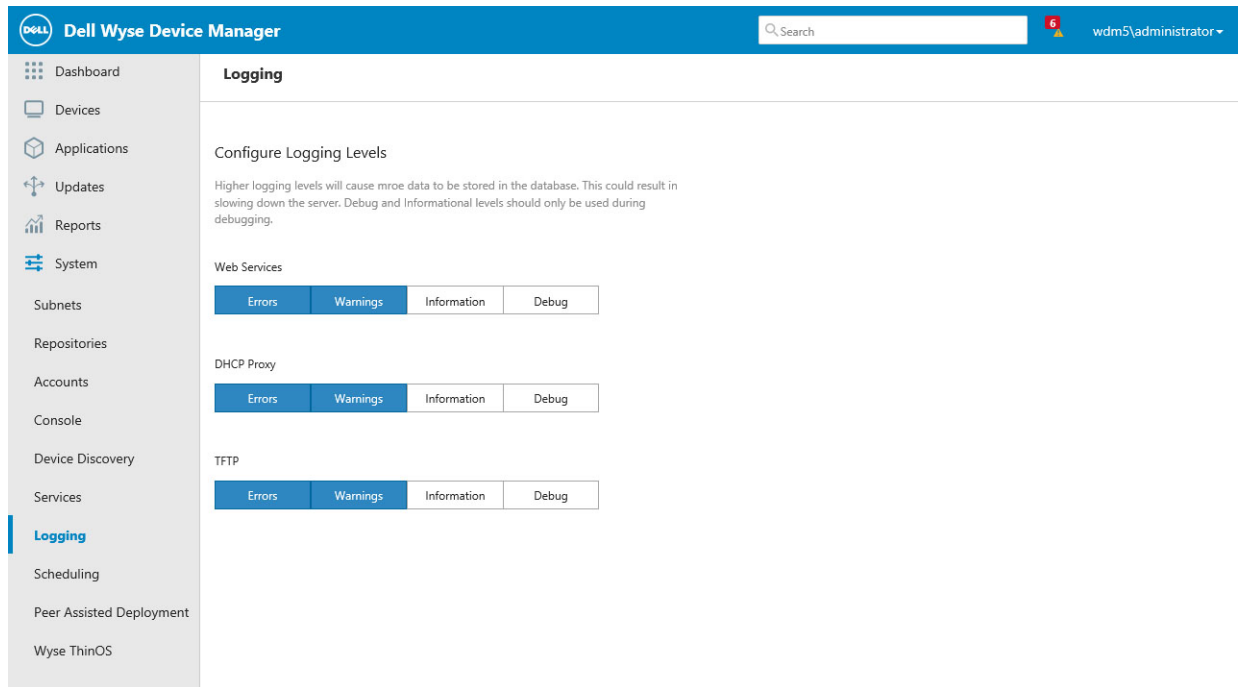


Abbildung 52. Protokollierung

- **Bereich der Protokollierungsdienste** – Wählen Sie die Protokollierungsebene für alle Kommunikationsprotokolle aus.
  - **Errors** (Fehler): Bestehen aus einfachen Fehlermeldungen.
  - **Warnings** (Warnungen): Bestehen aus Warnungen neben Fehlermeldungen (dies ist die Standardoption).
  - **Informational** (Informationen): Bestehen aus Fehler- und Warnmeldungen sowie anderen Informationselementen.
  - **Debug**: Bestehen aus sämtlichen Informationen von Fehler- und Warnmeldungen, Informationen und zusätzlichen Debugging-Daten, die für WDM-Entwickler, -Vertriebsmitarbeiter und -Administratoren nützlich sein könnten.
- **Web Services** (Webdienste): Beschreibt die Aktivität der WDM-Webdienste zur Geräteverwaltung.
- **DHCP Proxy** (DHCP-Proxy): Beschreibt die Aktivität des Dynamic Host Configuration Protocol von WDM bei der Erkennung des Geräts.
- **TFTP**: Beschreibt die Aktivität des Trivial File Transfer Protocol für die Verteilung von Softwarepaketen an Geräte.

## Planung

Auf der Seite „Scheduling“ (Planung) können Sie Details anzeigen, wie z. B. die maximale Anzahl gleichzeitiger Aktualisierungen, die Zeitzone von geplanten Aktualisierungen, die maximale Anzahl an Wiederholungsversuchen für die erneute Planung fehlgeschlagener Aktualisierungen und die automatische Synchronisierung von Remote-Software-Repositorys.

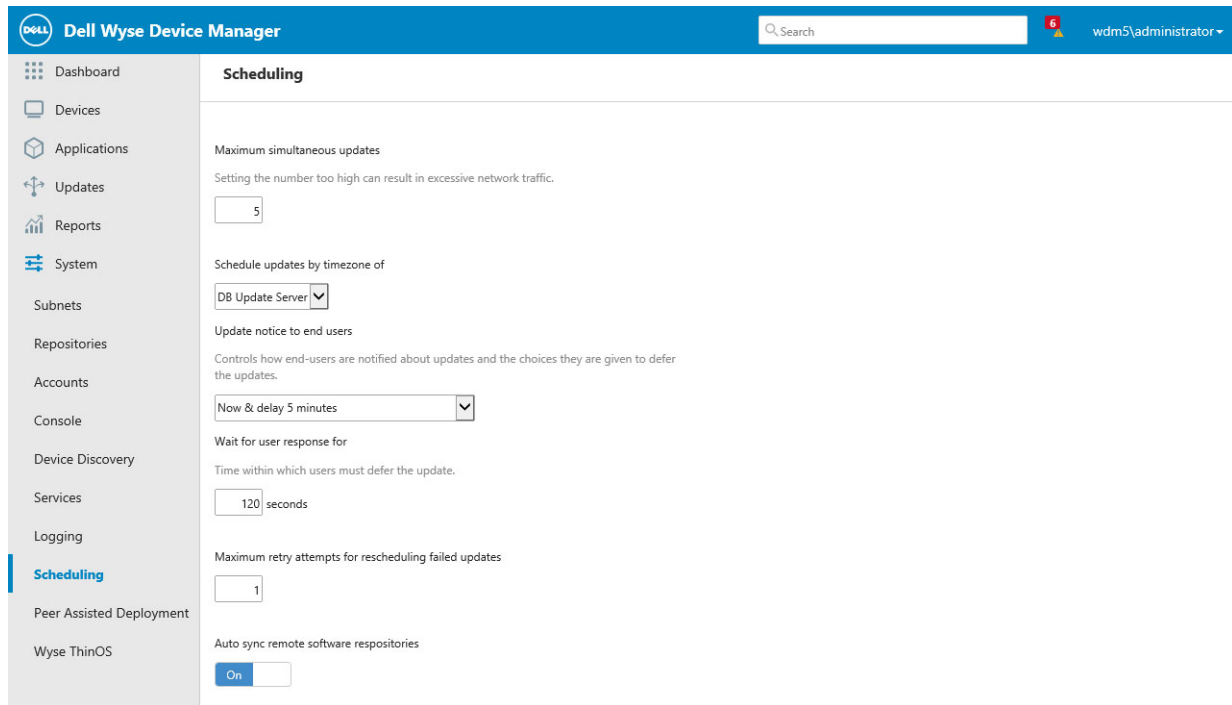


Abbildung 53. Planung

- **Maximum Simultaneous Updates** (Maximale Anzahl gleichzeitiger Aktualisierungen) – Die maximale Anzahl an Geräteaktualisierungen, die gleichzeitig im Subnetz ausgeführt werden können.
- **Scheduled updates by timezone of** (Geplante Aktualisierungen nach Zeitzone von) – Wählen Sie die WDM-Zeitzone, die für die Planung von Geräteaktualisierungen angewendet werden soll: Mögliche Optionen sind:
  - **DB Update Server** (DB-Aktualisierungsserver) – Die vom physischen Standort der WDM-Datenbank definierte Zeitzone.
  - **Console** (Konsole) – Die vom physischen Standort der WDM-Konsole definierte Zeitzone.
  - **Device** (Gerät) – Die von physischem Standort des Geräts, für das die tatsächliche Aktualisierung ausgeführt wird, definierte Zeitzone.
- **Update notice to end-users** (Aktualisierungsbenachrichtigung für den Endbenutzer) – Dies ist die Einstellung, um ein Fenster zum Abrufen einer Benutzerbenachrichtigung auf dem Client-Gerät anzuzeigen, wenn ein Aktualisierungspaket für den Client geplant ist.
- **Maximum retry attempts rescheduling failed updates** (Maximale Anzahl von Wiederholungsversuchen für die Neuplanung fehlgeschlagener Aktualisierungen) – Die maximale Anzahl von Wiederholungsversuchen gibt die Anzahl der Wiederholungsversuche an, die durchgeführt werden sollen, wenn die Paketbereitstellung fehlschlägt.
- **Auto-sync Remote Repositories** (Remote-Repositorys automatisch aktualisieren) – Wählen Sie diese Option, um WDM zu erlauben (nur Enterprise Edition), festzulegen, ob Remote-Repositorys synchronisiert werden sollen, bevor eine Aktualisierung für Geräte durchgeführt werden, die von einem Remote-Repository unterstützt werden.

## Peer-gestützte Verteilung

Peer-gestützte Verteilung (Peer Assisted Deployment, PAD) ist ein Mechanismus, mit dem Image-Erstellungsaktualisierungen für Thin Client-Geräte bereitgestellt werden, die über den WDM-Server verwaltet werden. Dieser Mechanismus funktioniert am besten in Umgebungen, in denen Geräte auf mehrere Subnetze verteilt sind. Bei Peer-gestützten Verteilungen wählt der WDM-Server einen Satz Geräte aus, die als Repository-Server für andere Geräte innerhalb der entsprechenden Subnetze fungieren sollen. Aus diesem Grund werden Updates über Peer-Knoten für andere Geräte bereitgestellt. Daher der Begriff Peer-gestützte Verteilung.

Die PAD-Funktion ist für die folgenden Plattformen anwendbar:

- SUSE Linux
- ThinLinux
- Windows Embedded Standard 7 (WES7)
- Windows Embedded Standard 7P (WES7P)

- Windows Embedded Standard 8 (WE8S)
- Windows 10 IoT Enterprise

Die folgenden Diagramme und Workflows beschreiben, wie PAD funktioniert.

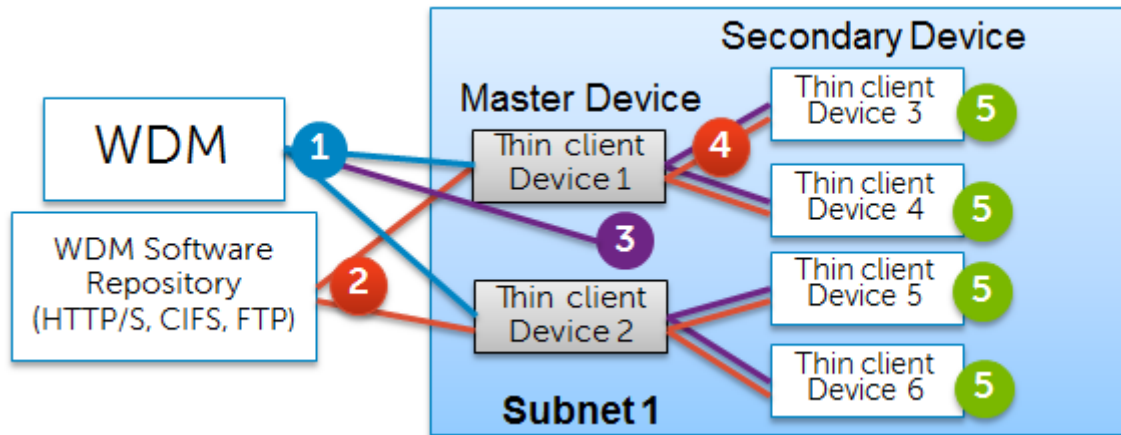


Abbildung 54. PAD-Funktionalität

#### Workflow vom WDM-Server zum Repository-Gerät

Das Image-Aktualisierungsverfahren für das für PAD konfigurierte Repository-Gerät besteht aus drei grundlegenden Schritten:

- Image-Erstellung durch das Gerät selbst.
- Herstellung der Repository-Fähigkeit des Geräts.
- Ausschalten des Repository, wenn der PAD-Zeitplan abgeschlossen ist.

Der Workflow kann in den folgenden Schritten definiert werden:

- 1 Das Gerät, das als erstes bei dem WDM-Server eincheckt, weist die niedrigste Flash-Größe auf und kann das ausgewählte PAD-Image aufnehmen, sodass es zum Repository-Gerät für dieses Subnetz wird. Für das Gerät sollten die Werte für **Peer Capable** (Peer-fähig) und **Repository Capable** (Repository-fähig) auf **True** (Wahr) festgelegt sein. Weitere Informationen finden Sie unter [Voraussetzungen für PAD](#).
- 2 Das Repository-Gerät startet neu und erstellt selbst ein Image vom WDM--Repository.
- 3 Das Repository-Gerät schließt die Image-Erstellung ab, startet neu, lädt das BIOS herunter und wird Repository-fähig. Das Gerät sendet anschließend den Status über die Fertigstellung des Pakets (V02) an den WDM-Server.
- 4 Nach Ablauf des Planbereichs sendet der WDM-Server eine Anweisung zum Ausschalten des Repository, wenn das Repository-Gerät eincheckt. Anschließend wird die Anwendung ausgeschaltet, die für die Aktivierung der Repository-Funktionen auf dem Gerät verantwortlich ist.

#### Workflow vom Repository-Gerät zu Peer-Geräten

Das Image-Aktualisierungsverfahren von Repository-Geräten zu Peer-Geräten mit PAD besteht aus den folgenden Schritten:

- 1 WDM plant die Imaging-Aufgabe für Peer-Geräte mit dem Repository-Gerätestandort und den Anmeldeinformationen zum Herunterladen des Image.
- 2 Die Peer-Geräte laden die Images vom Repository-Gerät.
- 3 Nach Abschluss des Imaging-Vorgangs starten die Peer-Geräte mit dem neuen Image.

Weitere Informationen zur PAD-Funktion finden Sie unter:

- [Voraussetzungen für PAD](#)
- [Konfigurieren von PAD](#)

- [Bereitstellen eines Pakets mit PAD](#)
- [Anzeigen von PAD-Details](#)
- [Bearbeiten und Löschen von PAD-Zeitplänen](#)

## Voraussetzungen für PAD

Die PAD-Funktion wird sowohl auf Windows- als auch auf Linux-Thin-Client-Systemen unterstützt. Damit Geräte zu einem Master-Gerät werden können, gibt es bestimmte Voraussetzungen.

Alle Linux-Geräte sind PAD-fähig und können als Master-Geräte fungieren.

Um die PAD-Fähigkeit von Linux-Geräten zu gewährleisten, laden Sie die neueste veröffentlichte Version des Betriebssystem-Images auf das Linux-Gerät herunter und installieren Sie sie. Das Image sollte ein PAD-fähiges Image sein. Sie können das Image von der Dell Wyse Support-Website herunterladen.

Weitere Informationen zur Konfiguration der Windows-Geräte für PAD finden Sie unter:

- [Herstellen der PAD-Fähigkeit für ein Windows-Gerät](#)
- [Herstellen der Repository-Fähigkeit für ein Windows-Gerät](#)
- [Erstellen von PAD-fähigen Images für Windows-Geräte](#)

## Herstellen der PAD-Fähigkeit für ein Windows-Gerät

So stellen Sie die PAD-Fähigkeit eines Windows-Geräts her:

- 1 Stellen Sie sicher, dass auf dem Gerät die aktuell veröffentlichte Windows-Version installiert ist.
- 2 Stellen Sie für WES7 sicher, dass es sich um Geräte der Z-, D-, ZQ-, DQ- oder 3290-C90D7-Klasse handelt und eine Flash-Laufwerk-Kapazität von mindestens 8 GB und 2 GB RAM vorhanden sind.
- 3 Stellen Sie für WES8 mit 64 Bit sicher, dass es sich um Geräte der Z-, D-, ZQ- oder DQ-Klasse handelt und eine Flash-Laufwerk-Kapazität von mindestens 16 GB und 4 GB RAM vorhanden sind.
- 4 Stellen Sie die aktuell verfügbare Version von **WES7WDAAgentUpgrade** auf WES7-Geräten, **WE8SWDAAgentUpgrade** auf WE8S-Geräten und **WIE10WDAAgentUpgrade** auf dem WIE10-Geräten bereit.
- 5 Stellen Sie die aktuell verfügbare Version von **BootAgentUpgradeWES7** auf WES7-Geräten und die aktuelle Version von **BootAgentUpgradeWE8S** und **BootAgentUpgradeWIE10** auf WE8S-Geräten bereit.

So bestätigen Sie, ob ein Gerät PAD-fähig ist oder nicht:

- 1 Wählen Sie auf der Seite „Device“ (Gerät) ein beliebiges Gerät.
- 2 Klicken Sie auf die Registerkarte **View details** (Details anzeigen), um die Details des ausgewählten Geräts anzuzeigen.
- 3 Schauen Sie sich auf der Seite „View details“ (Details anzeigen) den Abschnitt „Capabilities“ (Fähigkeiten) an.

Wenn das Gerät nicht PAD-fähig ist, ist das Kennzeichen **PAD Capable** (PAD-fähig) auf **Rot** gesetzt, wie unten dargestellt:

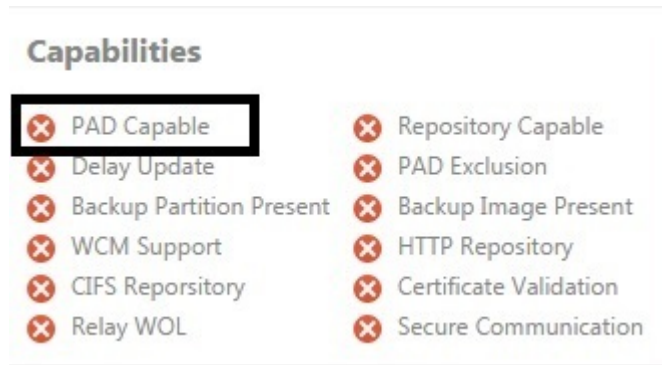


Abbildung 55. PAD-fähig

- 4 Nachdem die PAD-Fähigkeit des Geräts nach der Konfiguration hergestellt wurde, ist das Kennzeichen **PAD Capable** (PAD-fähig) auf **Grün** gesetzt, wie unten dargestellt:

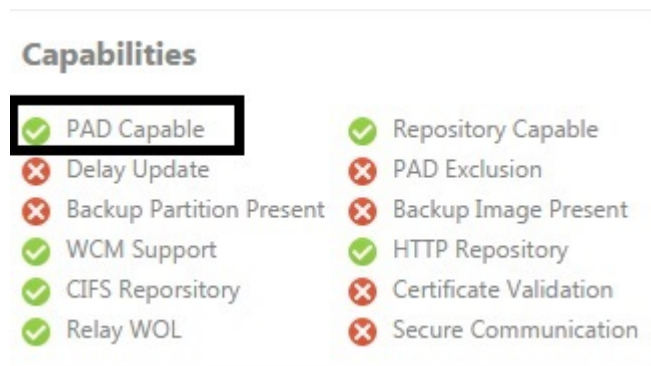


Abbildung 56. PAD-fähig

## Herstellen der Repository-Fähigkeit für ein Windows-Gerät

So stellen Sie die Repository-Fähigkeit eines Windows-Geräts her:

- 1 Stellen Sie **PADService\_SysprepScript\_WES7** auf dem WES7-Gerät bereit.
- 2 Stellen Sie **PADService\_SysprepScript\_WE8S** auf dem WES8-Gerät bereit.
- 3 Stellen Sie **PADService\_SysprepScript\_WE10S** auf dem WES10-Gerät bereit.

So bestätigen Sie, ob das Gerät Repository-fähig ist oder nicht:

- 1 Wählen Sie auf der Seite „Device“ (Gerät) ein beliebiges Gerät.
- 2 Klicken Sie auf die Registerkarte **View details** (Details anzeigen), um die Details des ausgewählten Geräts anzuzeigen.
- 3 Schauen Sie sich auf der Seite „View details“ (Details anzeigen) den Abschnitt „Capabilities“ (Fähigkeiten) an.

Wenn das Gerät nicht Repository-fähig ist, ist das Kennzeichen „Repository Capable“ (Repository-fähig) auf **Rot** gesetzt, wie unten dargestellt:



Abbildung 57. Repository-fähig

- 4 Nachdem die Repository-Fähigkeit des Geräts nach der Konfiguration hergestellt wurde, ist das Kennzeichen „Repository AD Capable“ (Repository-fähig) auf **Grün** gesetzt, wie unten dargestellt:

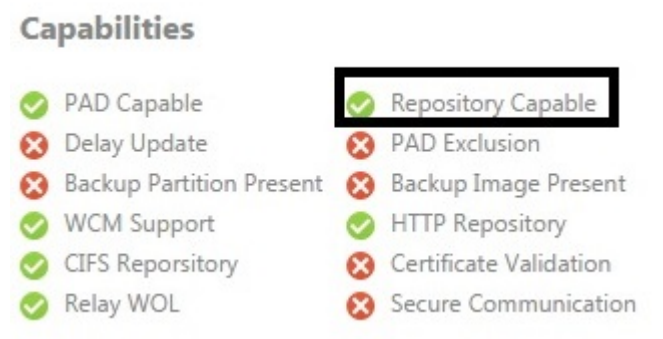


Abbildung 58. Repository-fähig

## Erstellen von PAD-fähigen Images für Windows-Geräte

So erstellen Sie ein PAD-fähiges Image für **WES7-**, **WE8S-** und **WIE10-**Geräte:

- 1 Stellen Sie das Anmeldeintervall in den WDM--GUI-Einstellungen auf mindestens eine Stunde ein.
- 2 Melden Sie sich am Gerät als Administrator an, deaktivieren Sie den Schreibfilter, melden Sie sich an und melden Sie sich erneut als Administrator an.
- 3 Löschen Sie die **HagentSettings.ini**- Datei unter C: \Program Files\Wyse\WDA\config und führen Sie den folgenden Befehl in der Eingabeaufforderung für **WES7**-Geräte aus:

```
Hagent.exe -Install
```

Für **WE8S** und **WIE10**-Geräte müssen Sie sich als Administrator angemeldet haben. Wechseln Sie zu C: \Windows\System32, klicken Sie mit der rechten Maustaste auf die Datei **Cmd.exe** und wählen dann die Option **Run as Administrator** (Als Administrator ausführen), bevor Sie den obigen Befehl ausführen.

