# Dell Wyse Management Suite

## Version 3.x – Schnellstarthandbuch

Februar 2022
Rev. A05

## Hinweise, Vorsichtshinweise und Warnungen

**ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

**VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.**

**WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.**

# Inhaltsverzeichnis

# 1

# Einführung

Wyse Management Suite ist die Managementlösung der nächsten Generation. Sie ermöglicht das zentrale Konfigurieren, Überwachen, Verwalten und Optimieren Ihrer mit dem Dell Hybrid Client betriebenen Endpunkte und Dell Thin Clients. Sie bietet außerdem erweiterte Optionen wie die Bereitstellung sowohl in der Cloud als auch vor Ort, eine Option zum Verwalten von überall aus über eine mobile App, erweiterte Sicherheit wie die BIOS-Konfiguration und die Portsperrung. Zu den weiteren Funktionen gehören die Suche nach Geräten und Registrierung, Bestands- und Inventarverwaltung, Konfigurationsmanagement, Bereitstellung von Betriebssystemen und Anwendungen, Echtzeitbefehle, Überwachung, Warnungen, Berichterstellung und Troubleshooting von Endgeräten.

## Editionen

Wyse Management Suite ist in den folgenden Editionen erhältlich:

- **Standard (kostenlos)** – Die Standard Edition der Wyse Management Suite bietet grundlegenden Funktionen und ist für die Bereitstellung in einer Private Cloud verfügbar. Ein Lizenzschlüssel ist nicht erforderlich, um die Standard-Edition zu verwenden. Diese Version kann Dell Thin Clients managen. Die Standard Edition eignet sich für kleine und mittelständische Unternehmen.
- **Pro (kostenpflichtig)** – die Pro Edition der Wyse Management Suite ist eine robustere Lösung. Sie ist für die Bereitstellung in öffentlichen und Private Clouds verfügbar. Zur Verwendung der Pro Edition (abonnementbasierte Lizenzierung) ist ein Lizenzschlüssel erforderlich. Mit der Pro-Lösung können Unternehmen ein Hybridmodell und bewegliche Lizenzen zum Wechsel zwischen der Bereitstellung in Public und Private Clouds nutzen. Diese Version ist für die Verwaltung von Teradici-basierten Geräten, Wyse Covert für PCs und Dell Hybrid Client betriebenen Geräten erforderlich. Sie bietet außerdem erweiterte Funktionen für die Verwaltung von Dell Thin Clients. Für eine Bereitstellung in der Public Cloud kann die Pro Edition in Nicht-Firmennetzwerken verwaltet werden (Home Office, Drittanbieter, Partner, mobile Thin Clients, usw.). Die Pro-Edition der Wyse Management Suite bietet außerdem:
  - Eine mobile App, zum Anzeigen von kritischen Warnungen sowie Benachrichtigungen und dem Senden von Befehlen in Echtzeit.
  - Verbesserte Sicherheit durch Zweifaktor-Authentifizierung und Active Directory-Authentifizierung für rollenbasierte Verwaltung.
  - Erweiterte App-Richtlinie und -Berichterstellung.

  **ANMERKUNG:**
  - Cloud-Services werden in den USA und Deutschland gehostet. Kunden in Ländern mit Einschränkungen für den Datenspeicherort werden u. U. nicht in der Lage sein, den Cloud-basierten Wyse Management Suite-Dienst zu nutzen.
  - Die lokale Version der Wyse Management-Pro-Edition ist eine bessere Lösung für Kunden mit Einschränkungen für den Datenspeicherort.

**Themen:**

- Wyse Management Suite-Funktionsmatrix

# Wyse Management Suite-Funktionsmatrix

Die folgende Tabelle enthält Informationen über die unterstützten Funktionen für jeden Abonnementtyp:

**Tabelle 1. Funktionen im Überblick für jeden Abonnementtyp**

| Funktionen | Wyse Management Suite Standard | Wyse Management Suite Pro – Private Cloud | Wyse Management Suite Pro – Cloud Edition |
|---|---|---|---|
| Hochgradig skalierbare Lösung zur Verwaltung von Thin Clients | Bis zu 10.000 Geräte freigeben | Bis zu 120.000 Geräte | Bis zu 1 Million Geräte |
| Lizenzbedingungen | Kostenloser Download | Abonnement pro Arbeitsplatz | Abonnement pro Arbeitsplatz |
| Lizenzschlüssel | Nicht erforderlich | Erforderlich | Erforderlich |

**Tabelle 1. Funktionen im Überblick für jeden Abonnementtyp (fortgesetzt)**

| Funktionen | Wyse Management Suite Standard | Wyse Management Suite Pro – Private Cloud | Wyse Management Suite Pro – Cloud Edition |
|---|---|---|---|
| Architektur | Private Cloud | Private Cloud | Public Cloud |
| Flexible Bereitstellung oder Hybrid Cloud | X | √ | √ |
| Erweitertes Installationsprogramm | X | √ | √ |
| Mehrmandantenfähigkeit | X | √ | √ |
| Delegierte Administration für die Granularität der Berechtigungen | X | √ | √ |
| Mehrere Repositories zur Unterstützung ihrer verteilten Architektur | X | √ | √ |
| Option zum Konfigurieren des Wyse Management Suite Server-Alias | X | √ | √ |
| Architektur für Hochverfügbarkeit | X | √ | X |
| Proxy-Support – SOCKS5 und HTTPS | √ | √ | √ |
| API-Unterstützung | X | √ | X |
| Dell ProSupport for Software enthalten | X | √ | √ |
| **Dell Endpunkte** | | | |
| OptiPlex 7070 Ultra mit Dell Hybrid Client | X | √ | √ |
| OptiPlex 3090 Ultra und 7090 Ultra mit Dell Hybrid Client | X | √ | √ |
| Latitude 3320 mit Dell Hybrid Client | X | √ | √ |
| Wyse 5070 mit Dell Hybrid Client | X | √ | √ |
| Wyse Thin Clients mit ThinOS | √ | √ | √ |
| Wyse Thin Clients mit ThinLinux | √ | √ | √ |
| Wyse Thin Clients mit Windows 10 IoT Enterprise | √ | √ | √ |
| Wyse PCoIP Zero Clients (Teradici-Firmware) | X | √ | √ |
| Software Thin Clients mit Wyse Converter for PCs | X | √ | √ |
| **Reporting und Überwachung** | | | |
| Lokalisierte Managementkonsole | X | √ | √ |
| Warnungen, Ereignisse und Auditprotokolle mithilfe von E-Mail- und mobilen Anwendungen | X | √ | √ |
| Berichterstellung der Unternehmensklasse | X | √ | √ |

Die folgende Tabelle enthält Informationen über die unterstützten Funktionen des Dell Hybrid Client-Managements für jeden Abonnementtyp:

### Tabelle 2. Dell Hybrid Client-Management Funktionsmatrix

| Funktionen des Dell Hybrid Client-Management | Wyse Management Suite Standard | Wyse Management Suite Pro – Private Cloud | Wyse Management Suite Pro – Cloud Edition |
|---|---|---|---|
| **Vollständige Sichtbarkeit des Bestands** | | | |
| Automatische Geräteermittlung | X | √ | √ |
| Anlagen-, Bestands- und Systemverwaltung | X | √ | √ |
| Effektive Konfiguration auf der Ebene der Wyse Management Suite nach Vererbung anzeigen | X | √ | √ |
| **Sicherheit** | | | |
| Sichere Kommunikation (HTTPS) | X | √ | √ |
| Sicheres MQTT | X | √ | √ |
| Multi-Factor Authentication | X | √ | √ |
| Active Directory-Authentifizierung für rollenbasierte Verwaltung | X | √ | √ |
| AD-Zuordnung mithilfe von LDAPs | X | √ | √ |
| Einmaliges Anmelden | X | √ | √ |
| Lockdown-Einstellungen (Aktivieren/Deaktivieren von Ports unterstützter Endpunkte) | X | √ | √ |
| **Umfassendes Management** | | | |
| Betriebssystempatch und Abbildverwaltung | X | √ | √ |
| Smarte Planung | X | √ | √ |
| Automatische Bereitstellung | X | √ | √ |
| Bundle-Anwendungen zur Vereinfachung der Bereitstellung und zum Minimieren von Neustarts | X | √ | √ |
| Dynamische Gruppenerstellung und -Zuweisung basierend auf Geräte-Attributen | X | √ | √ |
| Repository-Zuweisung zu Anwendungsrichtlinie und Subnetz-Zuordnung | X | √ | √ |
| Erweiterte Anwendungsverwaltung und Anwendungsrichtlinie | X | √ | √ |
| Nutzergruppenvererbung | X | √ | √ |
| Endnutzerausnahme | X | √ | √ |

### Tabelle 2. Dell Hybrid Client-Management Funktionsmatrix (fortgesetzt)

| Funktionen des Dell Hybrid Client-Management | Wyse Management Suite Standard | Wyse Management Suite Pro – Private Cloud | Wyse Management Suite Pro – Cloud Edition |
|---|---|---|---|
| Automatisches Aufheben der Registrierung von Geräten | X | √ | √ |
| **Konfiguration** | | | |
| Konfiguration des Assistenten für den Dell Hybrid Client | X | √ | √ |
| Multimonitor-Support | X | √ | √ |
| Follow-Me Profil | X | √ | √ |
| Dateizugehörigkeit zum Priorisieren des Anwendungsbereitstellungsmodus | X | √ | √ |
| BIOS-Einstellungen und Konfigurationsunterstützung | X | √ | √ |
| Konfiguration der Export- und Importrichtlinien | X | √ | √ |
| Standardmäßige Nutzergruppenrichtlinie | X | √ | √ |
| Browserkonfiguration | X | √ | √ |
| Konfigurieren des Cloud-Anbieters | X | √ | √ |
| Automatisierte Aktualisierung Dell signierter Anwendungen | X | √ | √ |
| Nutzerpersonalisierung Daten-Roaming | X | √ | √ |
| Konfigurieren von VNC | X | √ | √ |
| Konfigurieren von SSH | X | √ | √ |

**ANMERKUNG:** Dell Technologies empfiehlt das Upgrade des Systems auf 12 GB RAM, da für die sichere Kommunikation mehr Speicher erforderlich ist.