- 4 Bereiten Sie das **WES7**-Gerät auf das Abrufen des Image vor, indem Sie in der Eingabeaufforderung zum Ordner **C: \windows\setup** navigieren und den folgenden Befehl ausführen:

```
WES7_CustomSysprep4man.bat -r
```

Bereiten Sie das **WES8-** und **WIE10**-Gerät auf das Abrufen des Image vor, indem Sie in der Eingabeaufforderung zum Ordner **C: \windows\setup** navigieren und die folgenden Befehle ausführen:

```
Powershell.exe c:\windows\setup\WIE10_CustomSysprep4man.ps1 -r
```

**ANMERKUNG:** Bei WE8S-Geräten müssen Sie die Eingabeaufforderung als Administrator ausführen. Siehe Schritt 3.

- 5 Das Gerät darf nicht ins Betriebssystem laden. Geben Sie stattdessen den Befehl **Pull Image** (Image abrufen) mit Modus **PXE** für **WES7**-Geräte und im Modus **Non PXE** (Nicht PXE) für die **WE8S**- und **WIE10**-Geräte, auf denen **sysprep** ausgeführt wird.
- 6 Melden Sie sich auf dem System an, auf dem die WDM--Konsole ausgeführt wird, und klicken Sie mit der rechten Maustaste auf einen Zeitplan über **Update Manager > Schedule Packages (Zeitplanpakete)**.
- 7 Wählen Sie die Option **Roll to Boot** (Zum Start ausrollen).
- 8 Bei **WES7**-Geräten drücken Sie die Taste **P** und starten Sie das Gerät über den Modus **PXE LAN**. Bei **WE8S**- und **WIE10**-Geräten drücken Sie die Taste **P** und starten Sie das Gerät über den Modus **Merlin Non-PXE**.
- 9 Nach dem Abruf des Image wird es mithilfe der Option **Deploy via Peers in Subnet** (Über Peers im Subnetz bereitstellen) bereitgestellt.

## Konfigurieren von PAD

Um die PAD-Funktion zu verwenden, müssen Sie die Subnetzeinstellungen konfigurieren. Sie können die Anzahl der Geräte, die als Repositories fungieren sollen sowie die Informationen für die Verbindung zum Master-Gerät angeben.

**Abbildung 59. Peer-gestützte Verteilung**

So konfigurieren Sie PAD auf WDM:

- 1 Wählen Sie aus der WDM-Konsole, **System → Peer Assisted Deployment** (Peer-gestützte Verteilung).
- 2 Geben Sie die an, ob mindestens ein oder zwei Peer-fähige Repositories erforderlich sind.
- 3 Ändern Sie bei Bedarf die maximale Anzahl gleichzeitiger Verbindungen zum Master-Gerät. Die standardmäßige Anzahl gleichzeitiger Verbindungen beträgt 7.
- 4 Ändern Sie bei Bedarf die maximale Anzahl der Wiederholungsversuche für das Master-Gerät. Die standardmäßige Anzahl gleichzeitiger Verbindungen beträgt 3.
- 5 Geben Sie die Anmeldeinformationen für den Zugriff auf Repositories ein. Geben Sie den Benutzernamen, das Kennwort und den relativen Pfad für das folgende Gerät an.
  - **SUSE Linux (SCP)**
  - **ThinLinux**
  - **Windows Embedded Standard 7**
  - **Windows Embedded Standard 7P**

- **Windows Embedded Standard 8**
- **Windows 10 IoT Enterprise**

## Bereitstellen eines Pakets mit PAD

So stellen Sie ein Image mit PAD bereit:

- 1 Wählen Sie auf der WDM--Konsole **Images** unter **Application** (Anwendung).  
Die registrierten Images werden angezeigt.

**ANMERKUNG:** PAD kann nur Images bereitstellen, keine Anwendungspakete.

- 2 Wählen Sie ein Image und wählen Sie die Registerkarte **Deploy via peers** (Verteilung über Peers).  
Das Fenster **Deploy via peers** (Verteilung über Peers) wird angezeigt.

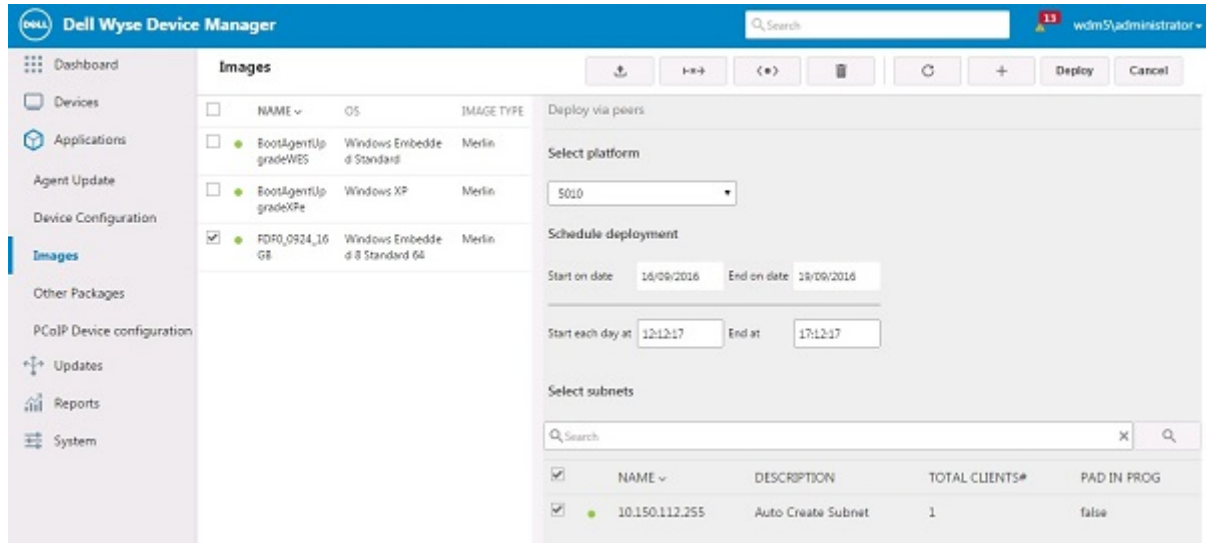


Abbildung 60. Verteilung über Peers

- 3 Wählen Sie aus der Dropdown-Liste Ihre bevorzugte Plattform.
- 4 Geben Sie das Startdatum, Enddatum und die Zeit im Format hh:mm:ss ein, um eine Bereitstellung zu planen.
- 5 Geben Sie die Subnetz-IP-Adresse ein, um ein verfügbares Subnetz auszuwählen.

**ANMERKUNG:** Zum Erstellen eines PAD-Zeitplans muss mindestens ein Subnetz ausgewählt werden.

- 6 Klicken Sie auf **Deploy** (Bereitstellen).

## Anzeigen von PAD-Details

Sie können PAD-Details (Peer Assisted Delivery), wie z. B. PAD-Zeitpläne, die als Master-Repositorys ausgewählten Clients und die Zusammenfassung des Image-Aktualisierungsvorgangs, anzeigen.

So können Sie die Details anzeigen:

- 1 Erweitern Sie in der WDM-Konsole den Knoten **Peer Assisted Delivery** (Peer-gestützte Verteilung) unter **Updates** (Aktualisierungen).  
Der Knoten zeigt die **Aufgaben**, **Repositories** (Repositorys) und **Summary** (Zusammenfassung) an.
- 2 Um die Liste der Clients, die als Master-Repositorys dienen, anzuzeigen, wählen Sie **Repositories** (Repositorys) unter **Peer Assisted Delivery** (Peer-gestützte Verteilung) aus.  
Die Liste der Clients wird angezeigt.

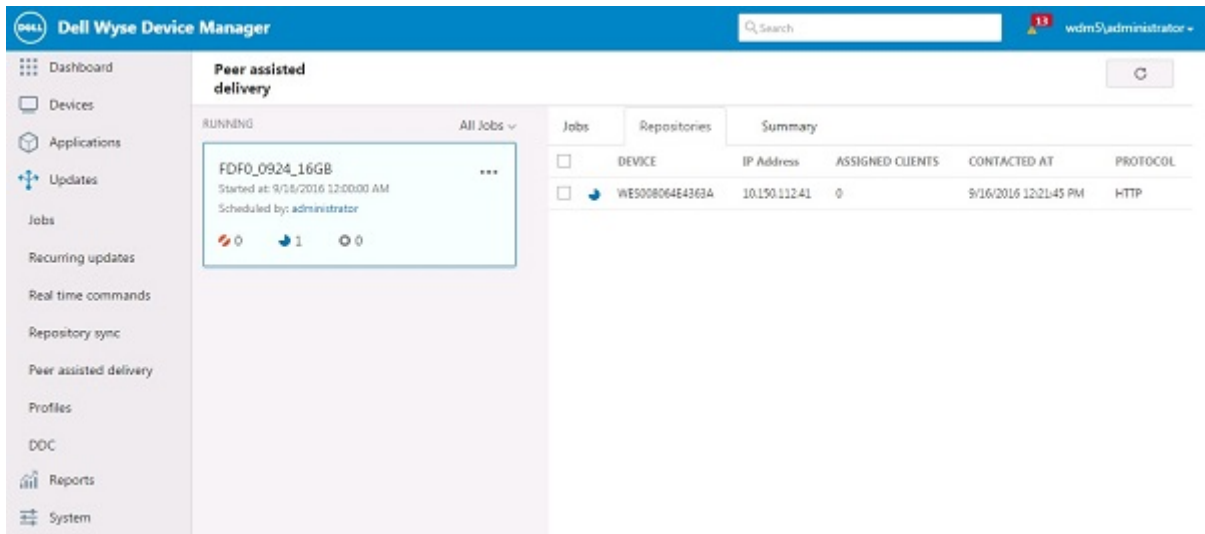


Abbildung 61. Repositories

- Um PAD-Zeitpläne anzuzeigen, wählen Sie **Aufgaben** unter **Peer Assisted Delivery** (Peer-gestützte Verteilung). Die Liste der Paketbereitstellungszeitpläne wird angezeigt.

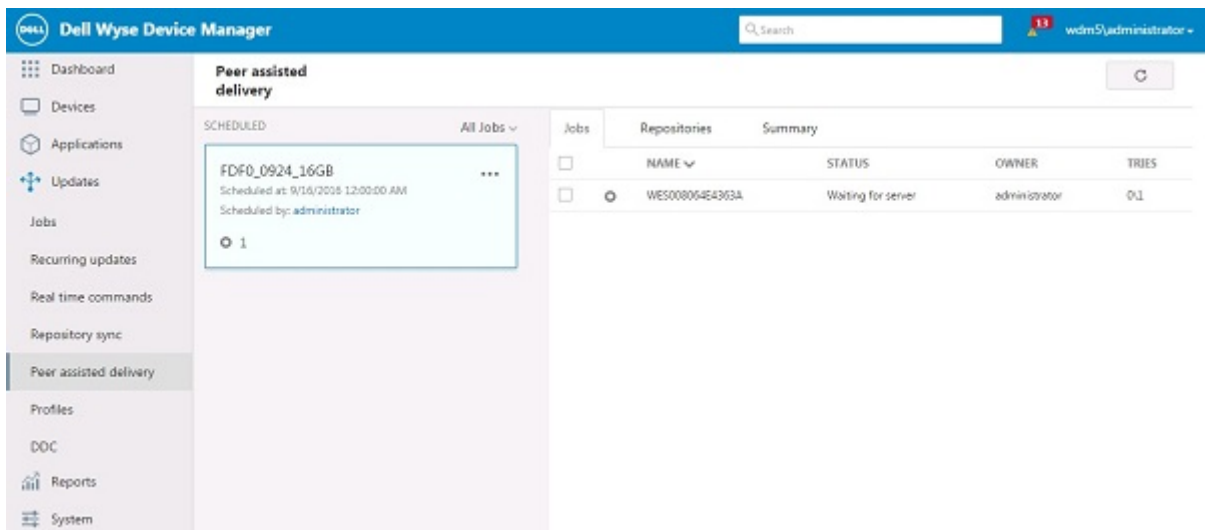


Abbildung 62. Aufgaben

- Um den PAD-Image-Aktualisierungsvorgang anzuzeigen, wählen Sie **Summary** (Zusammenfassung) unter **Peer Assisted Delivery** (Peer-gestützte Verteilung) aus. Der Fortschritt wird angezeigt.

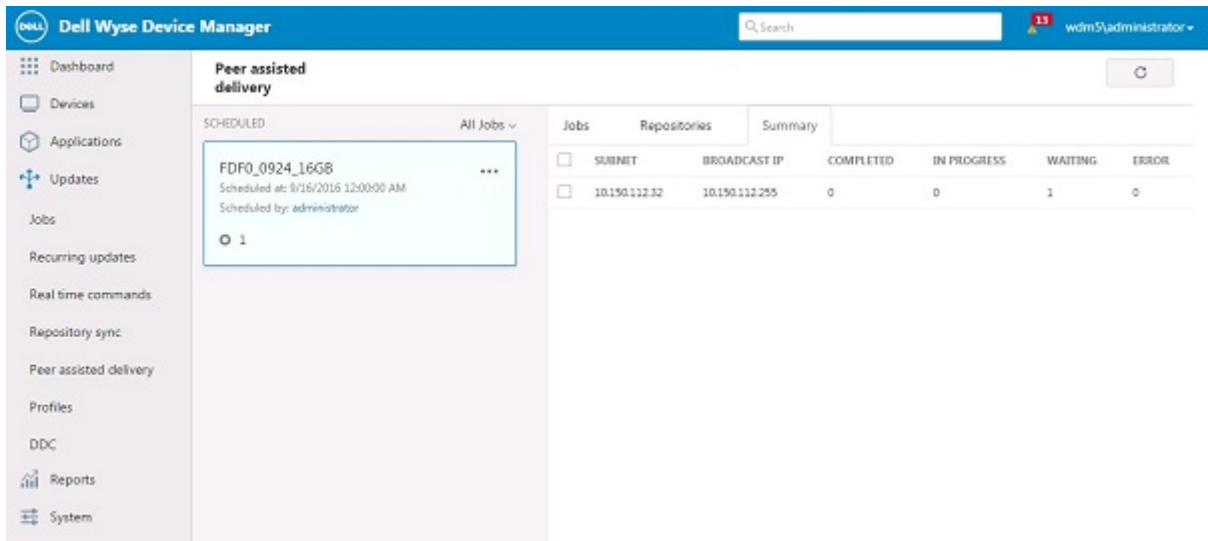


Abbildung 63. Zusammenfassung

## Bearbeiten und Löschen von PAD-Zeitplänen

Sie können PAD-Zeitpläne auf der WDM--Konsole bearbeiten und löschen.

- 1 So bearbeiten Sie einen PAD-Zeitplan:
  - a Erweitern Sie auf der WDM--Konsole die Option **Peer Assisted Delivery** (Peer-gestützte Verteilung) unter **Updates** (Aktualisierungen) und wählen Sie **Aufgaben**.  
Die Aufgaben werden angezeigt.
  - b Wählen Sie eine Aufgabe, klicken Sie auf die drei angezeigten Punkten und wählen Sie **Edit** (Bearbeiten).  
Das Fenster **Edit** (Bearbeiten) wird angezeigt.

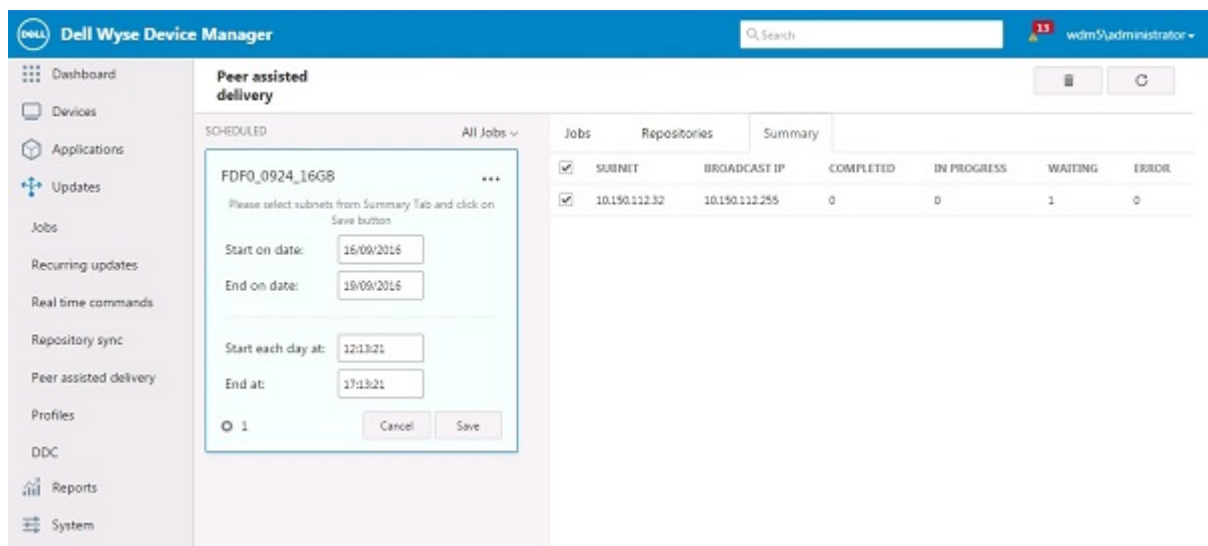


Abbildung 64. PAD-Bearbeitung

- c Ändern Sie Datum und Uhrzeit je nach Bedarf und klicken Sie auf **Save** (Speichern).  
Die geplante Aufgabe wird mit neuem Datum und neuer Uhrzeit angezeigt.
- 2 So löschen Sie einen PAD-Zeitplan:

- a Erweitern Sie auf der WDM--Konsole die Option **Peer Assisted Delivery** (Peer-gestützte Verteilung) unter **Updates** (Aktualisierungen) und wählen Sie **Summary** (Zusammenfassung).  
Die Zeitplanzusammenfassungen werden angezeigt.
- b Wählen Sie eine Zusammenfassung und klicken Sie auf die Registerkarte **Delete** (Löschen).  
Der Zeitplan wird gelöscht.

## Wyse ThinOS

Mit diesem Parameter können Sie den WTOS.INI-Stammpfad anzeigen.

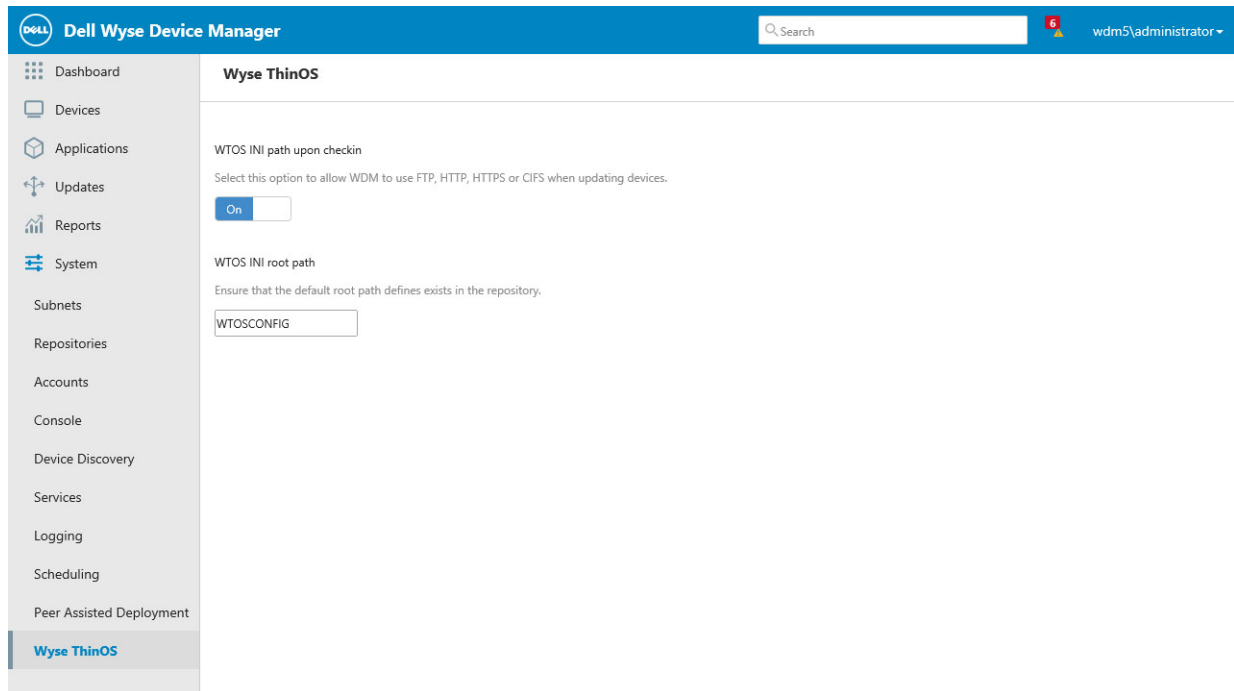


Abbildung 65. Wyse ThinOS

- **WTOS INI path upon checkin** (WTOS.INI-Pfad beim Einchecken): Wählen Sie diese Option aus, damit WDM zum Aktualisieren von Geräten FTP, HTTP, HTTPS oder CIFS verwendet.
- **WTOS INI Root Path** (WTOS.INI-Stammpfad): Geben Sie den WTOS.INI-Stammpfad ein.