**ANMERKUNG:** Für eine Standardlizenz können Sie eine sichere MQTT-Verbindung (8443) nutzen, indem Sie Port 1883 vom Wyse Management Suite-Server mit der Windows Firewall blockieren.

Die folgende Tabelle enthält Informationen über die Verwaltungsfunktionen für Wyse Thin Clients und Zero Clients, die für jedes Abonnement unterstützt werden.

### Tabelle 3. Wyse Thin Client- und Zero Client-Management-Funktionsmatrix

| Managementfunktionen für Wyse Thin Clients und Zero Clients | Wyse Management Suite Standard | Wyse Management Suite Pro – Private Cloud | Wyse Management Suite Pro – Cloud Edition |
|---|---|---|---|
| **Vollständige Sichtbarkeit des Bestands** | | | |
| Automatische Geräteermittlung | √ | √ | √ |
| Anlagen-, Bestands- und Systemverwaltung | √ | √ | √ |

**Tabelle 3. Wyse Thin Client- und Zero Client-Management-Funktionsmatrix (fortgesetzt)**

| Managementfunktionen für Wyse Thin Clients und Zero Clients | Wyse Management Suite Standard | Wyse Management Suite Pro – Private Cloud | Wyse Management Suite Pro – Cloud Edition |
|---|---|---|---|
| Effektive Konfiguration auf Geräteebene nach Vererbung anzeigen | √ | √ | √ |
| **Reporting und Überwachung** | | | |
| Remote-Shadow mithilfe von VNC | √ | √ | |
| Konfigurierbarer Heartbeat- und Check-in-Intervall | √ | √ | √ |
| **Sicherheit** | | | |
| Sichere Kommunikation (HTTPS) | √ | √ | √ |
| 802.1x-Zertifikatbereitstellung | √ | √ | √ |
| Sicheres MQTT | √ | √ | √ |
| Zweifaktor-Authentifizierung | X | √ | √ |
| Active Directory-Authentifizierung für rollenbasierte Verwaltung | X | √ | √ |
| Domänenbeitrittsfunktion (Windows 10 IoT Enterprise) | X | √ | √ |
| AD-Zuordnung mithilfe von LDAPs | X | √ | √ |
| Lockdown-Einstellungen (Aktivieren oder Deaktivieren von Ports unterstützter Endpunkte) | X | √ | √ |
| **Umfassendes Management** | | | |
| Betriebssystempatch und Abbildverwaltung | √ | √ | √ ** |
| Smarte Planung | √ | √ | √ |
| Automatische Bereitstellung | √ | √ | √ |
| Bundle-Anwendungen zur Vereinfachung der Bereitstellung und zum Minimieren von Neustarts | X | √ | √ |
| Dynamische Gruppenerstellung und -Zuweisung basierend auf Geräte-Attributen | X | √ | √ |
| Repository-Zuweisung zu Anwendungsrichtlinie und Subnetz-Zuordnung | X | √ | √ |
| Automatisches Aufheben der Registrierung von Geräten | √ | √ | √ |
| Erweiterte Anwendungsrichtlinie | X | √ | √ |
| **Konfiguration** | | | |

**Tabelle 3. Wyse Thin Client- und Zero Client-Management-Funktionsmatrix (fortgesetzt)**

| Managementfunktionen für Wyse Thin Clients und Zero Clients | Wyse Management Suite Standard | Wyse Management Suite Pro – Private Cloud | Wyse Management Suite Pro – Cloud Edition |
|---|---|---|---|
| Konfiguration des Assistenten für Wyse ThinOS 8.x und 9.x | √ | √ | √ |
| Multimonitor-Support | √ | √ | √ |
| Wyse Easy Setup und Wyse Overlay Optimizer | √ | √ | √ |
| Scripting-Support für nutzerspezifische Anwendungsinstallation | X | √ | √ |
| BIOS-Einstellungen und Konfigurationsunterstützung | X | √ | √ |
| Konfiguration der Export- und Importrichtlinien | X | √ | √ |
| RSP-Paketunterstützung | X | √ | √ |
| WDM-Import-Tool | X | √ | X |
| Massenspeichergeräte-Ausnahme | X | √ | √ |

**ANMERKUNG:** ** Doppeltes Sternchen gibt an, dass für die Betriebssysteme ThinLinux-und Windows 10 IoT Enterprise ein vor-Ort-Repository erforderlich ist, wenn Sie die Wyse Management Suite Public Cloud-Umgebung verwenden.

**ANMERKUNG:** Dell Technologies empfiehlt das Upgrade des Systems auf 12 GB RAM, da für die sichere Kommunikation mehr Speicher erforderlich ist.

**ANMERKUNG:** Für eine Standardlizenz können Sie eine sichere MQTT-Verbindung (8443) nutzen, indem Sie Port 1883 vom Wyse Management Suite-Server mit der Windows Firewall blockieren.

**ANMERKUNG:** ThinOS 9.1.x, Dell Hybrid Client 1.5 und spätere Versionen, Wyse Device Agent 14.5.3.11 und spätere Versionen unterstützen Secure MQTT.

2

# Erste Schritte mit der Wyse Management Suite

Dieser Abschnitt enthält Informationen über die allgemeinen Funktionsmerkmale für den Einstieg als Administrator und das Verwalten von Thin Clients über die Wyse Management Suite Software.

**Themen:**



## Anmelden bei der Wyse Management Suite in einer Public Cloud

Zum Anmelden bei der Wyse Management Suite-Konsole benötigen Sie einen unterstützten Webbrowser, der auf dem System installiert ist. So melden Sie sich an der Wyse Management Suite-Konsole an:

1. Greifen Sie auf die Public Cloud (SaaS) Edition der Wyse Management Suite mithilfe einer der folgenden Links zu:
   - **US-Rechenzentrum** –us1.wysemanagementsuite.com/ccm-web
   - **EU-Rechenzentrum** –eu1.wysemanagementsuite.com/ccm-web
2. Geben Sie Ihren Nutzernamen und Ihr Kennwort ein.
3. Klicken Sie auf **Anmelden**.

   Wenn Sie sich zum ersten Mal bei der Wyse Management Suite Konsole anmelden, wenn ein neuer Nutzer hinzugefügt wird oder wenn eine Nutzerlizenz erneuert wird, wird die Seite **Geschäftsbedingungen** angezeigt. Lesen Sie die Bedingungen und Bestimmungen, wählen Sie die entsprechenden Kontrollkästchen aus und klicken Sie auf **Akzeptieren**.

**ANMERKUNG:** Sie erhalten Ihre Anmeldeinformationen bei der Anmeldung für die Testversion der Wyse Management Suite auf www.wysemanagementsuite.com oder beim Kauf Ihres Abonnements. Sie können das Wyse Management Suite-Abonnement vom Dell Vertrieb oder von Ihrem lokalen Dell Partner erwerben. Weitere Informationen finden Sie auf www.wysemanagementsuite.com.

**ANMERKUNG:** Ein extern zugängliches Repository muss auf einem Server mit einer DMZ während der Verwendung der Pro Edition von Wyse Management Suite in der Public Cloud installiert werden. Zudem muss der vollständig qualifizierte Domainname (FQDN) des Servers im öffentlichen DNS registriert werden.

### Ändern Ihres Kennworts

So ändern Sie Ihr Anmeldekennwort:

1. Klicken Sie auf den Kontolink in der oberen rechten Ecke der Managementkonsole.
2. Klicken Sie auf **Kennwort ändern**.

**ANMERKUNG:** Es wird empfohlen, Ihr Kennwort nach der ersten Anmeldung zu ändern. Die Standardnutzernamen und Kennwörter für zusätzliche Administratoren werden von dem Wyse Management Suite-Kontobesitzer erstellt.

### Abmelden

So melden Sie sich bei der Managementkonsole ab:

1. Klicken Sie auf den Kontolink in der oberen rechten Ecke der Managementkonsole.
2. Klicken Sie auf **Abmelden**.

# Voraussetzungen für Wyse Management Suite in einer Private Cloud

### Tabelle 4. Voraussetzungen

| Beschreibung | 10 000 Geräte oder weniger | 50 000 Geräte oder weniger | 120 000 Geräte oder weniger | Wyse Management Suite – Software-Repository |
|---|---|---|---|---|
| Betriebssystem | Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019 Standard Der Wyse Management Suite Webserver verfügt über einen integrierten Apache Tomcat Webserver. Stellen Sie sicher, dass Sie Microsoft IIS Apache Tomcat Webserver nicht separat installieren.<br>Unterstützte Sprachpakete: Englisch, Französisch, Italienisch, Deutsch, Spanisch, Japanisch und Chinesisch (Vorschau-Version) | | | |
| Mindest-Festplattenspeicherplatz | 40 GB | 120 GB | 200 GB | 120 GB |
| Mindest-Arbeitsspeicher (RAM) | 8 GB | 16 GB | 32 GB | 16 GB |
| Minimale CPU-Anforderungen | 4 | 4 | 16 | 4 |
| Netzwerkkommunikationsports | Das Wyse Management Suite-Installationsprogramm fügt die TCP-Ports (Transmission Control Protocol) 443, 8080 und 1883 zur Firewall-Ausnahmeliste hinzu. Die Ports werden für den Zugriff auf die Wyse Management Suite-Konsole und zum Senden der Push-Benachrichtigungen an die Thin Clients hinzugefügt.<br>• TCP 443 – HTTPS-Kommunikation<br>• TCP 1883 – MQTT-Kommunikation<br>• TCP 3306 – MariaDB (optional, wenn Remote)<br>• TCP 27017 – MongoDB (optional, wenn Remote)<br>• TCP 11211 – Memcache<br>• TCP 5172, 49159 – End-User Management Software Development Kit (EMSDK) – optional und nur für Teradici Geräte erforderlich<br>Die Standardschnittstellen, die vom Installationsprogramm verwendet werden, können im Rahmen der Installation zu einem alternativen Port geändert werden. | | | Das Wyse Management Suite Repository Installationsprogramm fügt die TCP-Ports 443 und 8080 zur Firewall-Ausnahmeliste hinzu. Die Ports werden für den Zugriff auf die Betriebssystem-Abbilder und Anwendungs-Abbilder hinzugefügt, die von der Wyse Management Suite verwaltet werden. |
| Unterstützte Browser | Internet Explorer Version 11<br>Google Chrome, Version 58.0 und höher<br>Mozilla Firefox, Version 52.0 und höher<br>Edge-Browser unter Windows – nur in englischer Sprache | | | |