# Verwaltung von Teradici-Geräten mit WDM

Voraussetzung: Sie müssen zunächst einen WDM-Server mit ThreadX-Unterstützung für die 5.x-Firmware installieren.

Dieser Abschnitt enthält Informationen über die für die Geräte-Ermittlung erforderlichen Infrastrukturänderungen sowie die Registrierung mit Verwaltungsservern einschließlich Wyse Device Manager (WDM).

## Unterstützte Plattformen:

Unterstützt die folgenden Teradici-basierten Dell Wyse-Geräte:

- Wyse 5030 Zero Client für VMware
- Wyse 5050 AIO Thin Client mit PCoIP
- Wyse 7030 Zero Client für VMware

## Firmware-Versionen:

- 4.x
- 5.x

**ANMERKUNG:** Die folgenden Anweisungen beziehen sich auf Windows 2012 R2 DNS. Die genauen Einstellungen können je nach Windows-Version variieren.

Themen:

- [Schritte zum Erstellen einer DNS\\_SRV-Datensatzes](#)
- [Überwachung und Fehlerbehebung](#)
- [Konfigurieren der Firmware 5.x](#)
- [Aktualisieren der ThreadX 4.X-Geräte auf ThreadX 5.X über WDM](#)

## Schritte zum Erstellen einer DNS\_SRV-Datensatzes

Die Firmware 4.x verwendet entweder den DNS\_SRV-Datensatz oder DHCP-Datensatz für die Suche nach der Verwaltungskonsole.

**ANMERKUNG:** DNS\_SRV- und DHCP-Datensätze dürfen nicht gleichzeitig für die Suche nach der Firmware 4.x-Verwaltungskonsole verwendet werden.

Die Anweisungen in diesem Abschnitt gelten in erster Linie für DNS\_SRV-Datensatz. Der DNS-Datensatz ist `_tcp_pcoip-tool` in der Domäne, mit dem der Client kommuniziert, und die Konfigurationen müssen auf dem DNS-Server vorgenommen werden.

Im folgenden Beispiel lautet der Domänenname `delldemo.int` und WDM-Server ist `dell-wdm55.delldemo.int`.

- 1 Navigieren Sie zu `_tcp` unter Ihrer Domäne, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Other new records (Weitere neue Datensätze)**.



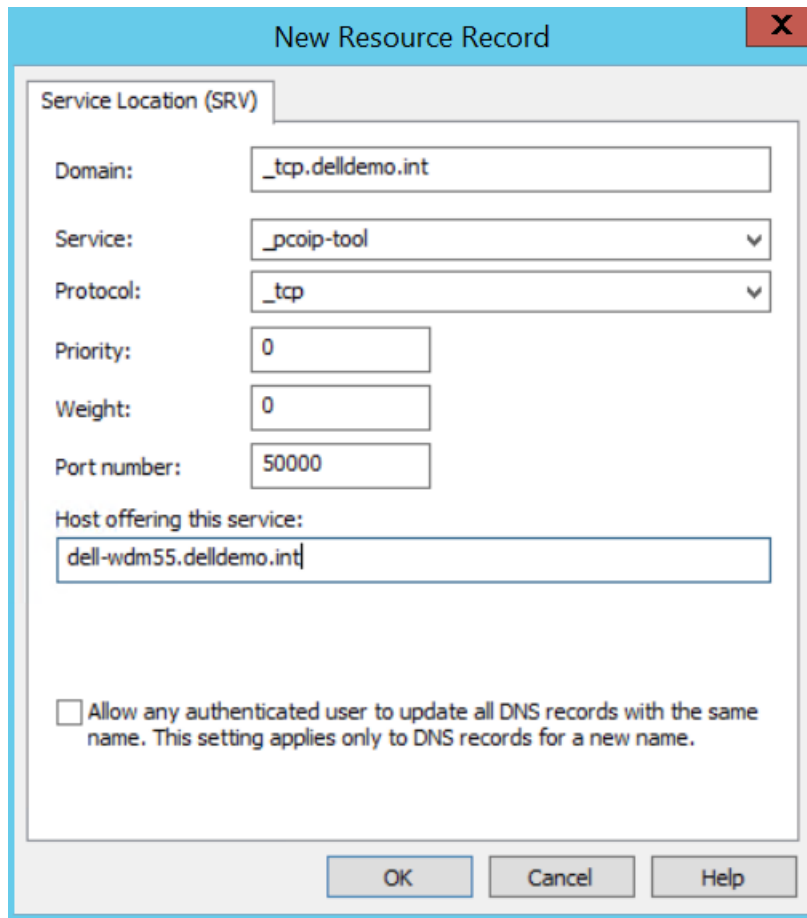


Abbildung 68. Neuer Ressourcendatensatz

Tabelle 21. Neuer Ressourcendatensatz

Parameter	Beschreibung
Domäne	delldemo.int
Dienstleistung	_pcoip-tool
Protokoll	_tcp
Priorität	0 (Null)
Gewicht	0 (Null)
Schnittstellennummer	50000
Host offering this service (Host, der diesen Dienst bietet)	Geben Sie den Namen oder die IP-Adresse des WDM-Servers ein.

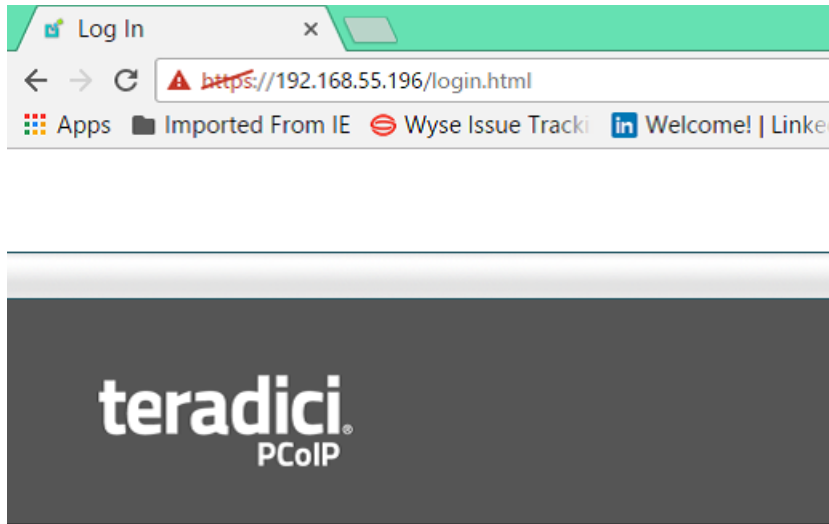
5 Klicken Sie auf OK.

**ANMERKUNG:** Ein . wird automatisch der Hostzeile von Windows nachgestellt.

## Überwachung und Fehlerbehebung

Die einfachste Möglichkeit zur Überwachung des Geräts stellt die Verwendung der Web-UI des Geräts und der Ereignisprotokolle dar.

- 1 Verbinden Sie den Browser mit der https://IP-Adresse des Geräts.
- 2 Geben Sie das standardmäßige Kennwort des Geräts ein. Das Standardkennwort lautet **Administrator**.



### Log In

Your session has ended. Please enter the administrative password to access this device

Password:

Idle Timeout:

Abbildung 69. Anmelden

- 3 Wählen Sie die Option **Diagnostics** (Diagnose) aus.

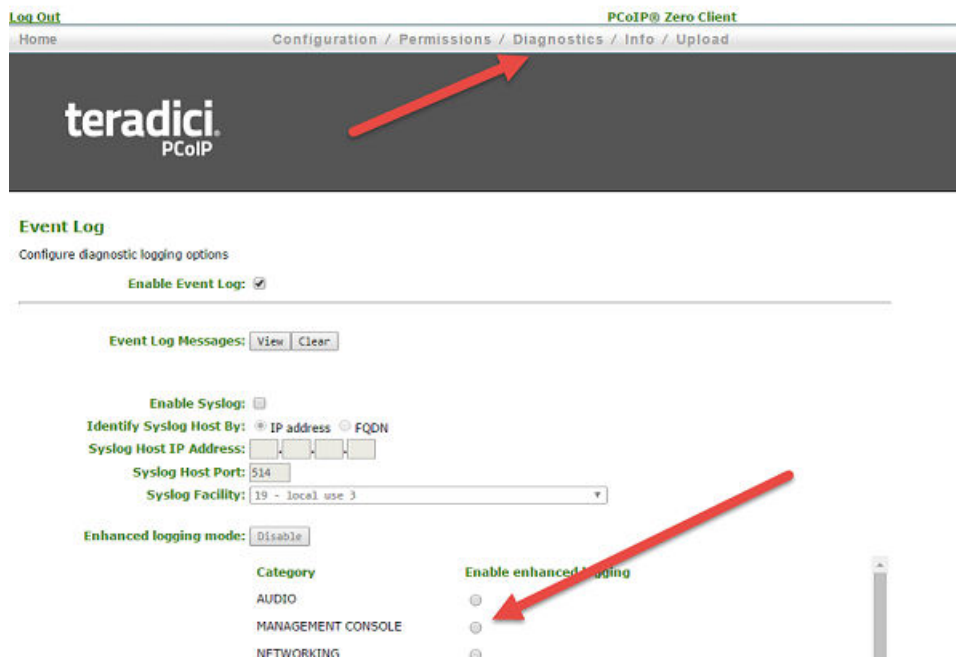


Abbildung 70. Diagnose

- 4 Aktivieren Sie die Option „Enable Event Log“ (Ereignisprotokoll aktivieren), um die Diagnoseprotokollierungsoptionen zu konfigurieren.

- Wählen Sie die Optionsschaltfläche der Option **Management Console** (Verwaltungskonsole) aus.
- Klicken Sie auf die Option **View** (Anzeigen), um die Meldungen im Ereignisprotokoll anzuzeigen.

## Event Log

Configure diagnostic logging options

Enable Event Log:

Event Log Messages:

Abbildung 71. Ereignisprotokoll

- Suchen Sie nach DNS-SRV-Informationen im Protokoll, insbesondere für MGMT\_DISC\_DNS. Suchen Sie in diesem Beispiel nach ordnungsgemäß ermitteltem WDM-Server mit dem Namen dell-wdm55.delldemo.int und der IP-Adresse 192.168.251.65.

```

:00:24.66> LVL:2 RC: 0 MGMT_DISC_DNS :DNS based discovery prefix:
:00:24.66> LVL:2 RC: 0 MGMT_DISC_DNS :(DNS SRV) Discovery (domain): delldemo.int
:00:24.66> LVL:2 RC: 0 MGMT_DISC_DNS :(DNS SRV) Discovery (hostname):
:00:24.79> LVL:1 RC: -510 MGMT_DISC_DNS :conduct_dns_record_search: (DNS SRV: CMS) DNS record not found
:00:25.08> LVL:1 RC: -510 MGMT_DISC_DNS :conduct_dns_record_search: (DNS SRV: VCS) DNS record not found
:00:25.13> LVL:3 RC: 0 MGMT_SYS :(cmi_cms_boot_notify_cback): transmit_success: 1
:00:25.13> LVL:3 RC: 0 MGMT_SYS :(cmi_cms_boot_notify_cback): queuing EVENT_CMI_BOOT_NOTIFY_SUCCESS
:00:25.13> LVL:3 RC: 0 MGMT_SYS :INIT.CMS_NOTIFY_BOOT: transition 84 into CONNECT_PROMPT
:00:25.13> LVL:2 RC: 0 MGMT_UI :tera_mgmt_ui_set_session_state: STANDALONE
:00:25.13> LVL:2 RC: 0 MGMT_UI :tera_mgmt_ui_osd_display_main_dialog: CONNECT
:00:25.13> LVL:2 RC: 0 MGMT_SYS :Ready to connect with host
:00:25.13> LVL:3 RC: 0 MGMT_SYS :CONNECT_PROMPT.INIT: transition 150 into CONNECT_PROMPT.PENDING_UI_OR_CMS_PROMPT
:00:25.13> LVL:2 RC: 0 MGMT_UI :DISCONNECTED: transition 21 into DISCONNECTED (MSG_SESSION_STATE_CHANGED: STANDALONE)
:00:25.44> LVL:2 RC: 0 MGMT_DISC_DNS :(DNS SRV: Config Tool) Discovery complete: 192.168.251.65
:00:46.81> LVL:1 RC: 0 MGMT_UI :SUCCESSFUL web login from 192.168.55.253.
:02:49.66> LVL:3 RC: 0 MGMT_CHI :(env_cback): event: 0x0

```

Abbildung 72. Protokolle

- Überprüfen Sie, ob das Gerät in der Verwaltungskonsole (WDM) aufgeführt wird.

NAME	IP ADDRESS	PLATFORM	OPERATING SYSTEM	MAC ADDRESS	LAST CHECK IN
pcoip-portal-0080648f67a6	10.150.122.44	PMS	ThreadX	00-80-64-8f-67-a6	11/15/2016 10:24:55 AM

Abbildung 73. Dell Wyse-Geräte-Manager

**ANMERKUNG:** Die Firmware 4.x Teradici verfügt über eine bekannte Einschränkung in der Kommunikation von Geräten, die mit WDM registriert werden. Es dauert ggf. 15 bis 30 Minuten, bis das Gerät in der Konsole angezeigt wird, selbst wenn das Gerät im Protokoll als registriert aufgeführt ist.

## Konfigurieren der Firmware 5.x

Firmware 5.x verwendet einen DNS\_SRV-Datensatz zusätzlich zum Textdatensatz, der den Fingerabdruck des SSL-Zertifikats für die Verwendung in der Verwaltungskonsole enthält.

WDM 5.7.3 unterstützt Teradici 5.x-Firmware mit umfassenden Funktionen.

Anweisungen für das weitere Vorgehen nach der Erstellung des DNS\_SRV-Datensatzes finden Sie unter [Schritte zum Erstellen einer DNS\\_SRV-Datensatzes](#). Führen Sie anschließend die folgenden Schritte durch:

- Der erste erforderliche Datensatz ist der DNS\_SRV-Datensatz für \_pcoip-bootstrap. Der Datensatz muss auf den Namen der Verwaltungskonsole (WDM) verweisen.

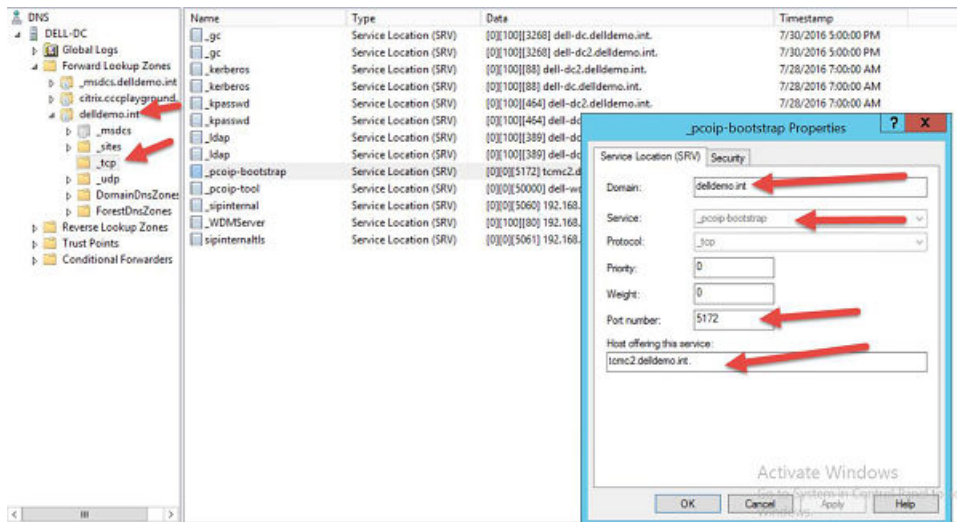


Abbildung 74. DNS\_SRV-Datensatz für \_pcoip-bootstrap

- 2 Der zweite erforderliche Datensatz ist ein A-Datensatz, der auf den im Feld **Host offering this service** (Host, der diesen Dienst bietet) verwendeten Namen verweist.

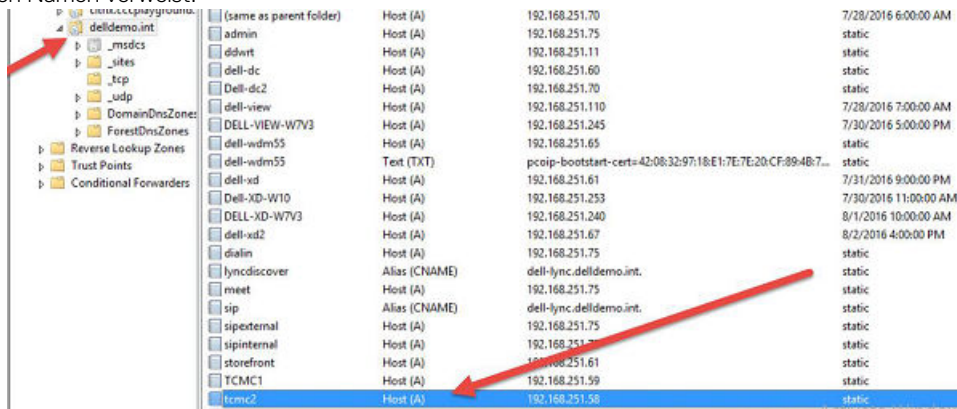


Abbildung 75. Host-Datensatz

- 3 Der dritte erforderliche Datensatz ist ein Txt-Datensatz. Der Txt-Datensatz ist der Fingerabdruck des SSL-Zertifikats, das von der Verwaltungskonsole verwendet wird.

Führen Sie die folgenden Schritte aus, um einen A-Datensatz für den Host sowie einen Txt-Datensatz zu erstellen:

- 1 Klicken Sie auf den Domain-Knoten (delldemo.int), wählen Sie **Other New Records** (Weitere neue Datensätze) und anschließend „Host“ (A oder AAAA) aus. Der Name ist der A-Datensatz der Verwaltungskonsole.



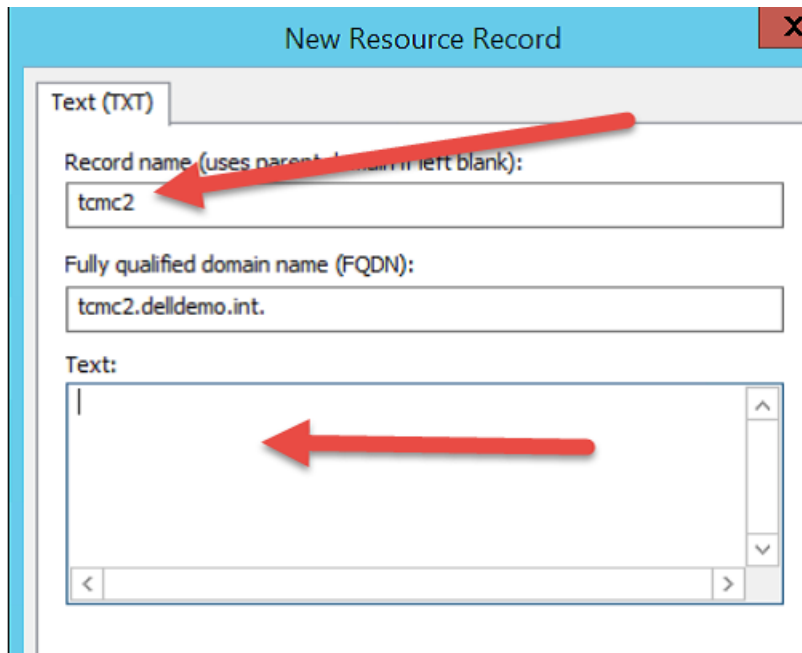


Abbildung 77. Neuer Ressourcendatensatz

Der Fingerabdruck Sha256 kann mit dem Firefox-Browser abgerufen werden.

Gehen Sie zum Abrufen des Fingerabdrucks folgendermaßen vor, wenn Wyse Device Manager (WDM) mit Teradici 5x installiert ist:

- 1 Öffnen Sie den Firefox-Browser von dem Gerät, auf dem die Teradici 5.x-Komponente installiert ist. Nach dem Öffnen des Browsers drücken Sie **Alt + T** zum Öffnen der Extras.
- 2 Wählen Sie in der Dropdown-Liste **Options** (Optionen) aus.

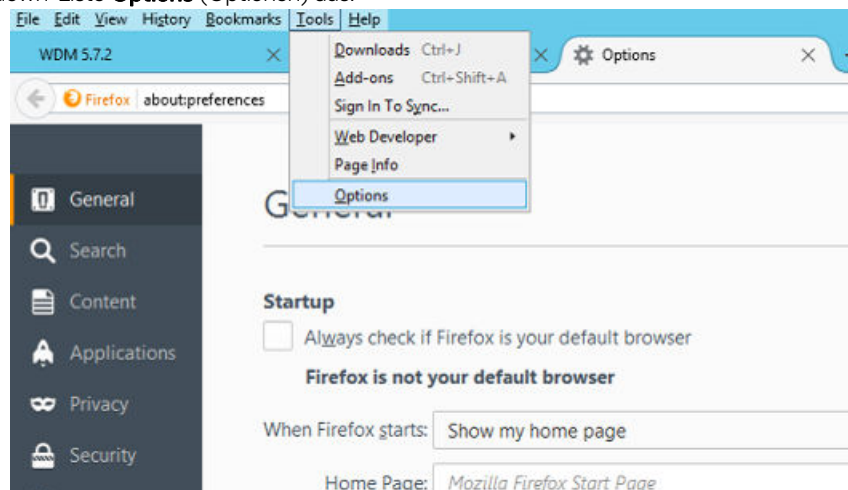


Abbildung 78. Registerkarte „General“ (Allgemein)

- 3 Klicken Sie im linken Fensterbereich der Seite **Options** (Optionen) auf die Registerkarte **Advanced** (Erweitert) und klicken Sie dann auf die Option **Certificates** (Zertifikate).

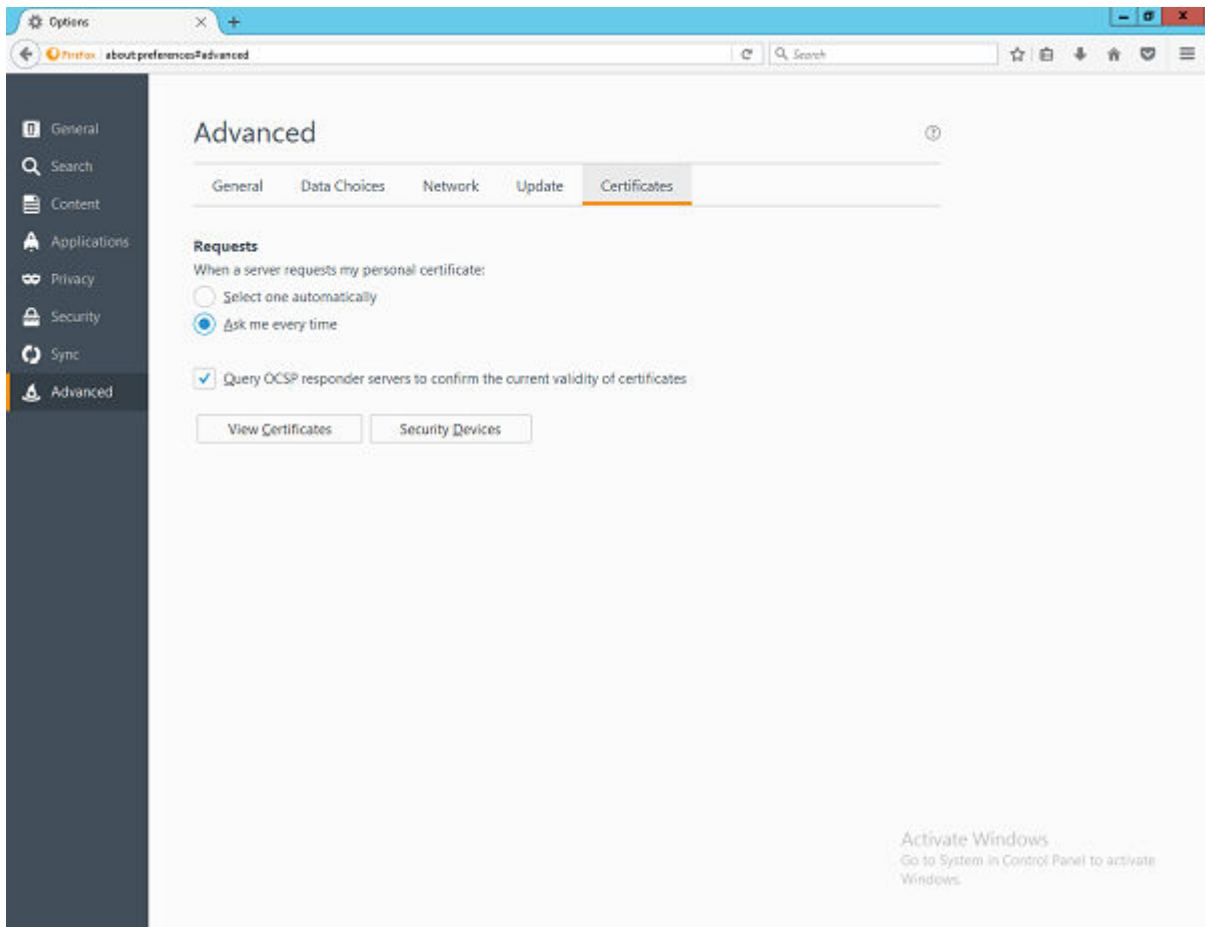


Abbildung 79. Advanced (Erweitert)

- 4 Klicken Sie zum Öffnen des Fensters „Certificate Manager“ (Zertifikat-Manager) auf **View Certificates** (Zertifikate anzeigen).
- 5 Wählen Sie die Registerkarte **Authorities** (Zertifizierungsstellen) im Fenster **Certificate Manager** (Zertifikat-Manager) aus und klicken Sie auf **Import** (Importieren).

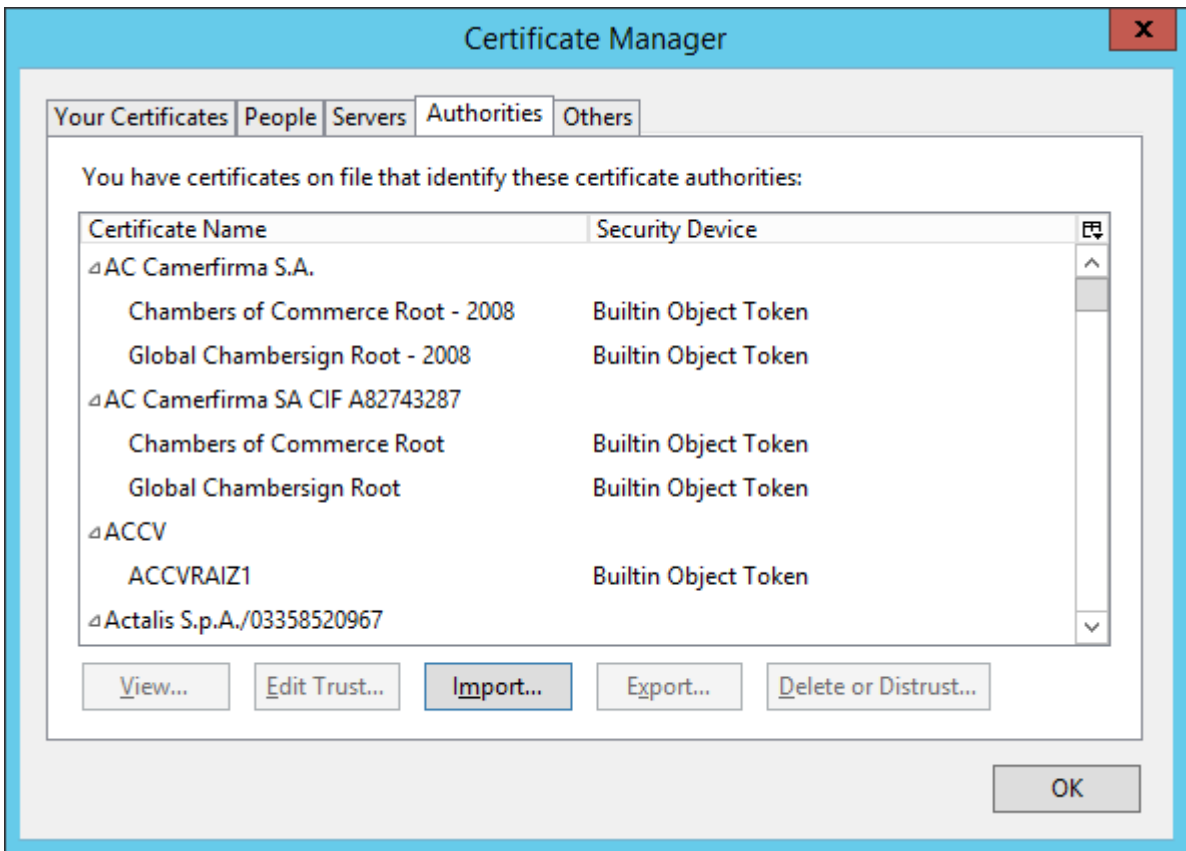


Abbildung 80. Certificate Manager (Zertifikat-Manager)

- 6 Navigieren Sie im Datei-Browser-Dialogfeld zum Speicherort der WDM-Installation, zum Beispiel: `\\Wyse\WDM\TeraDici`. Je nach Betriebssystem und Installationspfad kann der Root-Pfad folgendermaßen lauten `C:\Program Files (x86)`.
- ① **ANMERKUNG:** In manchen Fällen (wenn die Teradici-Komponenten benutzerdefiniert installiert oder manuell konfiguriert sind) müssen auf demselben Gerät die obigen Schritte beachtet werden und der standardmäßige Installationspfad trifft unter Umständen nicht zu. In einem solchen Fall navigieren Sie zum entsprechenden Root-Pfad, unter dem der Teradici-Ordner verfügbar ist.
- 7 Wählen Sie die Datei mit dem Namen **cert.pem** aus und klicken Sie dann auf **Open** (Öffnen).
- 8 Klicken Sie im Fenster **Downloading Certificate** (Zertifikat herunterladen) auf die Schaltfläche **View** (Anzeigen).

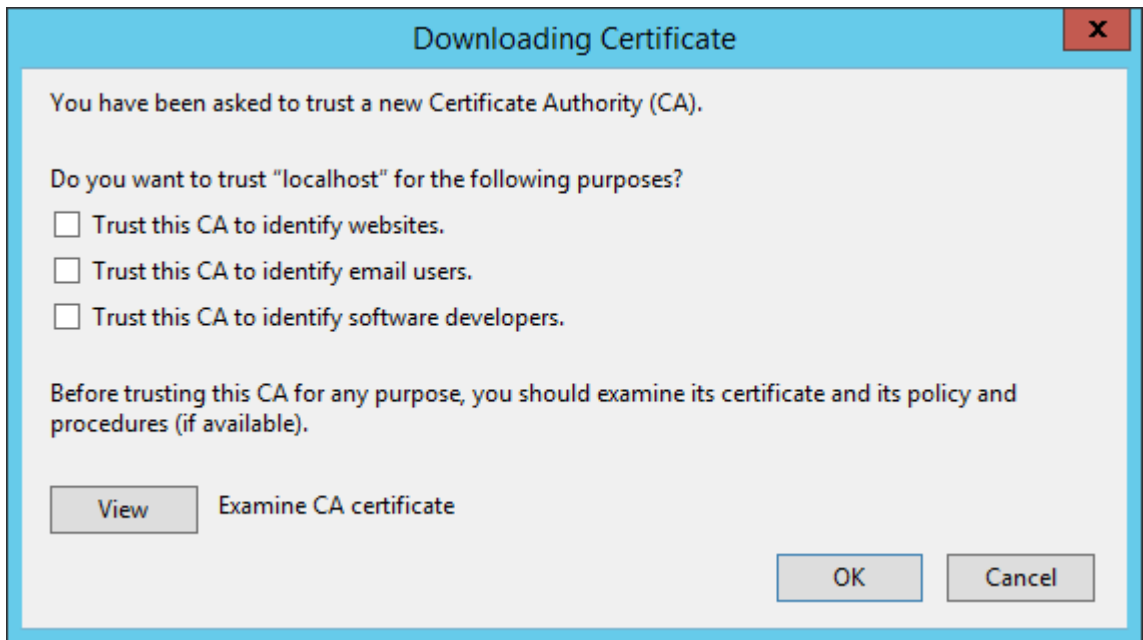


Abbildung 81. Downloading Certificate (Zertifikat herunterladen)

- 9 Kopieren Sie den Wert des Fingerabdrucks „sha256“ Klicken Sie auf **Close** (Schließen) und schließen Sie alle Firefox-Fenster.

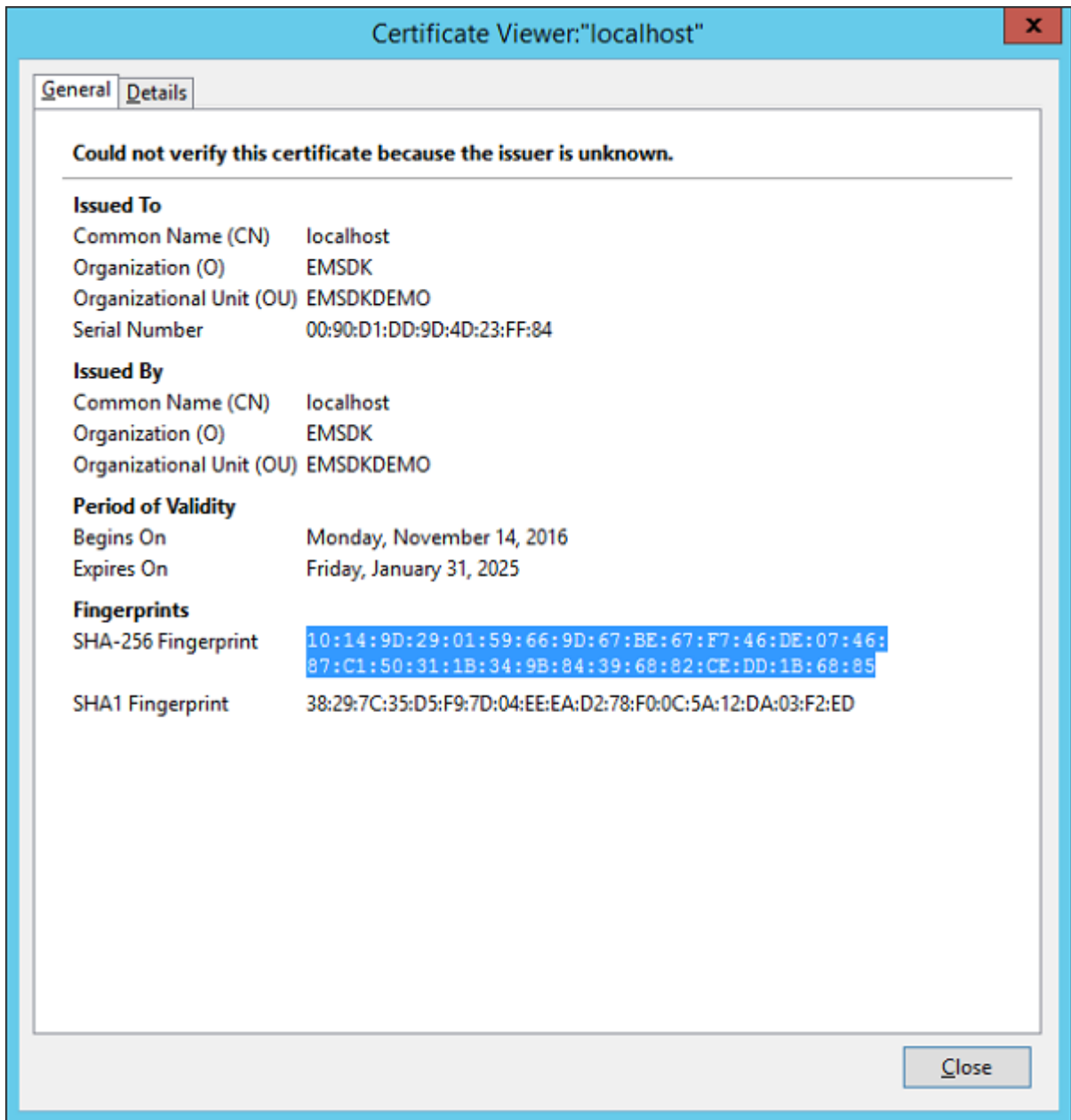


Abbildung 82. Certificate Viewer (Zertifikat-Viewer)

① **ANMERKUNG:** Im Feld Text muss vor den bereits abgerufenen Fingerabdruck sha256 das Präfix `pcyip-bootstrap-cert=` gesetzt werden.

Nach dem Kopieren des Zertifikatfingerabdrucks führen Sie die folgenden Schritte auf dem DNS-Server durch:

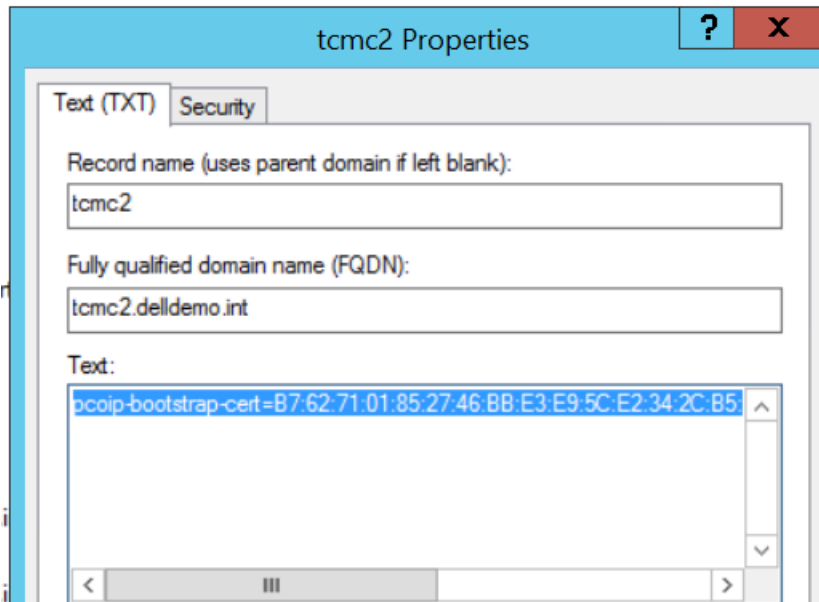


Abbildung 83. tcmc2-Eigenschaften

- 10 Der vierte und letzte Datensatz ist ein umgekehrter PTR-Datensatz für den Verwaltungs-Host.

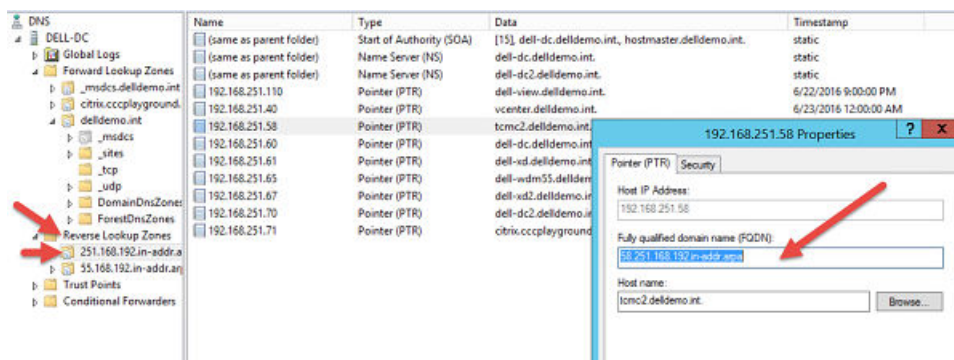


Abbildung 84. PTR-Datensatz

- 11 Die Zone muss mit dem Subnetz übereinstimmen, in dem sich der Host befindet, und der Datensatz ist die IP-Adresse, die der Verwaltungskonsole zugewiesen ist.
- 12 Nach Abschluss der DNS\_SRV-Konfiguration befolgen Sie die Anweisungen zum Upgrade der Firmware unter [Aktualisieren der Teradici-Firmware von 4.x auf 5.x mithilfe von WDM](#).

## Aktualisieren der ThreadX 4.X-Geräte auf ThreadX 5.X über WDM

In diesem Abschnitt werden die Schritte definiert, die beim Upgrade vorhandener ThreadX 4.x-Geräte auf ThreadX 5.x-Geräte von WDM befolgt werden müssen. Dadurch können Sie nach dem Upgrade ThreadX 5.x-Geräte in WDM weiterhin verwalten, und zwar mit der neuen ThreadX-Verwaltungslösung.

Für die Aktualisierung von ThreadX 4.x-Geräten auf ThreadX 5.x über WDM gelten folgende Voraussetzungen:

- Für die Aktualisierung muss die neueste veröffentlichte ThreadX 5.x-Firmware in Form eines **.rsp**-Pakets zur Verfügung stehen.
- Der FQDN des WDM-Servers muss für **DHCP**- oder **DNS**-Konfigurationen zur Verfügung stehen.

- Cert.pem muss unter dem Pfad **WDM Installed directory (WDM-Installationsverzeichnis) > Wyse > WDM > Teradici** zur Verfügung stehen. Dies ist nicht erforderlich, wenn der Fingerabdruck zum DHCP-Options-Tag oder über den DNS\_SRV-Datensatz hinzugefügt wurde, wie in vorangegangenen Kapiteln erläutert.

**ANMERKUNG:** Cert.pem wird zum Erstellen des Zertifikatspakets und Bereitstellen auf ThreadX 4.x-Clients verwendet.

Vor der Aktualisierung der ThreadX-Geräte müssen Sie folgende Richtlinien berücksichtigen:

- Informationen zum Suchen nach ThreadX-Geräten mithilfe des DNS-SRV-Eintrags finden Sie unter [Hinzufügen des DNS-SRV-Eintrags.Verwaltung von Teradici-Geräten mit WDM](#)
- Informationen zum Bereitstellen des Zertifikats auf ThreadX 4.x-Geräten finden Sie unter [Bereitstellen des Zertifikats auf ThreadX 4.x-Geräten](#).
- Informationen zum Upgrade von ThreadX-Geräten finden Sie unter [Upgrade der Client-Firmware auf ThreadX 5.x](#).