- Die Installationsskripte für den Overlay Optimizer Version 1.0 werden mit dem Wyse Management Suite-Installationsprogramm mitgeliefert. Der Administrator muss die Skripte ausführen, damit der Overlay Optimizer in der Wyse Management Suite verfügbar gemacht werden kann.
- Die Installationsskripte für den Dell Secure Client Version 1.0 werden mit dem Wyse Management Suite-Installationsprogramm mitgeliefert. Der Administrator muss die Skripte ausführen, damit der Dell Secure Client in der Wyse Management Suite verfügbar gemacht werden kann.

**ANMERKUNG:** WMS.exe und WMS_Repo.exe müssen auf zwei verschiedenen Servern installiert werden. Sie müssen das Wyse Management Suite Remote-Repository für die Public Cloud installieren. Für eine Private Cloud müssen Sie zunächst das Wyse Management Suite Remote-Repository und das lokale Repository herunterladen. Die Software kann auf einer physischen oder einer virtuellen Maschine installiert werden. Es ist nicht notwendig, dass der Software-Repository- und der Wyse Management Suite-Server das gleiche Betriebssystem aufweisen.

**ANMERKUNG:** Für die Einrichtung von 10.000 Geräten sollte der Mindest-Arbeitsspeicher (RAM) 12 GB für die sichere MQTT-Kommunikation betragen.

**ANMERKUNG:** Ab Wyse Management Suite 3.3 wird empfohlen, MongoDB-Version 4.2.12 für verteilte Setups zu verwenden. Sie können Wyse Management Suite Version 3.3 nicht mit einer anderen Version des externe MongoDB Servers installieren oder aktualisieren.

**ANMERKUNG:** Die Wyse Management Suite Server- und Repository-Installation wird auf Cloud-gehosteten Servern wie Azure, Amazon Web Services und Google Cloud-Plattform nicht unterstützt.

# 3

# Installieren von Wyse Management Suite in Private Cloud

### Voraussetzungen

- Abrufen und konfigurieren Sie die komplette erforderliche Hardware und Software. Sie können die Wyse Management Suite-Software von downloads.dell.com/wyse/wms herunterladen.
- Installieren Sie ein unterstütztes Serverbetriebssystem auf einem oder mehreren Servern.
- Stellen Sie sicher, dass die Systeme mit den aktuellen Service Packs, Patches und Updates von Microsoft auf dem neuesten Stand sind.
- Stellen Sie sicher, dass die neueste Version des unterstützten Browsers installiert ist.
- Rufen Sie die Administratorrechte und Zugangsdaten auf allen Systemen ab, die für die Installationen benötigt werden.
- Fordern Sie für die Pro-Funktionen eine gültige Wyse Management Suite-Lizenz an. Die Standardedition erfordert keine Lizenz.
- Stellen Sie sicher, dass genügend Speicherplatz auf dem Laufwerk vorhanden ist, auf dem Wyse Management Suite installiert ist, und das lokale Repository konfiguriert ist.
- Wenn Sie Antiviren- oder andere Überwachungstools auf dem Wyse Management Suite-Setup installiert oder konfiguriert haben, empfiehlt Dell Technologies, die Tools vorübergehend zu deaktivieren, bis das Upgrade abgeschlossen ist. Sie können auch den entsprechenden Ausschluss zum Installationsverzeichnis, temporären Verzeichnis und lokalen Repository von Wyse Management Suite hinzufügen.

### Info über diese Aufgabe

Eine einfache Installation der Wyse Management Suite besteht aus den folgenden Komponenten:

- Wyse Management Suite-Server (umfasst Repository für Anwendung und Betriebssystemimages).
- Optional – Zusätzliche Wyse Management Suite-Repository-Server (Repository-Server (Repositorys für zusätzliche Images, Anwendungen und AD-Authentifizierung)
- Optional – HTTPS-Zertifikat von einer Zertifizierungsstelle wie www.geotrust.com/.

### Schritte

1. Doppelklicken Sie auf das Installationspaket.
2. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
   Die **EULA**-Details werden angezeigt.
   **ANMERKUNG:** Dieser Bildschirm wird nur auf Wyse Management Suite-Version 3.1 oder später angezeigt.
3. Lesen Sie die Lizenzvereinbarung.
4. Wählen Sie **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Setup-Typ** die gewünschten Komponenten aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.
   Die verfügbaren Optionen sind:
   - Wyse Management Suite – Es gibt zwei Setup-Typen, die für Wyse Management Suite Komponenten verfügbar sind.
     - Typisch – erfordert minimale Nutzerinteraktion und installiert eingebettete Datenbanken.
     - Nutzerdefiniert – erfordert maximale Nutzerinteraktion und wird für fortgeschrittene Nutzer empfohlen. Weitere Informationen finden Sie unter Nutzerdefinierte Installation.
   - Teradici EM SDK – Teradici EM SDK Komponenten sind als Dienst installiert.