## Bereitstellen des Zertifikats auf ThreadX 4.x-Geräten

So stellen Sie das Zertifikat auf ThreadX 4.x-Geräten bereit:

- 1 Starten Sie die WDM-GUI und melden Sie sich bei WDM mit Administratorrechten an.
- 2 Navigieren Sie zu **Applications (Anwendungen) > PCoIP Configuration Packages (PCoIP-Konfigurationspakete)**.
- 3 Klicken Sie auf die Schaltfläche „+“ und laden Sie das Utility **PCoIP Configuration Manager** herunter.
- 4 Starten Sie das heruntergeladene Utility und wählen Sie die Optionsschaltfläche **Version 4.x**.
- 5 Klicken Sie auf die Option **Security (Sicherheit)** und deaktivieren Sie das Kontrollkästchen „Certificate“ (Zertifikat).
- 6 Kopieren Sie den Inhalt von **cert.pem** einschließlich der ersten und letzten Zeile (Beginnzertifikat und Endzertifikat).
- 7 Fügen Sie den Inhalt aus **cert.pem** in das vorgesehene Textfeld ein.
- 8 Geben Sie den Namen und die Beschreibung des Pakets in das entsprechende Textfeld ein.
- 9 Klicken Sie auf das Menü **Register (Registrieren)** und **speichern** Sie die Konfiguration.
- 10 Rufen Sie die Seite **Devices (Geräte)** in der in WDM-Web-UI auf und wählen Sie das gewünschte Gerät mithilfe des Kontrollkästchens.
- 11 Klicken Sie auf die Schaltfläche für die **Aktualisierung** und wählen Sie das erstellte Konfigurationspaket aus der Kategorie **PCoIP Configuration Packages (PCoIP-Konfigurationspakete)** und klicken Sie auf **save (Speichern)**.
- 12 Rufen Sie die Seite **Jobs** und bestätigen Sie, dass die Paketbereitstellung erfolgreich abgeschlossen wurde.

## Aktualisieren der Client-Firmware auf ThreadX 5.x

### Bereitstellen der Teradici-Image-Version 5.x

Zum Aktualisieren der Zero-Clients mit Firmware-Version 4.8.0, die mit dem neuen WDM-5.7.3-Zertifikat aktualisiert wurden oder falls der Sicherheitsmodus auf dem Client gering ist, muss das Repository Support Package (rsp) für die Teradici-Firmware-Aktualisierung mit dem alten Betriebssystemtyp als TDC erstellt werden. Dies ist für das Upgrade der Firmware von der kompatiblen Version 4.x auf Version 5.x erforderlich.

Gehen Sie wie folgt vor, um ein RSP-Paket zu erstellen:

- 1 Gehen Sie zu der [Teradici-Support-Website](#) und laden Sie die aktuelle ThreadX 5.X-Firmware herunter.
- 2 Erstellen Sie eine Datei mit folgendem Inhalt, speichern Sie die Datei im **.rsp**-Format und geben Sie den Dateinamen als *Zahlenwert* in der Datei an.

**ANMERKUNG:** Der Wert im Feld *Number* (Zahl) ist der Name der Firmwaredatei. Im folgenden Beispiel lautet der Wert `522r5_2@39075.03b193e.5957929`.

```
[Version]
Number=522r5_2@39075.03b193e.5957929
Description=PCoIP Tera2 Firmware Release 5.2.2 for P25, P45, and 5050 AIO
OS=TDC
ImageSize=0
ImageType=merlin
Category=Images
[Script]
RB
```

- Erstellen Sie einen neuen Ordner und platzieren Sie die `.all`-Datei.

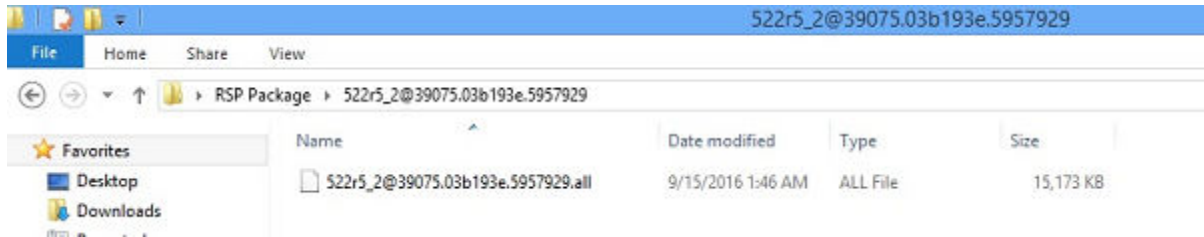


Abbildung 85. RSP-Paketordner

- Benennen Sie den Ordner in einen *Zahlenwert* in der `.rsp`-Datei um.
- Platzieren Sie die `.rsp`-Datei außerhalb des Ordners.

**ANMERKUNG:** Der Dateiname der `.rsp`-Datei, der Name des Paketordners und der Zahlenwert müssen übereinstimmen.

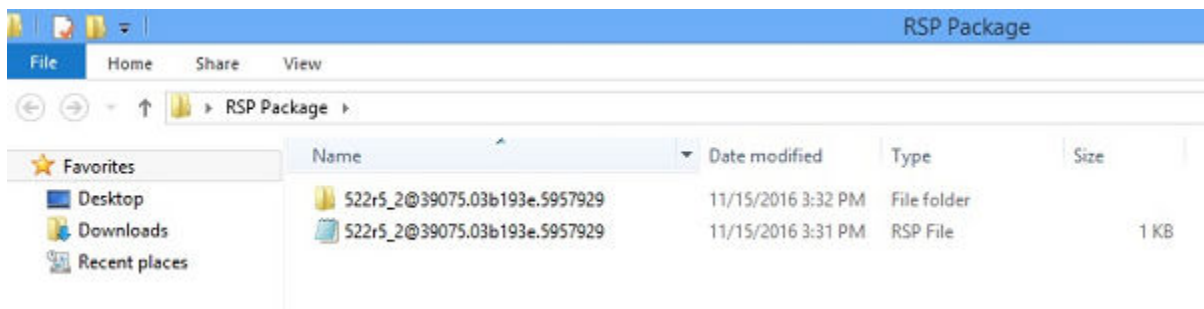


Abbildung 86. RSP-Paketordner

Nach der Bereitstellung des erstellten RSP-Pakets über WDM wie unter [Bereitstellen der Teradici-Image-Version 5.x von 4.x Firmware mithilfe von DDC in WDM](#) und [Bereitstellen der Teradici-Image-Version 5.x mithilfe ausgewählter Geräte in WDM](#) beschrieben, checkt der Client nach erfolgreichem Upgrade der Firmware auf 5.x als 5.x-Gerät bei WDM ein und WDM erkennt diese als ThreadX 5.x-Geräte. Für das künftige RSP-Paket für die 5.x-Firmwareaktualisierung ist der neue Betriebssystemtyp TDC5 (BS=TDC5) erforderlich.

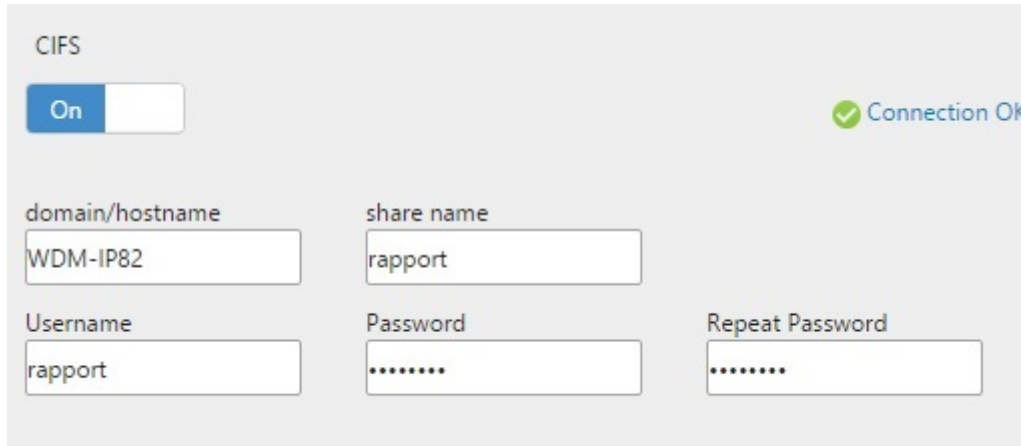
**ANMERKUNG:** Alle Verwaltungsfunktionen von ThreadX 5.x-Geräten (Geräte mit WDM-kompatibler 5.x-Firmware) einschließlich der Bereitstellung von RSP-Paketen mit TDC5 als Betriebssystemtyp (Betriebssystemtyp) können nur über die WDM-Web-UI bereitgestellt werden und werden bei Verwendung der Desktopversion von WDM nicht unterstützt.

## Voraussetzung für WDM-Repository für die Bereitstellung von Firmware und des OSD-Logos über die WDM-Web-UI für ThreadX 5.x-Geräte

Für die Bereitstellung von Firmwarepaketen mit Betriebssystemtyp TDC5 und Paketen mit OSD-Logo (On Screen Display) für ThreadX 5.x-Geräte ist es erforderlich, dass das CIFS-Protokoll aktiviert ist, um die Dateien aus dem WDM-Repository hochzuladen.

Stellen Sie sicher, dass die Test-Verbindung zum Software-Repository für CIFS erfolgreich hergestellt wurde. Gehen Sie zum Testen der CIFS-Verbindung wie folgt vor:

- 1 Öffnen Sie die WDM-Web-UI und melden Sie sich als Administrator an.
- 2 Gehen Sie zu **System > Repositories (Repositorys)**.
- 3 Klicken Sie im CIFS-Abschnitt auf den Link **Check Connection** (Verbindung prüfen).



CIFS

On

Connection OK

domain/hostname: WDM-IP82

share name: rapport

Username: rapport

Password: .....

Repeat Password: .....

Abbildung 87. CIFS

Fügen Sie nach einem Test der CIFS-Verbindung die folgenden Konten zum FTP-Ordner **Rapport** hinzu und geben Sie Freigabeberechtigungen auf dem Computer an, auf dem das WDM-Repository konfiguriert ist:

- Systemkonto des Servers, auf dem die ThreadX 5.X-Komponente installiert ist.
- Benutzerkonto, das für die WDM-Installation verwendet wird.

**ANMERKUNG:** Wenn das Repository auf einem anderen Server installiert ist, fügen Sie das Computerkonto des ThreadX 5.x-Servers anstelle des Systemkontos sowie das Benutzerkonto hinzu.

Um Berechtigungen für den im WDM-Repository verfügbaren Ordner **Rapport** zu gewähren, führen Sie die folgenden Schritte durch:

- 1 Gehen Sie zum Speicherort des **ftproot**-Ordners, wo der Ordner **Rapport** vorhanden ist.
- 2 Klicken Sie mit der rechten Maustaste auf den Ordner **Rapport** und wählen Sie **Properties** (Eigenschaften) aus.
- 3 Klicken Sie auf die Registerkarte **Sharing** (Freigabe) und anschließend auf **Advanced Sharing** (Erweiterte Freigabe).

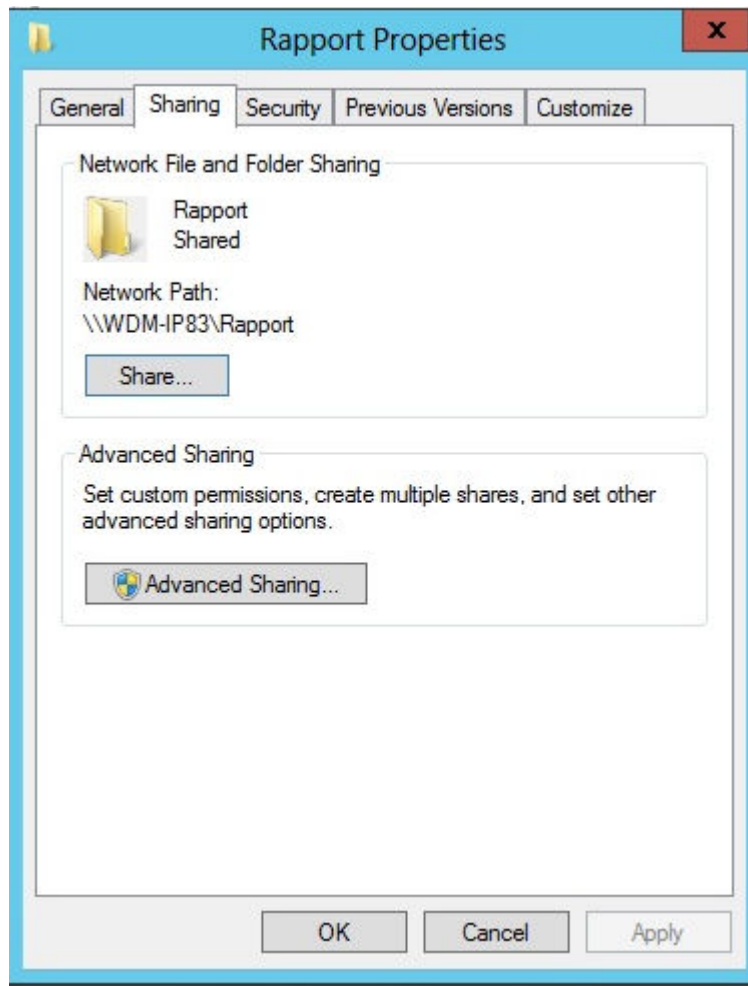


Abbildung 88. Rapport-Eigenschaften

- 4 Klicken Sie im Dialogfeld **Advanced Sharing** (Erweiterte Freigabe) auf **Permissions** (Berechtigungen).

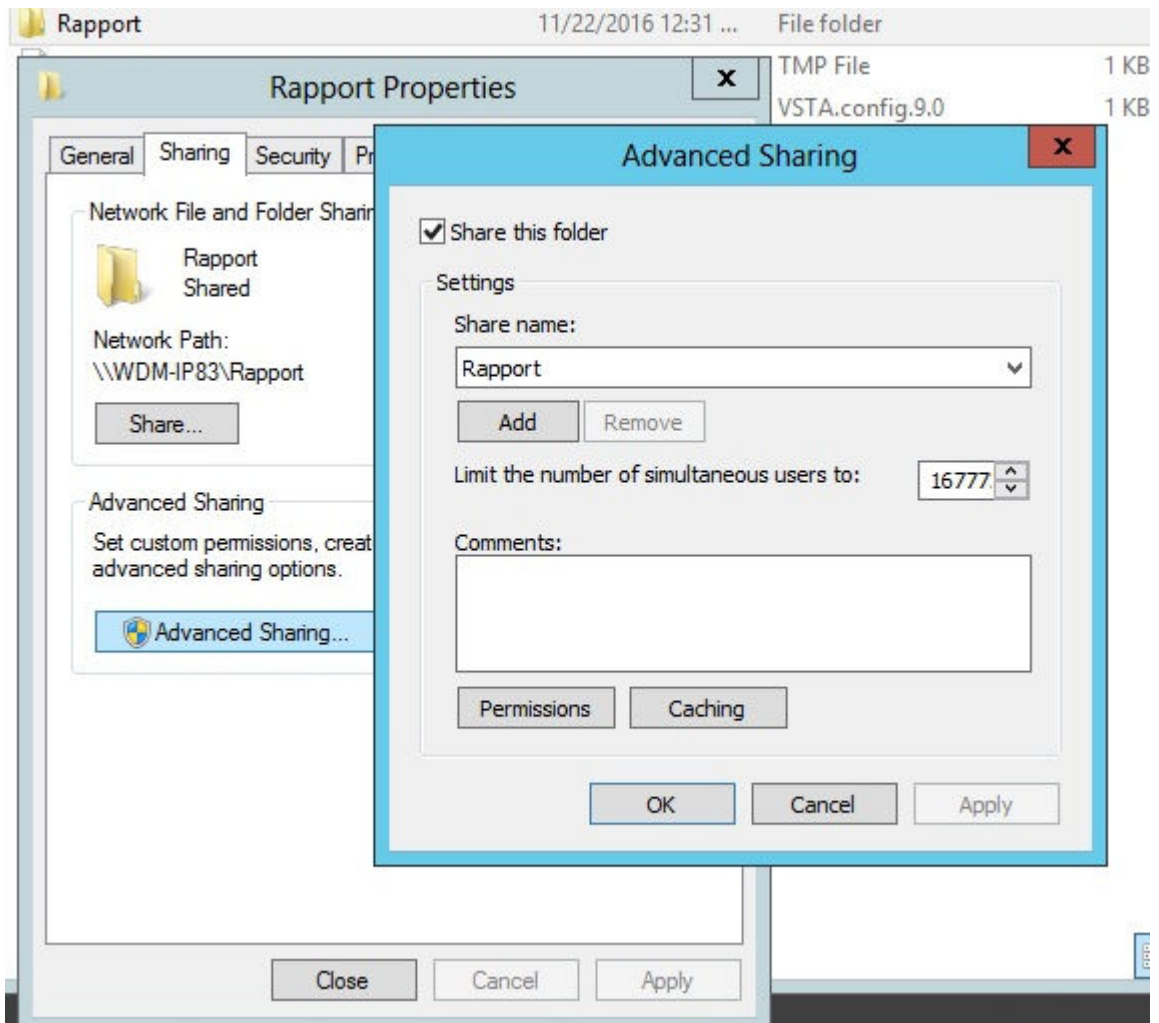


Abbildung 89. Erweiterte Freigabe

- 5 Klicken Sie auf die Schaltfläche **Add** (Hinzufügen) und erteilen Sie dem oben genannten Benutzer volle Berechtigungen.

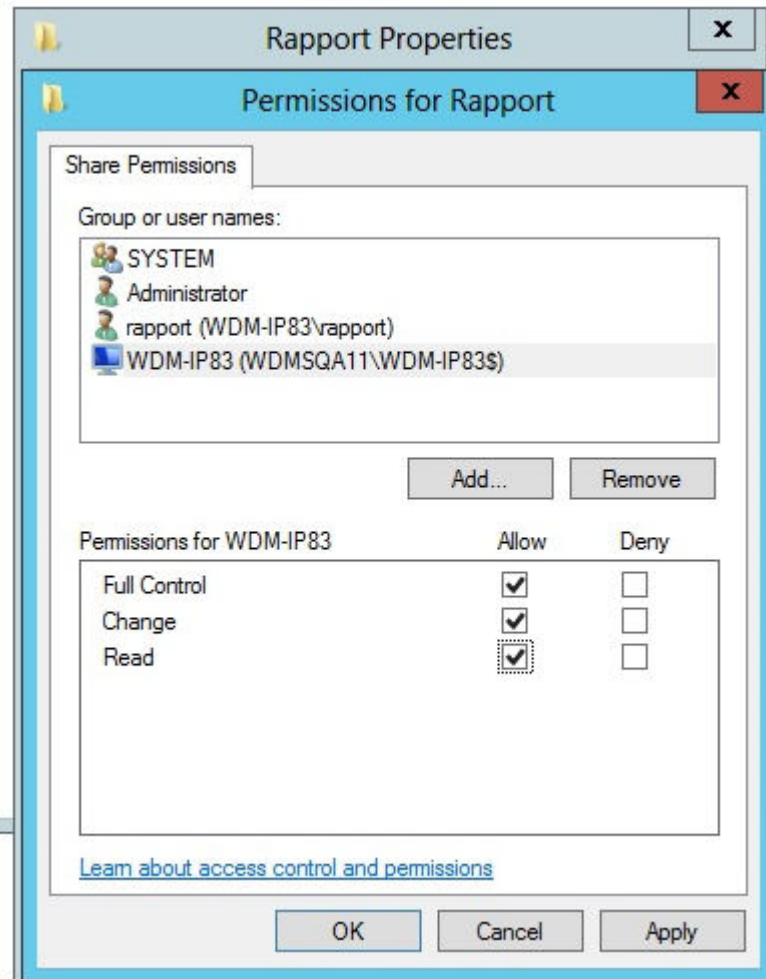


Abbildung 90. Berechtigungen für Rapport

## Bereitstellen der Teradici-Abbildversion 5.x von 4.x Firmware mithilfe von DDC in WDM

Um die Teradici-Abbildversion 5.x von 4.x Firmware mithilfe von DDC in WDM bereitzustellen, führen Sie die folgenden Schritte durch:

- 1 Öffnen Sie die WDM Web UI und melden Sie sich als Administrator an.
- 2 Gehen Sie zu **System > Console** (Konsole), aktivieren Sie **Default Device Configuration (DDC) (Standardgerätekongfiguration)** und klicken Sie auf die Schaltfläche **Save (Speichern)**.
- 3 Gehen Sie zu **Updates > DDC** und klicken Sie auf die Schaltfläche **+**, um eine neue DDC hinzuzufügen.
- 4 Wählen Sie ThreadX als Betriebssystem in der Dropdown-Liste **Select Operating System (Betriebssystem auswählen)** aus.
- 5 Wählen Sie die gewünschte Mediengröße in der Dropdown-Liste **Select Media Size (Mediengröße auswählen)** aus.
- 6 Wählen Sie die gewünschte Ansicht aus der Dropdown-Liste.
- 7 Klicken Sie auf **Add (Hinzufügen)**, um die neue DDC in die Gruppen zu integrieren.
- 8 Wählen Sie ein registriertes Abbild aus der Dropdown-Liste „Image“ (Abbild).
- 9 Wählen Sie das registrierte Zertifikatpaket aus der Dropdown-Liste „Packages“ (Pakete).
- 10 Wählen Sie das Einchecken für Geräte aus der Dropdown-Liste „Execute DDC“ (DDC ausführen) aus.
- 11 Klicken Sie auf die Schaltfläche **Save (Speichern)**, um DDC zu speichern.
- 12 Wechseln Sie zur Seite **Devices (Geräte)** und aktualisieren Sie die Geräteinformationen. Das Gerät wird neu gestartet und von WDM automatisch als ThreadX 5x-Gerät erkannt.

# Bereitstellen der Teradici-Image-Version 5.x mithilfe ausgewählter Geräte in WDM

Führen Sie zum Bereitstellen der Teradici-Image-Version 5.x mithilfe ausgewählter Geräte in WDM die folgenden Schritte durch:

- 1 Öffnen Sie die WDM Web UI und melden Sie sich als Administrator an.
- 2 Navigieren Sie zu **Applications (Anwendungen) > Images** und klicken Sie auf die Schaltfläche **+** um das Dienstprogramm für die Paketregistrierung herunterzuladen.
- 3 Klicken Sie auf die Schaltfläche **RSP** im Utility für WDM-Paketregistrierung.
- 4 Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen) und laden Sie das ThreadX 5.x-Firmware-Paket zu WDM hoch.
- 5 Wechseln Sie erneut zur WDM-Web-UI und navigieren Sie zur Seite **Devices** (Geräte).
- 6 Wählen Sie über die Kontrollkästchen die zu aktualisierenden Geräte.
- 7 Klicken Sie auf die Schaltfläche **Update** (Aktualisierung) und wählen Sie ein registriertes Paket aus der Kategorie Images.
- 8 Klicken Sie auf die Schaltfläche **Save** (Speichern), um die Paketbereitstellung zu planen. Das Paket wird bereitgestellt.
- 9 Rufen Sie die Seite **Aufgaben** auf und bestätigen Sie, dass die Paketbereitstellung erfolgreich abgeschlossen wurde. Das Gerät wird neu gestartet und von WDM automatisch als ThreadX 5x-Gerät erkannt.

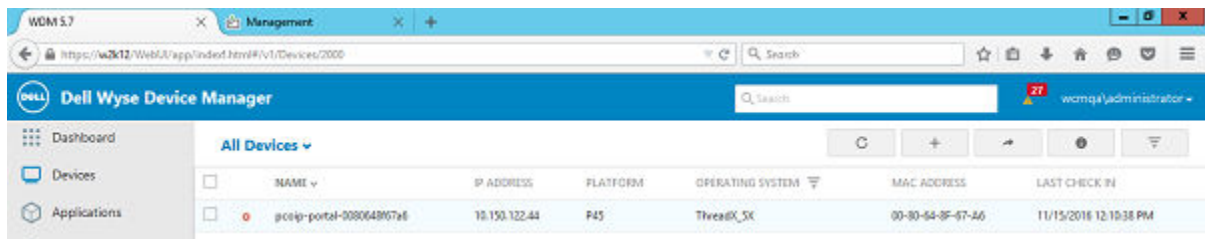


Abbildung 91. Geräte

- ⓘ **ANMERKUNG:** Wenn nach der erfolgreichen Bereitstellung der 5.x-Firmware auf dem Client die Geräte in WDM nicht als ThreadX5x-Geräte aufgeführt sind, befolgen Sie die Anweisungen unter **EMSDK wird aufgrund der Portnummer nicht gestartet** zur Behebung des Portkonflikts der ThreadX 5x-Softwarekomponenten und prüfen Sie anschließend, ob das Problem dadurch behoben werden konnte.

# Fehlerbehebung

Dieser Abschnitt enthält Fehlerbehebungsinformationen für WDM.

Themen:

- Probleme beim Erkennen von Geräten
- Probleme beim Erkennen von PXE-Geräten
- Paketfehler
- Wake-on-LAN-Befehl wird nicht auf Remote-Geräten ausgeführt
- Probleme bei der Peer-gestützten Verteilung
- Profil-Manager-Fehler
- Tipps zur Behebung von Fehlern beim Repository
- Fehlerbehebung bei T50- und WTOS-Fehlern
- Fehlerbehebung bei WCM-Problemen
- Paketaktualisierung schlägt fehl, wenn das CIFS-Repository aktiviert ist
- PAD Image-Erstellung und Drag-and-Drop-Funktionen funktionieren auf Linux-Geräten nicht
- Standardgerätekonfiguration zeigt exportierte Images nicht an
- VNC-Protokoll wird nicht generiert
- Das Fenster „Update Now“ (Jetzt aktualisieren) wird für den Benutzer für WCM-Linux nicht angezeigt
- Abgerufenes Image kann nicht zurück auf T50-Gerät übertragen werden
- Bereitstellung des PCoIP-Sprachpakets fehlgeschlagen
- Geräte meldet sich nicht bei japanischem BS an
- Anwendungsfehler nach der WDM-Aktualisierung von Version 5.5 oder MR auf 5.7
- ThinOS-Gerät unterbricht Anmeldung beim WDM-Server
- Problem beim Erkennen von Geräten mit alten HAagents – 6.3.2.54 und niedriger – auf lokalisiertem WDM-Server
- Anmeldeseite erscheint nicht in der Web-UI
- Problem bei der Anmeldung bei der Web-UI
- EMSDK startet nicht aufgrund der Portnummer
- Fehler bei Domain-Benutzeranmeldungen und HAPI-Protokoll
- Probleme beim Zugriff auf die Seite „Device“ (Gerät)
- OSD-Logo-Konfigurations- oder Firmware-Übertragungsfehler auf ThreadX 5.X-Geräten
- ThreadX 5.X-Gerätestatus wechselt zu „Offline“
- Manuelles Konfigurieren von ThreadX 5.X-Geräten unter Verwendung der Teradici-Verwaltungskonsole, wenn keine automatische Konfiguration möglich ist
- Konfiguration von WDM-Dienstprogrammen nicht möglich
- Konfiguration von WCM, Paketregister, Remote-Shadow und PCoIP nicht möglich

## Probleme beim Erkennen von Geräten

**Problem:** Sie haben Probleme beim Erkennen von Geräten.

Lösung: Stellen Sie Folgendes sicher:

- 1 Der Geräteservice wird korrekt ausgeführt.
- 2 Der Serverservice wird korrekt ausgeführt.
- 3 Der Pfad zwischen dem Geräteservice und dem Serverservice wird korrekt ausgeführt (verwenden Sie Ping).
- 4 Subnetz- und IP-Bereiche sind ordnungsgemäß konfiguriert (wenn Sie versuchen, Geräten anhand des Subnetz- oder IP-Bereichs zu erkennen).

Sie können auch das **Utility DNS\_DHCP\_Lookup** ausführen, um zu überprüfen, ob der WDM--Server erreichbar ist oder nicht.

## Probleme beim Erkennen von PXE-Geräten

Problem: Sie haben Probleme beim Erkennen von PXE-Geräten.

Lösung: Stellen Sie sicher, dass:

- 1 Port 4011 bei allen Routern offen ist.
- 2 IP-Helper-Adressen definiert sind und auf den WDM--Server verweisen.
- 3 Die PXE-Geräte nach der Erkennung durch WDM- mindestens 1x neu gestartet wurden (bevor WDM- sie als PXE-Geräte erkennt, müssen die PXE-Geräte nach der Erkennung mindestens 1x neu gestartet werden).

## Paketfehler

Problem: Sie erhalten Paketfehler.

Lösung: Versuchen Sie Folgendes:

- 1 Überprüfen Sie die Skript-Syntax.
- 2 Bearbeiten Sie das Skript (\*.rsp) und deaktivieren Sie den LU-Befehl (Zielgerät muss verfügbar sein).
- 3 Verwenden Sie einen Network Sniffer.
- 4 Stellen Sie sicher, dass sich die WDM--Server-IP-Adresse nicht verändert hat.
- 5 Stellen Sie sicher, dass die Repository-Informationen korrekt sind
- 6 Stellen Sie sicher, dass Sie einen manuellen FTP-Vorgang für eine Datei für das Repository durchführen können.
- 7 Stellen Sie sicher, dass Sie eine unbeaufsichtigte Installation durchführen können
- 8 Stellen Sie sicher, dass die Paketstruktur korrekt ist (Ordner = \*.rsp name = scripts'NUMBER'value).

## Wake-on-LAN-Befehl wird nicht auf Remote-Geräten ausgeführt

Problem: Der HServer kann den WOL-Befehl nicht an die Remote-Geräte senden.

Lösung: Port-Weiterleitung für UDP-Port 16962 aktivieren.

## Probleme bei der Peer-gestützten Verteilung

Dieser Abschnitt beschreibt einige häufig auftretende Probleme oder Fragen, die Sie möglicherweise in Bezug auf Peer-gestützte Verteilung haben.

**Feststellen, ob die für PAD verwendete HTTP-Anwendung ausgeführt wird und reagiert.**

Die für PAD verwendete HTTP-Anwendung akzeptiert den V99-Befehl, der zu Systemen über den Browser gesendet werden kann. Die Antwort auf den V99-Befehl von der HTTP-Anwendung wäre &00. Wenn die HTTP-Anwendung zum Beispiel auf einem System mit der URL 10.150.202.101 ausgeführt wird und sie Port 9980 abhört, würde der V99-Befehl wie folgt lauten:

```
http://10.150.202.101:9980/v99
```

Die entsprechende Antwort auf diesen Befehl würde wie folgt lauten:

&00

**ANMERKUNG:** Das System verwendet keine Standardauthentifizierung für den V99-Befehl.

### HTTP-Anwendung manuell ausführen.

So führen Sie die HTTP-Anwendung manuell aus:

- 1 Starten Sie die Eingabeaufforderung auf dem System, auf dem Sie WDM installiert haben.
- 2 Geben Sie den folgenden Befehl ein:

```
Wyse-Http-server.exe -u < Username > -p < Password > -Po < Port number >
```

- **u** ist hierbei der Benutzername für die Standardauthentifizierung, **-p** das Kennwort für die Standardauthentifizierung und **-po** die Portnummer, über die die HTTP-Anwendung ausgeführt wird.

### Das Peer-Gerät kann keine Image-Datei herunterladen.

Wenn das Peer-Gerät die Dateien **bios.img** oder **cmos.img** nicht herunterladen kann, müssen Sie überprüfen, ob sich die Dateien unter folgendem Ordnerpfad auf dem PAD-Master-Gerät befinden: **C:\Program Files\WDM**.

### Feststellen, ob sich die Kommunikation zwischen dem WDM-Agent- und dem WDM-Server auf den PAD-Zeitplan bezieht.

Bei sämtlicher Kommunikation zwischen dem WDM--Agent und dem WDM--Server, die sich auf den PAD-Zeitplan bezieht, müsste der PAD-Tag im Rahmen der Anforderung oder Antwort auf **1** gesetzt sein.

## Profil-Manager-Fehler

Dieser Abschnitt beschreibt die Probleme, die beim Profil-Manager auftreten können, und die Schritte zur Fehlerbehebung.

### Die WCM-Anwendung startet während der Erstellung des Profil-Manager-Pakets nicht.

Dieses Problem kann auftreten, wenn die WCM-Anwendung oder ihre Komponenten beschädigt oder im Installationsordner nicht verfügbar sind.

### Profil-Manager-Paket wird nicht bereitgestellt.

So beheben Sie dieses Problem:

- 1 Überprüfen Sie, ob der Profil-Manager in den Einstellungen aktiviert ist, um weitere Informationen zu erhalten.
- 2 Überprüfen Sie, ob die Profil-Manager-Bereitstellung vom Client-System unterstützt wird. Gehen Sie dazu wie folgt vor:
  - a Wählen Sie den Knoten **Device Manager (Geräte-Manager)** im Baumstrukturbereich der WDM--Konsole.
  - b Wählen Sie im rechten Fensterbereich das Gerät, für das Sie das Paket bereitstellen möchten.
  - c Klicken Sie im Fensterbereich **Device Properties (Geräteeigenschaften)** auf die Registerkarte **Hardware Info (Hardwareinformationen)**.
  - d Das Feld **WCM Support (WCM-Unterstützung)** sollte auf **True (Wahr)** gesetzt sein. Wenn das Feld auf **False (Falsch)** eingestellt wird, bedeutet das, dass der Client die Bereitstellung des Profil-Manager-Pakets nicht unterstützt und Sie den WDM-Agent auf dem Client aktualisieren müssen.
- 3 Überprüfen Sie, ob es geplante Pakete gibt, die noch bereitgestellt werden müssen. Warten Sie, bis die Pakete erfolgreich bereitgestellt wurden.
- 4 Überprüfen Sie, ob geplante Pakete mit Status **Error (Fehler)** vorhanden sind. Wenn solche Pakete vorhanden sind, löschen Sie diese.
- 5 Überprüfen Sie vor der Bereitstellung, ob der Client bereits mit dem Profil-Manager-Paket aktualisiert wurde. Um dies zu überprüfen, konfigurieren Sie den Profil-Manager für die Bereitstellung eines weiteren Pakets mit einer anderen Konfiguration.

# Tipps zur Behebung von Fehlern beim Repository

## Allgemeine Tipps:

Wenn die Repository-Testverbindung fehlschlägt, stellen Sie sicher, dass folgende Einstellungen vorliegen, die zur ordnungsgemäßen Ausführung des Repository erforderlich sind:

- Stellen Sie sicher, dass die Benutzer-ID und das Kennwort für das Repository korrekt sind.
- Navigieren Sie zum rapport-Benutzer und aktivieren Sie die Option **Password never expires** (Kennwort läuft nie ab).
- Stellen Sie sicher, dass die IP-Adresse bzw. der Hostname des Repository-Servers korrekt ist.

## Tipps zur Übertragungsart FTP:

Wenn die Repository-Testverbindung im Falle von FTP fehlschlägt, stellen Sie sicher, dass folgende Einstellungen vorliegen, die zur ordnungsgemäßen Ausführung des Repository erforderlich sind:

- Der FTP-Dienst wird ausgeführt.
- Die FTP-Site wurde erstellt.
- Für alle Benutzer mit „Basic“ (Standardauthentifizierung) und „Anonymous“ (Anonyme Authentifizierung) sind die Berechtigungen „Read“ (Lesen) und „Write“ (Schreiben) aktiviert.
- Versuchen Sie, mithilfe der Eingabeaufforderung eine FTP-Verbindung herzustellen.
  - ftp <ip address> <userid>.
  - Bei diesem Befehl werden Sie zur Eingabe des Kennworts aufgefordert und es wird eine Verbindung zum FTP-Verzeichnis hergestellt.

## Tipps zur Übertragungsart HTTP:

Wenn die Repository-Testverbindung im Falle von HTTP fehlschlägt, stellen Sie sicher, dass folgende Einstellungen vorliegen, die zur ordnungsgemäßen Ausführung des Repository erforderlich sind:

- Stellen Sie sicher, dass das virtuelle Verzeichnis vorhanden ist. Wenn dies nicht der Fall ist, befolgen Sie die unten angegebenen Schritte, um es zu erstellen:
  - Klicken Sie in der Taskleiste auf **Start->Administrative Tools (Verwaltungstools)->Internet Information Services (IIS) Manager (Internetinformationsdienste (IIS)-Manager)**, um das Fenster **IIS Manager** zu öffnen.
  - Klicken Sie mit der rechten Maustaste im Strukturbereich auf **Sites (Websites)->Default Web Site (Standardwebsite)** und wählen Sie dann **Add Application...** (Anwendung hinzufügen...) aus, um mit der Erstellung eines virtuellen Verzeichnisses zu beginnen.
  - Geben Sie den **Alias** (den Namen des virtuellen Verzeichnisses, z. B. **MyWDM** (MeinWDM)) ein, wählen Sie unter **Physical path** (Physischer Pfad) das FTP-Stammverzeichnis (z. B. c:\inetpub\ftproot) aus und klicken Sie anschließend auf **OK**.
  - Wählen Sie **Sites (Websites)->Default Web Site (Standardwebsite)->MyWDM (Mein WDM)** aus und doppelklicken Sie dann auf „Authentication“ (Authentifizierung). Aktivieren Sie „Basic Authentication“ (Standardauthentifizierung) im Bereich „Actions“ (Actions).
  - Um zu überprüfen, ob das virtuelle Verzeichnis konfiguriert ist oder nicht, wählen Sie im Strukturbereich **Sites (Websites)->Default Web Site (Standardwebsite)->MyWDM (Mein WDM)** aus und klicken Sie anschließend im rechten Fensterbereich auf **Browse\*: 80(http)** (\*:80(http) durchsuchen). Daraufhin wird das ftp-Verzeichnis im Browser (IE) geöffnet.
- Suchen Sie nach folgender Einstellung im IIS, um zu überprüfen, ob folgende Rollendienste installiert sind:
  - WebDAV-Veröffentlichung
  - Standardauthentifizierung
  - Windows-Authentifizierung
  - IIS Management Console (IIS-Verwaltungskonsole)

- IIS-Verwaltungsskripte und -tools
- Stellen Sie sicher, dass die folgenden Rollendienste nicht in IIS installiert sind:
  - Request Filtering (Anfragefilter)
  - Static Content Compression (Statische Inhaltskomprimierung)
  - Dynamische Inhaltskomprimierung
- Stellen Sie sicher, dass in der Anwendungspoolliste im Bereich „Advanced Settings“ (Erweiterte Einstellungen) von DefaultAppPool folgende Einstellungen vorliegen:
  - Stellen Sie sicher, dass „Enable 32-Bit Applications“ (32-Bit-Anwendungen aktivieren) im Abschnitt „General“ (Allgemein) auf „True“ (Wahr) gesetzt ist.
  - Stellen Sie sicher, dass „Idle Time-out (minutes)“ (Leerlaufzeit (Minuten)) im Abschnitt „Process Model“ (Prozessmodell) auf 0 (null) gesetzt ist.

### Tipps zur Übertragungsart HTTPS:

Wenn die Repository-Testverbindung im Falle von HTTPS fehlschlägt, sind dieselben Schritte durchzuführen, die auch zur Überprüfung der Richtigkeit der Konfigurationen für HTTP angewendet werden. Gehen Sie bei HTTPS wie folgt vor:

- 1 Starten Sie den IIS Manager und klicken Sie mit der rechten Maustaste auf **Default Web Site** (Standardwebsite).
- 2 Wählen Sie **Bindings** (Bindungen) in den Menüoptionen aus.
- 3 Überprüfen Sie im Fenster **Site Bindings** (Sitebindungen), ob **https** unter „Type“ (Typ) angegeben ist.
- 4 Überprüfen Sie, ob für die Standardportnummer **443** angezeigt wird.

### Tipps zur Übertragungsart bei CIFS:

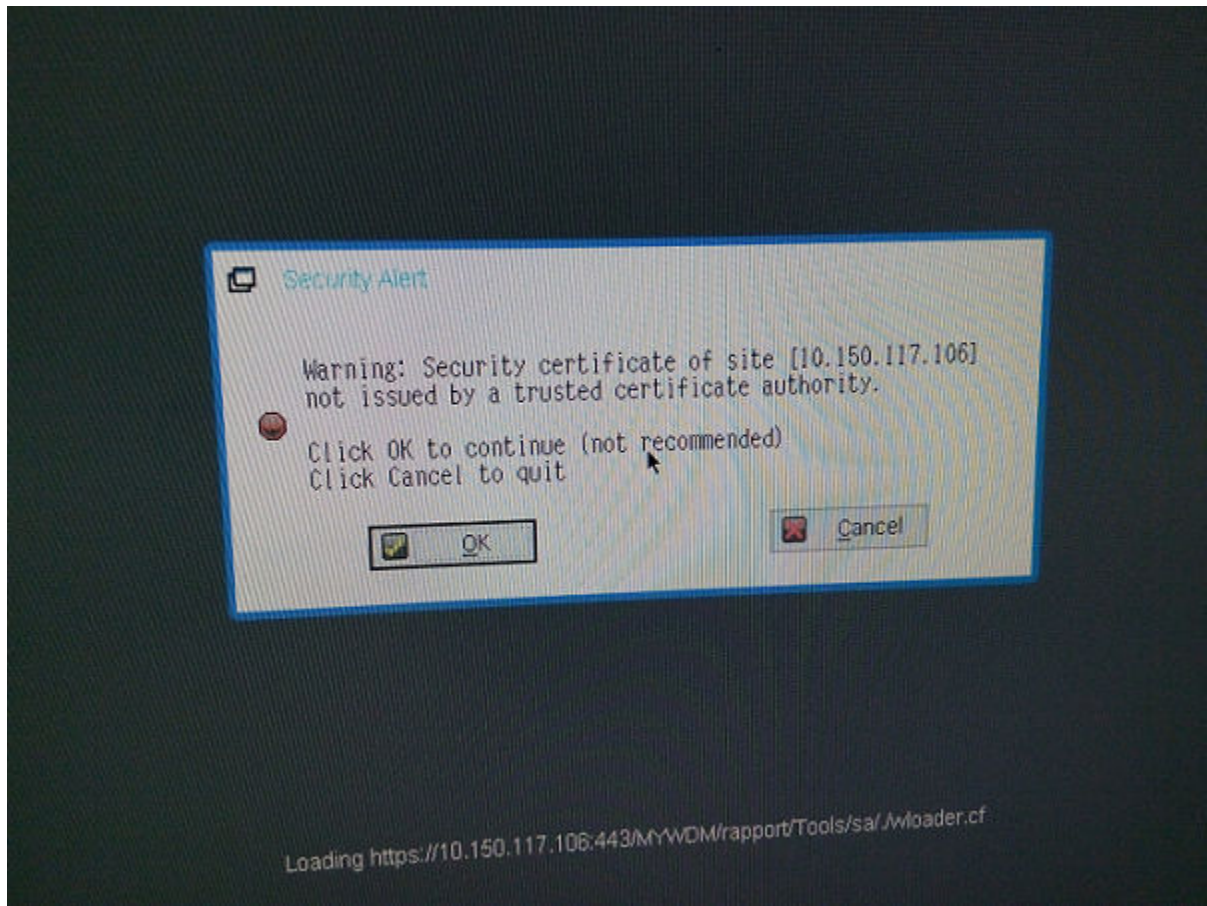
Wenn die Repository-Testverbindung im Falle von CIF fehlschlägt, stellen Sie sicher, dass die folgenden Einstellungen den Anforderungen entsprechen, damit das Repository funktioniert:

- Der Ordner **Rapport** ist freigegeben.
- Der Ordner **Rapport** weist die Berechtigungen **Read** (Lesen) und **Write** (Schreiben) für **Everyone** (Alle) oder bestimmte Benutzer auf.
- Geben Sie den Host-/Domännennamen, den Benutzernamen und das Kennwort für den Zugriff auf den freigegebenen Ordner ein und versuchen Sie, eine Verbindung herzustellen.