   **ANMERKUNG:** Ein Meldungsfenster wird angezeigt, wenn die Internet Explorer Konfigurationsfunktion Erhöhte Sicherheit aktiviert ist. Um diese Funktion zu deaktivieren, wählen Sie das Kontrollkästchen **Verstärkte Sicherheitskonfiguration für IE ausschalten** auf der **Setup-Typ**-Seite aus.

   Wenn das EM SDK zusammen mit der Wyse Management Suite aus einer früheren Installation auf dem Server installiert ist, werden die Teradici EM SDK-Komponenten automatisch aktualisiert.
6. Wählen Sie **Typisch** als **Setup-Typ** aus.
7. Geben Sie die neuen **Datenbank-Zugangsdaten** für die integrierten Datenbanken und die neuen **Administrator-Zugangsdaten** ein und klicken Sie auf **Weiter**.

**ANMERKUNG:** Die Administrator-Zugangsdaten sind erforderlich, um sich nach der Installation in der Wyse Management Suite-Webkonsole anmelden zu können.

8. Führen Sie auf der Registerkarte **Konfiguration** Folgendes aus:
   a. Konfigurieren Sie den freigegebenen Ordner sowie die Zugangsberechtigungen für die CIFS-Nutzer. Die verfügbaren Optionen sind:
      - **Verwenden eines bestehenden Nutzers** – Wählen Sie diese Option aus, um die Zugangsdaten für den vorhandenen Nutzer zu validieren.
      - **Einen neuen Nutzer erstellen** – Wählen Sie diese Option aus und geben Sie die Zugangsdaten für einen neuen Nutzer ein.

        Das Kennwort muss mindestens acht Zeichen enthalten.

        **ANMERKUNG:** Wenn die Option **Teradici EM SDK** auf der Seite **Setup-Typ** aktiviert ist, können Sie den Port für den Teradici-Server auf der Seite **Konfiguration** konfigurieren.

   b. Klicken Sie auf **Weiter**.

      Es wird der Bildschirm **Servicekonto-Zugangsdaten** mit folgenden Optionen angezeigt:
      - **Einen neuen lokalen Nutzer erstellen** – Wählen Sie diese Option aus, um Anmeldeinformationen einzugeben und einen neuen lokalen Nutzer mit den geringsten Berechtigungen zu erstellen. Der neue Nutzer wird der Gruppe **Nutzer** hinzugefügt, aber der Nutzer verfügt nicht über Administratorrechte.

        **ANMERKUNG:** Der Nutzername, den Sie auf dem Bildschirm **Servicekonto-Anmeldeinformationen** eingeben, darf nicht mit Ihrem Teradici-Nutzernamen identisch sein. Der Nutzername muss zwischen 2 und 20 Zeichen enthalten. Ihr Kennwort muss 9 bis 127 Zeichen lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten. Leerzeichen sind im Kennwort nicht zulässig.
      - **Einen vorhandenen lokalen Nutzer verwenden** – Wählen Sie diese Option aus, um die Anmeldeinformationen eines vorhandenen lokalen Nutzers einzugeben. Wenn Sie diese Option auswählen, wird eine Meldung angezeigt. Stellen Sie sicher, dass der Nutzer bereits vorhanden ist, über Serviceanmeldungsrechte (**SeServiceLogonRight**) verfügt und sich mindestens einmal erfolgreich beim System angemeldet hat. Dell Technologies empfiehlt, sicherzustellen, dass der Nutzer keine Administratorrechte hat.

        **ANMERKUNG:** Wenn Sie diese Option auswählen, wird die Komplexität des Kennworts nicht überprüft und der Nutzername, den Sie eingeben, muss 2 bis 20 Zeichen lang sein.
      - **Einen vorhandenen Domainnutzer verwenden** – Wählen Sie diese Option aus, um die Anmeldeinformationen eines vorhandenen Domainnutzers einzugeben. Wenn Sie diese Option auswählen, wird eine Meldung angezeigt. Stellen Sie sicher, dass der Nutzer bereits in der Domain vorhanden ist, über Serviceanmeldungsrechte (**SeServiceLogonRight**) verfügt und sich mindestens einmal erfolgreich beim System angemeldet hat. Dell Technologies empfiehlt, sicherzustellen, dass der Nutzer keine Administratorrechte hat.

        **ANMERKUNG:** Wenn Sie diese Option auswählen, wird die Komplexität des Kennworts nicht überprüft.

   c. Klicken Sie auf **Weiter**, nachdem Sie die Anmeldeinformationen eingegeben haben.
      Der Bildschirm **Software-Vault-Zugangsdaten** wird angezeigt. Software-Vault wird verwendet, um sensible Daten zu speichern, die von der Dell Wyse Management Suite-Anwendung benötigt werden.
   d. Geben Sie das Kennwort für Software-Vault ein.
      Das Kennwort muss mindestens acht Zeichen enthalten.
   e. Klicken Sie auf **Weiter**.
9. Stellen Sie sicher, dass Sie alle entsprechenden Versionen von TLS basierend auf den Support-Kriterien der verwalteten Geräte auswählen.

   **ANMERKUNG:** Die WDA-Version niedriger als WDA_14.4.0.135_Unified, das Import-Tool und das 32-Bit-Merlin-Image sind nicht kompatibel mit TLSv1.1 und höher. Wählen Sie TLSv1.0 aus, wenn in der Wyse Management Suite Umgebung Geräte mit einer älteren Version von WDA, des Import-Tools oder von Geräten mit 32-Bit-Merlin-Image vorhanden sind.

10. Navigieren Sie zu dem Speicherort, an dem Sie die Software und das lokale Mandanten-Datei-Repository installieren möchten, und klicken Sie dann auf **Weiter**.

    Der Standardpfad des Zielordners für die Installation der Software ist `C:\Program Files\DELL\WMS`.
11. Klicken Sie auf **Weiter**.
    Die Seite **Vorinstallations-Zusammenfassung** wird angezeigt.
12. Klicken Sie auf **Weiter**, um die Software zu installieren.

    Das Installationsprogramm benötigt etwa 4 bis 5 Minuten, um die Installation abzuschließen. Es kann jedoch länger dauern, wenn abhängige Komponenten, wie VC-Runtime, nicht auf dem System installiert sind.
13. Klicken Sie zum Öffnen der Wyse Management Suite-Webkonsole auf **Starten**.
14. Klicken Sie auf der Webkonsole auf **Erste Schritte**.

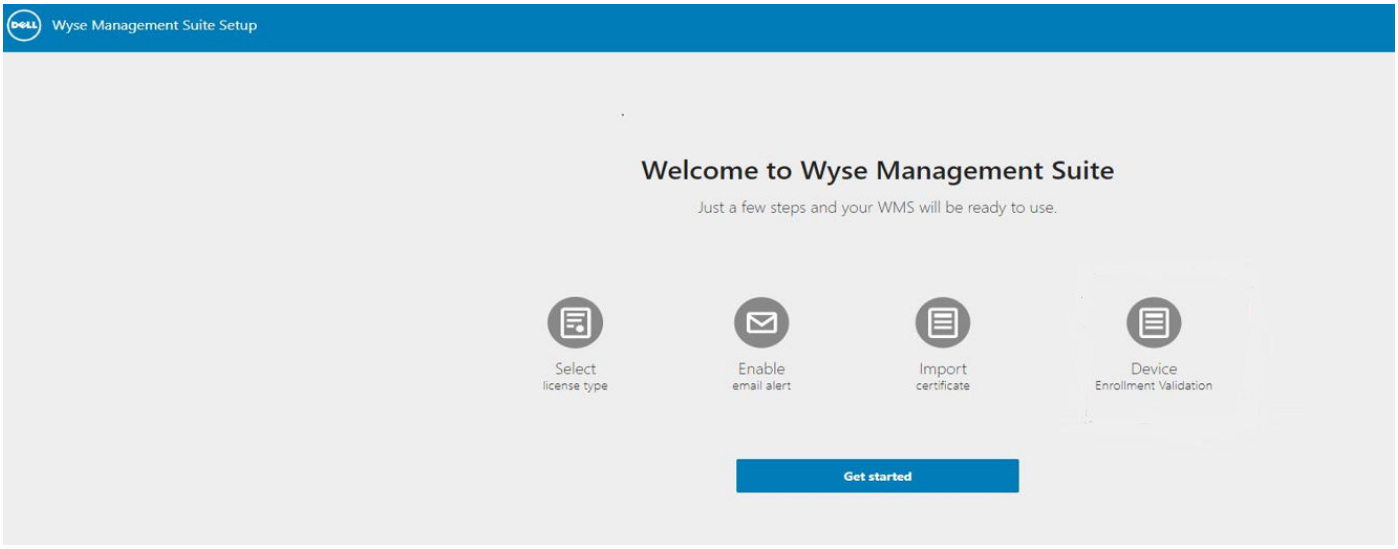


**Abbildung 1. Startseite**

15. Wählen Sie Ihre bevorzugte Lizenz aus.
    - Wenn Sie als Lizenztyp **Standard** auswählen, klicken Sie anschließend zum Fortfahren der Standard-Wyse Management Suite-Installation auf **Weiter**.
    - Wenn Sie als Lizenztyp **Pro**, auswählen, müssen Sie eine gültige Wyse Management Suite-Lizenz importieren. Importieren Sie die Wyse Management Suite-Lizenz, indem Sie die angeforderten Informationen zum Lizenzimport angeben, wenn Ihr Server über eine Internetverbindung verfügt. Sie können aber auch den Lizenzschlüssel generieren, indem sie sich beim Public-Cloud-Portal der Wyse Management Suite anmelden und den Schlüssel in das Feld „Lizenzschlüssel“ eingeben.