## Fehlerbehebung bei T50- und WTOS-Fehlern

Wenn sich T50-Geräte bei WDM 5.0 anmelden, werden möglicherweise Sicherheitswarnungen angezeigt.

Für Ubuntu T50-Geräte wird die folgende Meldung angezeigt:



**Abbildung 92. Sicherheitswarnung**

Klicken Sie auf **OK**, um fortzufahren.

Für WTOS-Geräte wird die folgende Meldung angezeigt:

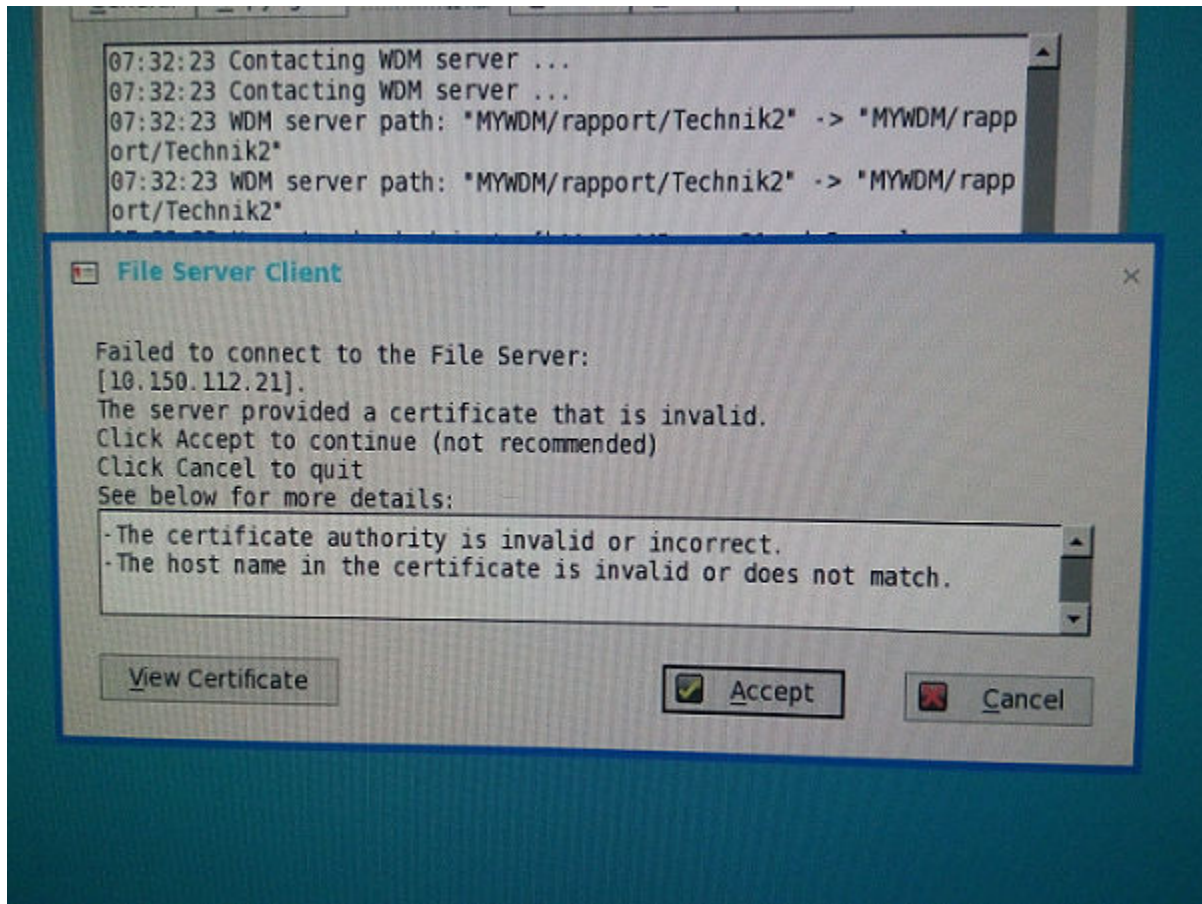


Abbildung 93. Dateiserver-Client

Klicken Sie auf **Accept** (Annehmen), um fortzufahren.

## Fehlerbehebung bei WCM-Problemen

Bei der Verwendung von WCM von WDM zum Erstellen von Konfigurationsdateien, die für Geräte bereitgestellt werden sollen, können möglicherweise die folgenden Probleme auftreten.

Wenn Sie die Konfigurationselemente auswählen und die Datei **configuration.xml** erstellen, fehlt der relative Pfad der XML-Datei. Die Lösung für dieses Problem lautet folgendermaßen: Bei der Erstellung von WCM-Paketen dürfen keine Leerzeichen im Dateinamen verwendet werden. Wenn Sie Ihre Konfigurationsdatei beispielsweise **WCM Config** nennen möchten, sollte Sie den Namen wie folgt angeben: **WCM\_Config**.

## Paketaktualisierung schlägt fehl, wenn das CIFS-Repository aktiviert ist

**Problem:** Wenn Sie CIFS Repository für alle Paketaktualisierungen aktivieren und das Paket auf einigen WES7-, WES7P-, WE8S- oder WES2009-Geräten bereitstellen, schlägt die Paketaktualisierung unter Umständen fehl. Dies könnte passieren, wenn der WDM-Agent bereits älter ist und keine Unterstützung für das CIFS-Protokoll bietet.

**Lösung:** Sie müssen den WDM-Agent auf allen Geräten, auf denen die Paketaktualisierung fehlschlägt, auf die aktuell verfügbare Version aktualisieren.

# PAD Image-Erstellung und Drag-and-Drop-Funktionen funktionieren auf Linux-Geräten nicht

**Problem:** Die Drag-and-Drop-Funktion des Pakets und die PAD-Image-Erstellungen funktionieren nicht auf SUSE Linux-Geräten mit dem MR 3 Build und der aktuellen WDM-Agent-Version 5.3.06, wenn die Windows-Authentifizierung auf WDM und das HTTPS-Protokoll im Software-Repository aktiviert ist.

**Lösung:** Aktivieren Sie die Standardauthentifizierung in IIS Manager oder ändern Sie das Protokoll in CIFS im Software-Repository.

# Standardgerätekonfiguration zeigt exportierte Images nicht an

**Problem:** Wenn Sie ein abgerufenes Image exportieren und in WDM erneut registrieren, wird das Image nicht im DDC-Fenster angezeigt.

**Lösung:**

- 1 Navigieren Sie zum Ordner, in dem sich die **.rsp**-Datei befindet.
- 2 Öffnen Sie die Datei in Notepad und nehmen Sie die folgende Änderung vor:

```
Command=%imageread% to Command=%imagewrite%
```

- 3 Speichern und schließen Sie die Datei. Das Image wird im DDC-Fenster angezeigt, wenn Sie die WDM-Konsole starten.

# VNC-Protokoll wird nicht generiert

**Problem:** Das VNC-Protokoll kann nicht generiert werden, wenn Sie ein FTP-Repository verwenden.

**Lösung:** Sie müssen die Firewall deaktivieren oder eine bestimmte eingehende Regel hinzufügen, um das VNC-Protokoll zu generieren.

# Das Fenster „Update Now“ (Jetzt aktualisieren) wird für den Benutzer für WCM-Linux nicht angezeigt

**Problem:** Das Fenster **Update Now (Jetzt aktualisieren)** wird für einen Benutzer nach der Übertragung der WCM-Datei für Linux-Geräte für den Benutzer nicht unmittelbar angezeigt.

**Lösung:** RebootQU wird zusammen mit der WCM-Konfiguration für Linux-Geräte geplant. RebootQU wird ausgeführt, wenn sich das Gerät teilweise oder vollständig anmeldet oder der Administrator das Gerät manuell aktualisieren muss.

# Abgerufenes Image kann nicht zurück auf T50-Gerät übertragen werden

**Problem:** Das abgerufenes Image kann nicht zurück auf ein T50-Gerät mit 8-MB-MICRON-Chip übertragen werden.

**Lösung:** Registrieren Sie das abgerufene Bild erneut, indem Sie den Tag `<wdmMessage> < \wdmMessage>` aus der `.rsp`-Datei löschen.

# Bereitstellung des PColP-Sprachpakets fehlgeschlagen

**Problem:** Das mit Erstellungswerkzeug **PColP-Konfigurationspaket** erstellte Sprachpaket konnte nicht bereitgestellt werden.

**Lösung:** Wenn sowohl Details für **Connection Management Interface (Verbindungsmanagementschnittstelle)** als auch für **VMware View Server (VMware View-Server)** angegeben sind, schlägt die Bereitstellung des Sprachpakets fehl, da sich beide Einstellungen gegenseitig ausschließen.

## Geräte meldet sich nicht bei japanischem BS an

**Problem:** Bei Geräten mit einer niedrigeren HAgent-Version als 6.3.2.54 melden sich diese nicht beim einem japanischen BS an.

**Lösung:** Aktualisieren Sie HAgent auf die aktuelle Version und führen Sie eine Erkennung der Geräte mit dem WDM-Server durch (es muss mindestens die Hagent-Version 6.3.2.54 installiert sein).

## Anwendungsfehler nach der WDM-Aktualisierung von Version 5.5 oder MR auf 5.7

**Problem:** Wenn Sie die Web-UI nach der Aktualisierung von WDM von Version 5.5 oder MR auf 5.7 starten, wird die Fehlermeldung **Application not found** (Anwendung nicht gefunden) angezeigt.

**Ursache:** Dieses Problem tritt auf, wenn die ID des Anwendungspools nicht richtig eingestellt ist, und das Kennwort abgelaufen oder beschädigt wurde.

Lösung:

- 1 Rufen Sie den IIS-Manager auf (geben Sie `inetmgr` unter Run unter Windows ein).

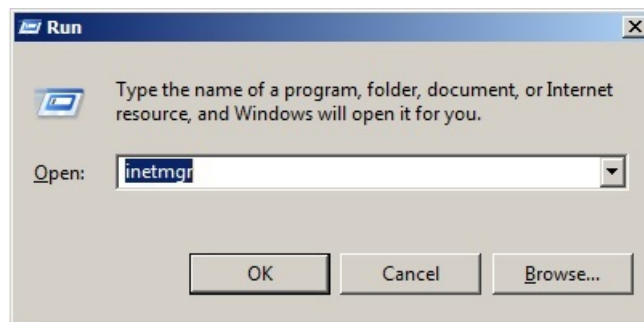


Abbildung 94. inetmgr

- 2 Navigieren Sie zum **ASP.NET v4.0**-App-Pool und wählen Sie die erweiterten Einstellungen. Wenn Sie diese Problembhebung zum ersten Mal durchführen, müssen Sie sich den Identitätswert notieren (siehe Abbildung für Beispiel) (`LINUXSERVER\Administrator`).

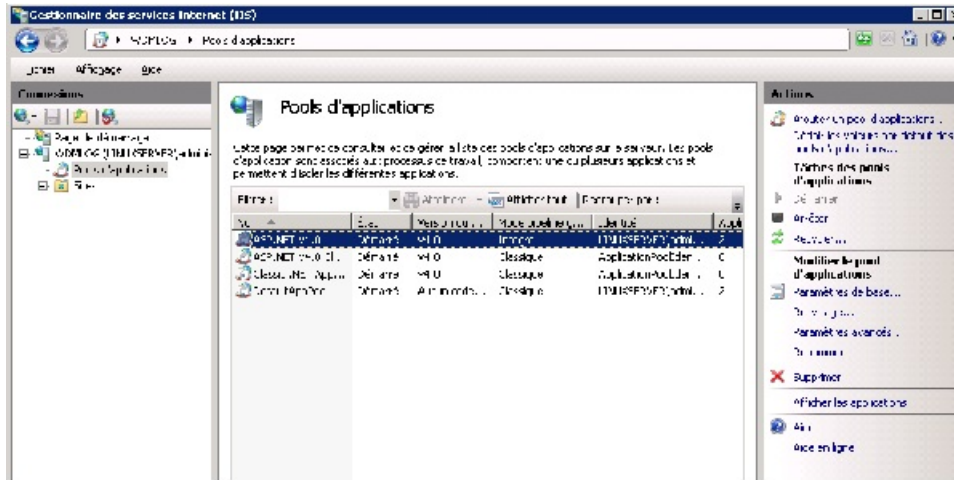


Abbildung 95. Anwendungen

- 3 Ändern Sie die Identitätseigenschaft in **ApplicationPoolIdentity**.

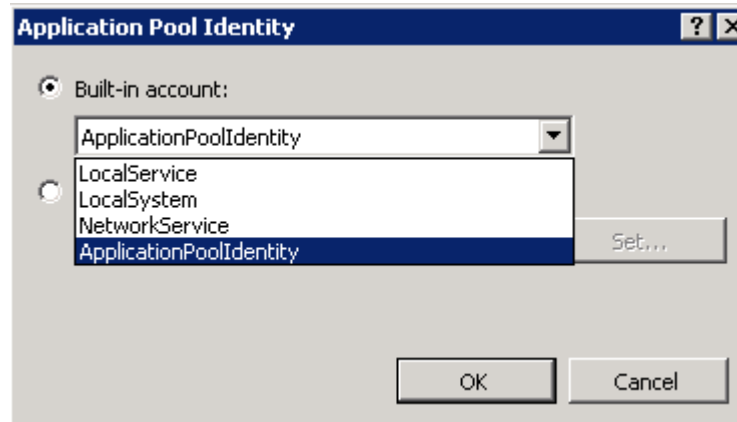
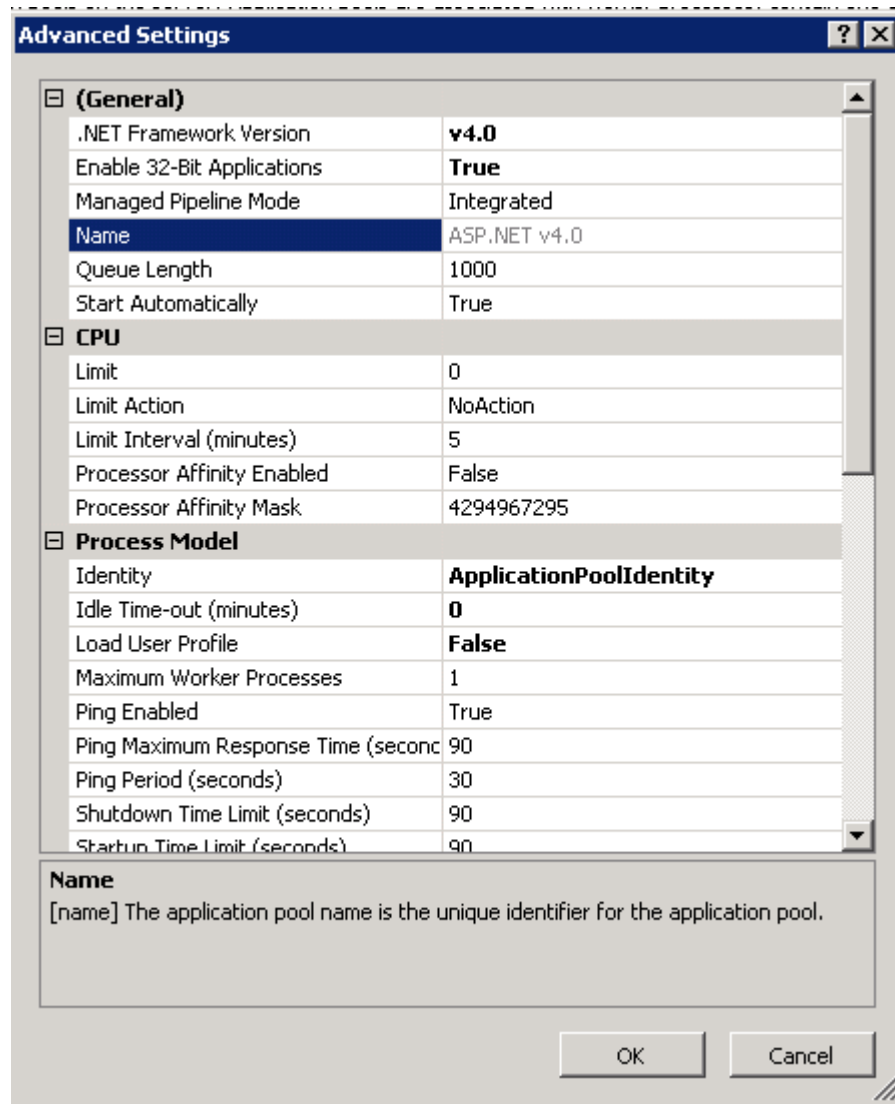


Abbildung 96. Erweiterte Einstellungen

- 4 Übernehmen Sie die Einstellungen und starten Sie den Anwendungspool, um die WDM-Web-UI auszuführen, um festzustellen, ob die Anwendung startet.
  - Wenn der Anmeldebildschirm in der Anwendung angezeigt wird, führen Sie Schritt 5 aus.

- 5 Befolgen Sie nun die Schritte 1 und 2 und legen Sie die Identität des **ASP.NET v4.0**-App-Pools auf die ursprüngliche Einstellung fest. Sie werden zur Eingabe des Kennworts und zur Bestätigung aufgefordert. Wenden Sie nach Eingabe des Kennworts die Einstellungen an und starten Sie den App-Pool. Sobald dies abgeschlossen ist, können Sie mit der Verwendung der Web-UI beginnen.

## ThinOS-Gerät unterbricht Anmeldung beim WDM-Server

Problem: ThinOS-Gerät unterbricht Anmeldung beim WDM-Server aufgrund eines nicht vertrauenswürdigen Zertifikats und eine Verwaltung ist nicht möglich.

Lösung: Es müssen die folgenden .ini-Einstellung an das Gerät gesendet werden:

**securitypolicy=low**

Schritte zur Bereitstellung für das Gerät:

- Erstellen Sie einen Ordner mit dem Namen **wnos** unter **ftp**.
- Erstellen Sie eine .ini-Datei mit dem Namen **wnos.ini** im Ordner **wnos** und fügen Sie in der .ini-Datei den Inhalt als **securitypolicy=low** hinzu.
- Geben Sie auf dem Gerät den Speicherort des **ftp**-Servers an.
- Das Gerät lädt die .ini-Datei herunter und übernimmt die Einstellungen.

## Problem beim Erkennen von Geräten mit alten HAgents – 6.3.2.54 und niedriger – auf lokalisiertem WDM-Server

Problem: Geräte mit alten HAgents (6.3.2.54 & niedriger) auf lokalisiertem WDM-Server werden nicht erkannt.

Voraussetzungen: Wenn die Regeln zu **RequestFilteringModule** hinzugefügt wurden, müssen Sie diese anhand der folgenden Schritte exportieren. .

Lösung:

- 1 Klicken Sie auf den Stamm **IIS**.
- 2 Wählen Sie **Modules** (Module) im rechten Fensterbereich.
- 3 Klicken Sie mit der rechten Maustaste auf **RequestFilteringmodule** und wählen Sie **Unlock** (Entsperren), um den Vorgang fortzusetzen.
- 4 Wählen Sie den **Rapport-HTTP-Server** im linken Fensterbereich von IIS.
- 5 Doppelklicken Sie auf **Modules** (Module) im rechten Fensterbereich, wählen Sie **RequestFilteringModule** und löschen Sie das **Modul**, um den Vorgang fortzusetzen.
- 6 Starten Sie den **Rapport-HTTP-Server** neu.
- 7 Starten Sie die **Geräte** neu oder der Agent meldet sich beim WDM-Server an.
- 8 Aktualisieren Sie den **HAgent** auf das aktuell verfügbare Paket.
- 9 Fügen Sie **RequestFilteringmodule** hinzu, um diese Schritte einzuhalten.
- 10 Wählen Sie den **Rapport-HTTP-Server**, doppelklicken Sie auf **Modules** (Module) und wählen Sie **Revert** (Zurück), um aus dem rechten Menü zurückzukehren.
- 11 Wählen Sie **RequestFilteringmodule** und klicken Sie auf **OK**,  
um fortzufahren.

12 Gehen Sie zurück zum Stamm **IIS**, wählen Sie **Modules** (Module), klicken Sie mit der rechten Maustaste auf **RequestFilteringmodule** und wählen Sie dann **Lock** (Sperren).

13 Starten Sie den Server neu.

Importieren Sie nach Beendigung alle Schritte die Regeln wieder zurück in das Modul.

## Anmeldeseite erscheint nicht in der Web-UI

**Problem:** Als zum ersten Mal eine Verbindung mit der Web-UI über den IE-Browser hergestellt wurde, ist der Bildschirm leer und es wird nicht der Anmeldebildschirm angezeigt.

**Lösung:** Aktualisieren Sie den Browser, um die Anmeldeseite anzuzeigen.

## Problem bei der Anmeldung bei der Web-UI

**Problem:** Eine Anmeldung bei der WDM-Web-UI ist nicht möglich, wenn der WDM-Server dem Windows Server 2012-Domänencontroller beigetreten ist.

**Lösung:** Die Funktion **GetAuthorizationGroups()** schlägt auf Ihnen standardmäßig hinzugefügten Gruppen (SIDs) fehl, wenn ein 2012-Domänencontroller beteiligt ist.

Durch die Installation von [KB2830145](#) auf dem WDM-Server wird das Problem behoben.

## EMSDK startet nicht aufgrund der Portnummer

**Problem:** EMSDK-Komponente nutzt für die Kommunikation standardmäßig Portnummer 49155. Wenn das Starten von EMSDK aufgrund der Nichtverfügbarkeit des genannten Ports fehlschlägt, muss der Benutzer den EMSDK-Server, der auf der Konsole des Rechners ausgeführt wird, auf dem Software installiert ist, manuell stoppen und eine verfügbare Portnummer in den folgenden Dateien angeben:

Lösung:

- 1 Wechseln Sie zum Programmdateipfad, in dem die EDM-Datei installiert ist `\\Wyse\WDM\Teradici\EMSDK`, öffnen Sie die `emsdk.properties`-Datei in Notepad und weisen die verfügbare Portnummer im Feld `emserver.serverPort=49155` zu, z. B. 49159.
- 2 Stellen Sie die neue Portnummer in der Datei `C:\inetpub\wwwroot\ThreadXApi\Web.config` fest, indem Sie die gleiche Datei im Texteditor öffnen und bringen die Portnummer unter folgendem Tag ersetzen:
  - `<appSettings><add key="EmSdkPort" value="49155"/></appSettings>`
- 3 Starten Sie den Rechner neu.

## Fehler bei Domain-Benutzeranmeldungen und HAPI-Protokoll

**Problem:** Anmeldefehler bei Domänenbenutzer. Die folgende HApi-Protokoll-Fehlermeldung wird angezeigt:

**An error (1301) occurred while enumerating the groups. The group's SID could not be resolved** (Beim Aufzählen der Gruppen ist ein Fehler [1301] aufgetreten. Die SID der Gruppe konnte nicht aufgelöst werden).

**Lösung:** Installieren Sie den Microsoft-Hotfix über den Link und versuchen Sie erneut, WDM zu verwenden:  
[www.support.microsoft.com/en-us/kb/2830145](http://www.support.microsoft.com/en-us/kb/2830145)

**Problem:** Bei der Web-UP-Anmeldung tritt ein Fehler auf, wenn Sie den Rechnernamen den Benutzeranmeldeinformationen voranstellen.

**Lösung:** Geben Sie den Benutzernamen und die Anmeldeinformationen OHNE vorgestellten Rechnernamen ein.

# Probleme beim Zugriff auf die Seite „Device“ (Gerät)

**Problem:** Sie haben Probleme mit dem Zugriff auf die Seite „Device“ (Gerät). Sie werden abgemeldet, wenn Sie versuchen auf die Seite zuzugreifen.

**Lösung:** Löschen Sie die Cookies und den Cache des Systems und versuchen Sie, sich erneut anzumelden.

# OSD-Logo-Konfigurations- oder Firmware-Übertragungsfehler auf ThreadX 5.X-Geräten

**Problem:** Die OSD-Logo-Konfiguration oder die Firmware-Aktualisierung konnte nicht übertragen werden.

**Lösung:** Stellen Sie sicher, dass die Test-Verbindung zum Software-Repository für CIFS erfolgreich erstellt wurde.

Fügen Sie die folgenden Konten zu den Freigabeberechtigungen für den Ordner „Rapport“ hinzu:

- Systemkonto des Servers, auf dem ThreadX 5.X installiert ist.
- Benutzerkonto, das für die WDM-Installation verwendet wird.

So erteilen Sie Berechtigungen für einen Benutzer:

- 1 Klicken Sie mit der rechten Maustaste auf den Ordner „Rapport“ im Repository und wählen Sie Eigenschaften aus.
- 2 Klicken Sie auf die Registerkarte **sharing** (Freigabe).
- 3 Rufen Sie die Option für die erweiterte Freigabe auf und klicken Sie auf **permissions** (Berechtigungen).
- 4 Klicken Sie auf die Schaltfläche „Add“ (Hinzufügen) und erteilen Sie dem oben genannten Benutzer volle Berechtigungen.

# ThreadX 5.X-Gerätestatus wechselt zu „Offline“

**Problem:** ThreadX 5.X-Gerätestatus wechselt nach einigen Tagen nach Erkennung zu „Offline“.

**Lösung:**

- 1 Gehen Sie zu IIS Management Console.
- 2 Navigieren Sie zu „Application Pools“ (Anwendungspools).
- 3 Klicken Sie mit der rechten Maustaste auf den ASP.NET v4.0-Anwendungspool und klicken Sie auf **Stop** (Anhalten).
- 4 Klicken Sie mit der rechten Maustaste auf „Advanced Settings“ (Erweiterte Einstellungen) für den ASP.NET v4.0-Anwendungspool.
- 5 Scrollen Sie nach unten bis zum Abschnitt „Recycling“.
- 6 Legen Sie den Wert für **Regular Time Interval(minutes)** (Reguläres Zeitintervall in Minuten) auf 0 fest.

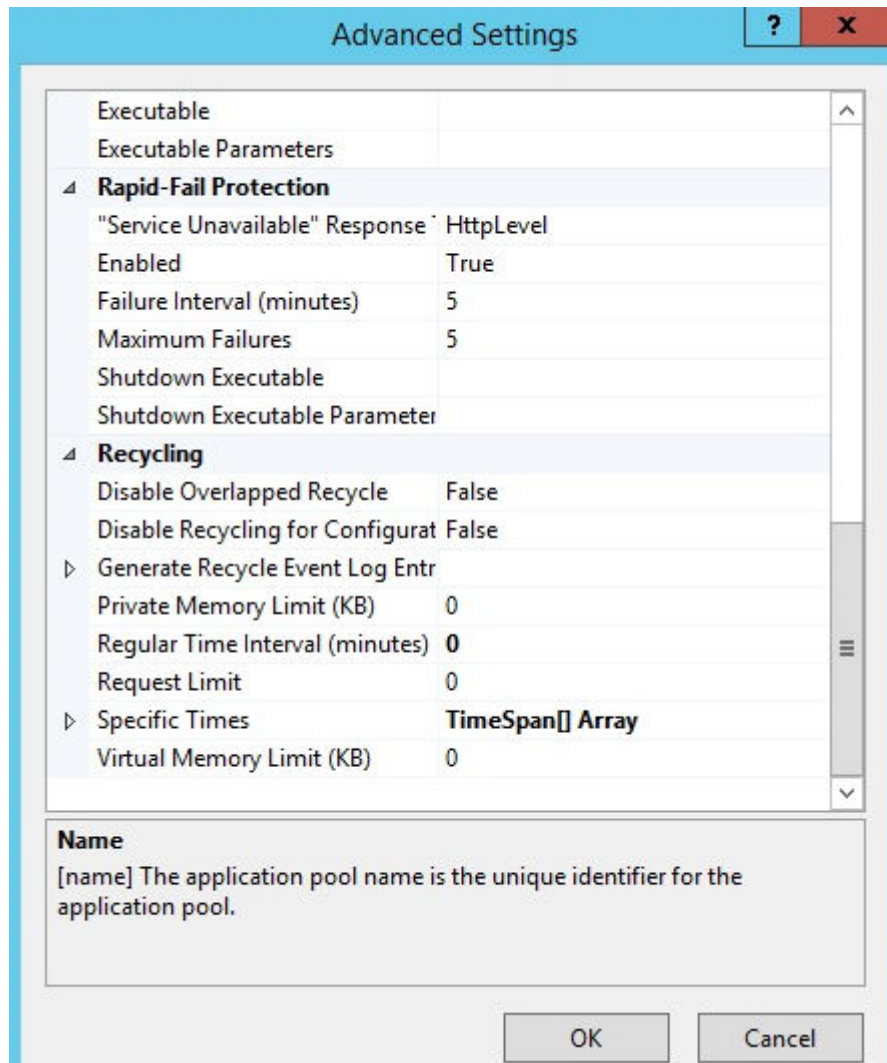


Abbildung 97. Erweiterte Einstellungen

- 7 Klicken Sie mit der rechten Maustaste auf den ASP.NET v4.0-Anwendungspool und klicken Sie auf **Start**.

## Manuelles Konfigurieren von ThreadX 5.X-Geräten unter Verwendung der Teradici-Verwaltungskonsole, wenn keine automatische Konfiguration möglich ist

Voraussetzung: Stellen Sie sicher, dass EMSDK und ThreadXapi installiert sind und erfolgreich auf dem Gerät ausgeführt werden.

- 1 Wählen Sie in der Verwaltungskonsole des ThreadX-Geräts **Upload Menu (Upload-Menü) > Certificate (Zertifikat)** aus und navigieren Sie zum Zertifikat **cert.pem** unter `<Wyse install folder>\WDM\TeraDici\cert.pem`, in dem WDM installiert ist. Nachdem Sie die Datei ausgewählt haben, klicken Sie auf **Upload** (Hochladen).

**ANMERKUNG:** Der Upload des cert.pem-Zertifikats ist für den Client wichtig, um eine Verbindung mit dem EMSDK-Server herzustellen, da der EMSDK-Server beim Verbindungsaufbau mit dem Server die Zertifikatsdaten des Clients validiert. Jegliche Abweichungen in den Zertifikatsdaten führen dazu, dass der Server die Verbindungsanfrage vom Gerät ablehnt.

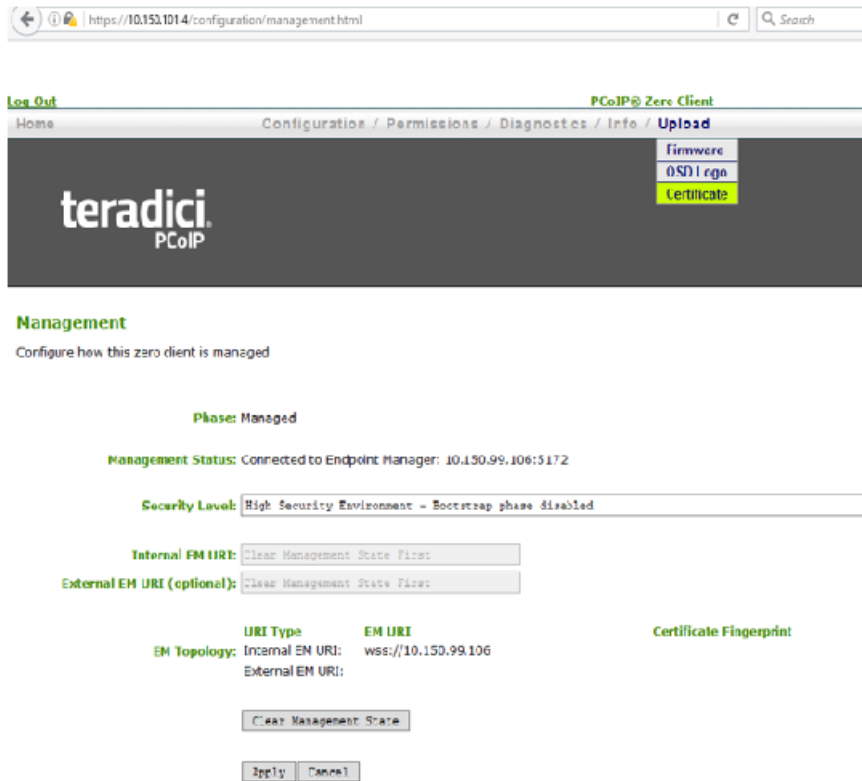


Abbildung 98. Bildschirm zur Konfiguration des Zertifikats

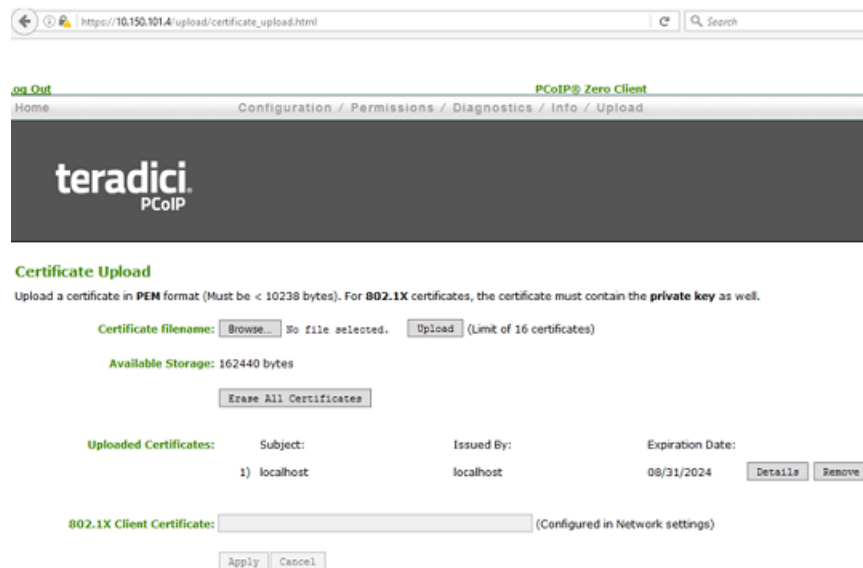


Abbildung 99. Bildschirm „Certificate Upload“ (Zertifikat hochladen)

- 2 Das erfolgreich hochgeladene Zertifikat wird im Abschnitt „Certificate Upload“ (Zertifikat hochladen) angezeigt.
- 3 Wählen Sie im Konfigurationsmenü der ThreadX-Geräteverwaltungskonsole **Management sub menu (Untermenü Verwaltung) > Security Level (Sicherheitsstufe) > High Security Environment – Bootstrap phase disabled (Umgebung mit hoher Sicherheit – Bootstrap-Phase deaktiviert)** aus.

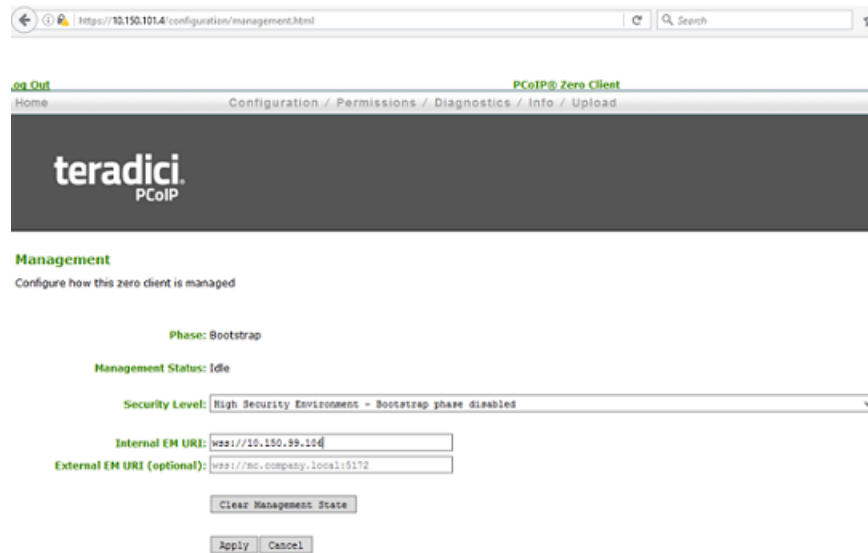


Abbildung 100. Bildschirm „Management“ (Verwaltung)

Geben Sie in das Feld **Internal EM URI** (Internes EM-URI) das URI des EMSDK-Server als **wss://<IP Address** des Rechners ein, auf dem ThreadX 5.X installiert ist, und klicken Sie auf die Schaltfläche **Apply** (Anwenden).

- 4 Klicken Sie auf die Schaltfläche **Continue** (Weiter), um den Vorgang fortzusetzen.

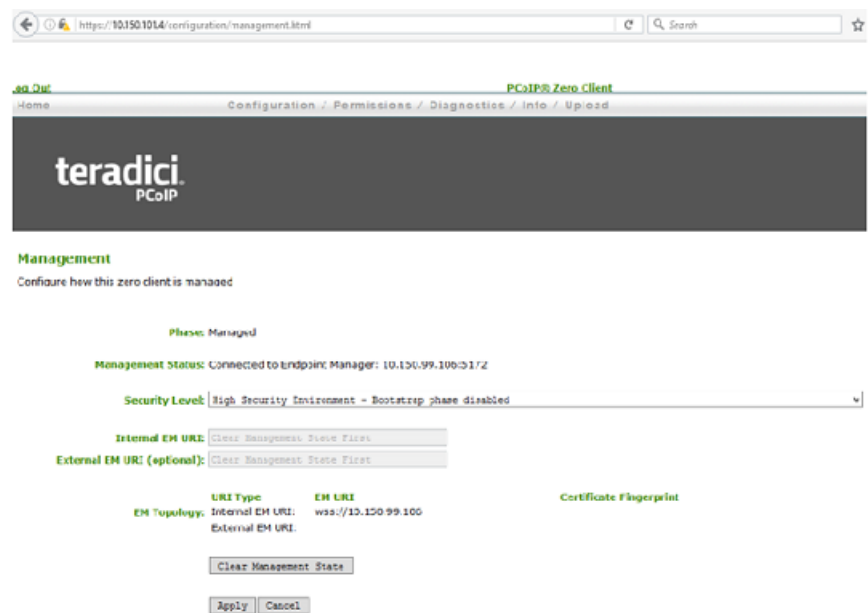


Abbildung 101. Bildschirm der mit dem EMSDK-Server verbundenen Konsole

**ANMERKUNG:** Geräte können in WDM nicht ermittelt werden, wenn die Clients verbunden sind, bevor der ThreadXApi-Dienst gestartet wird. Wenn keine Geräte ermittelt werden können, nachdem die Clients eine Verbindung mit EMSDK hergestellt haben, müssen Sie prüfen, ob der ThreadXApi-Dienst ausgeführt wird, indem Sie in der Protokolldatei unter C:\inetpub\wwwroot\ThreadXApi mit dem Namen ThreadXApi.txt nachschauen.

Nach erfolgreicher Überprüfung im WDM-Server werden die ermittelten Geräte in der WDM-UI angezeigt. Sie sollten die Befehle **Reboot** (Neu starten) und **Shutdown** (Herunterfahren) in Echtzeit ausführen, sobald diese in der Web UI verfügbar sind.

# Konfiguration von WDM-Dienstprogrammen nicht möglich

Problem: WDM-Dienstprogramme können nicht konfiguriert werden

Lösung: Versuchen Sie die folgenden Schritte zum Konfigurieren der WDM-Dienstprogramme.

- Während der erstmaligen Konfiguration des Dienstprogramms wird ein Fenster angezeigt.
- Sie müssen sicherstellen, dass der Inhalt von **WDMutilsExtract.exe** in dasselbe Verzeichnis extrahiert wird, in das die Datei **CustomprotocolforWDMutils.exe** heruntergeladen wird.
- Geben Sie den Pfad für die Datei **CustomprotocolforWDMutils.exe** in **Extrahieren in Verzeichnis** im Extraktionswerkzeug WDMutils ein.
- Wenn sich WDMutils nach der Konfiguration nicht öffnet, löschen Sie den Browser-Cache und den lokalen Speicher zum erneuten Einleiten des Konfigurationsvorgangs. Stellen Sie sicher, dass Sie die Datei **WDMutilsExtract.exe** in dasselbe Verzeichnis extrahieren, in das die Datei **CustomprotocolforWDMutils.exe** heruntergeladen wird.
- Wenn Sie den Browser-Cache und den Speicher nicht löschen möchten, gehen Sie zu dem Speicherort, an den Sie die Datei **CustomprotocolforWDMutils.exe** heruntergeladen haben. Führen Sie die Datei **CustomprotocolforWDMutils.exe** aus. Das Extraktionswerkzeug WDMutils wird angezeigt. Geben Sie den Pfad von **CustomprotocolforWDMutils.exe** im Feld **Extract to Directory** (Extrahieren in Verzeichnis) ein und klicken Sie auf **Extract** (Extrahieren).

# Konfiguration von WCM, Paketregister, Remote-Shadow und PCoIP nicht möglich

Problem: WDM-Dienstprogramme können nicht konfiguriert werden

Lösung: Wenn sich die benutzerdefinierte Protokolldatei nach der Konfiguration nicht öffnet, löschen Sie den Browser-Cache und den lokalen Speicher zum erneuten Einleiten des Konfigurationsvorgangs.