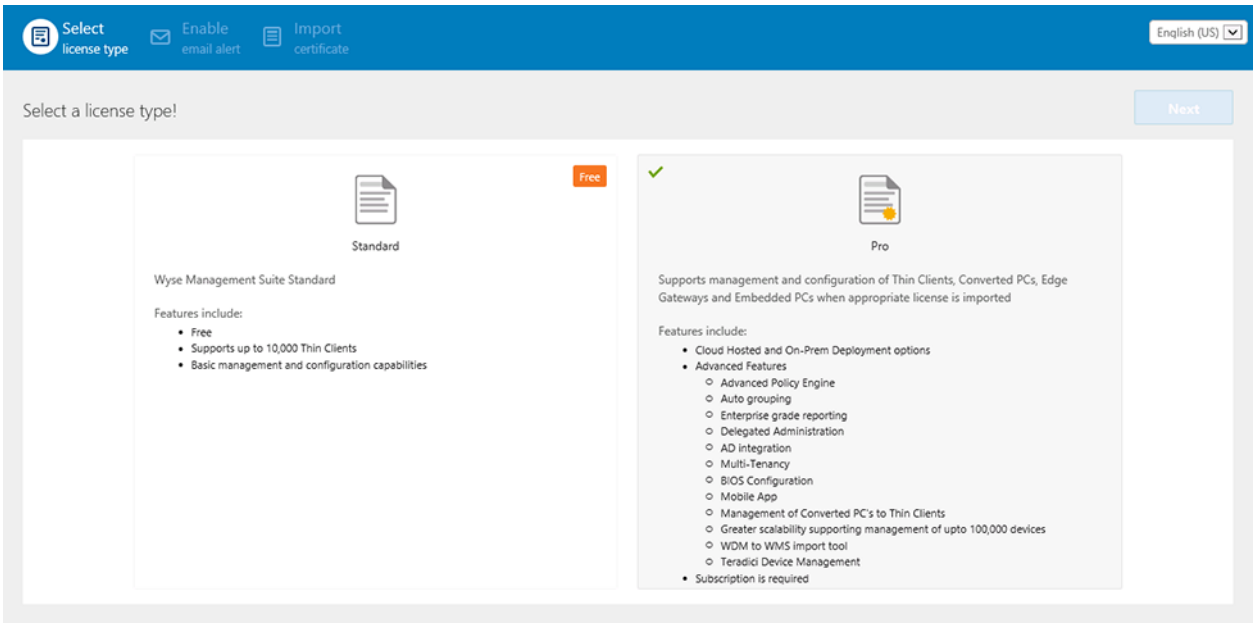


**Abbildung 2. Lizenztyp**

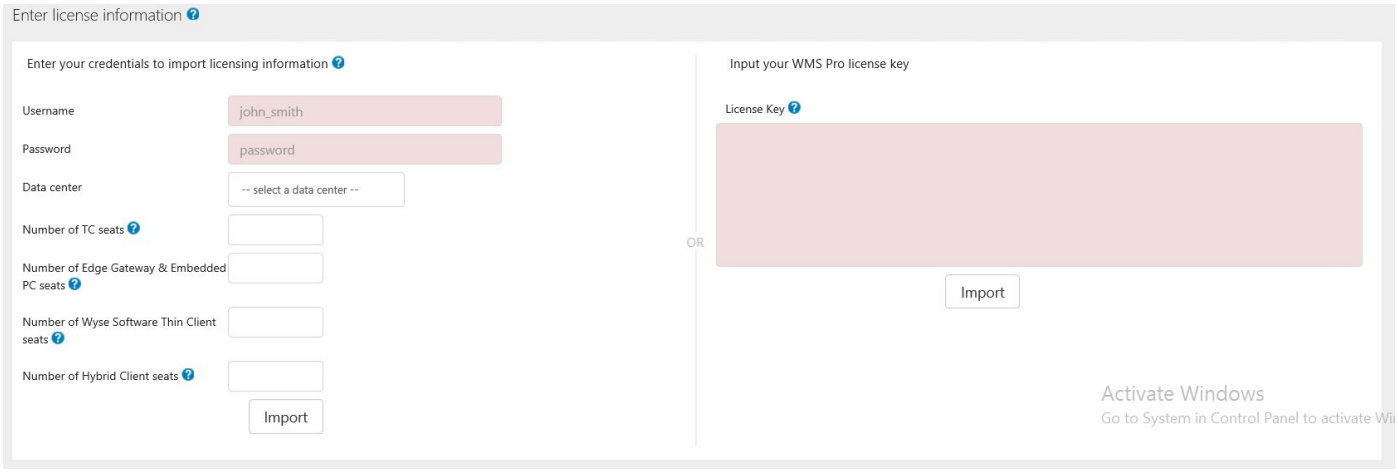


**Abbildung 3. Lizenzinformationen**

So exportieren Sie einen Lizenzschlüssel aus dem Wyse Management Suite-Cloud-Portal:

a. Melden Sie sich beim Wyse Management Suite-Cloud-Portal über einen der folgenden Links an:
   - US Data Center – us1.wysemanagementsuite.com/ccm-web
   - EU Data Center – eu1.wysemanagementsuite.com/ccm-web

b. Gehen Sie zu **Portalverwaltung** > **Abonnement**.

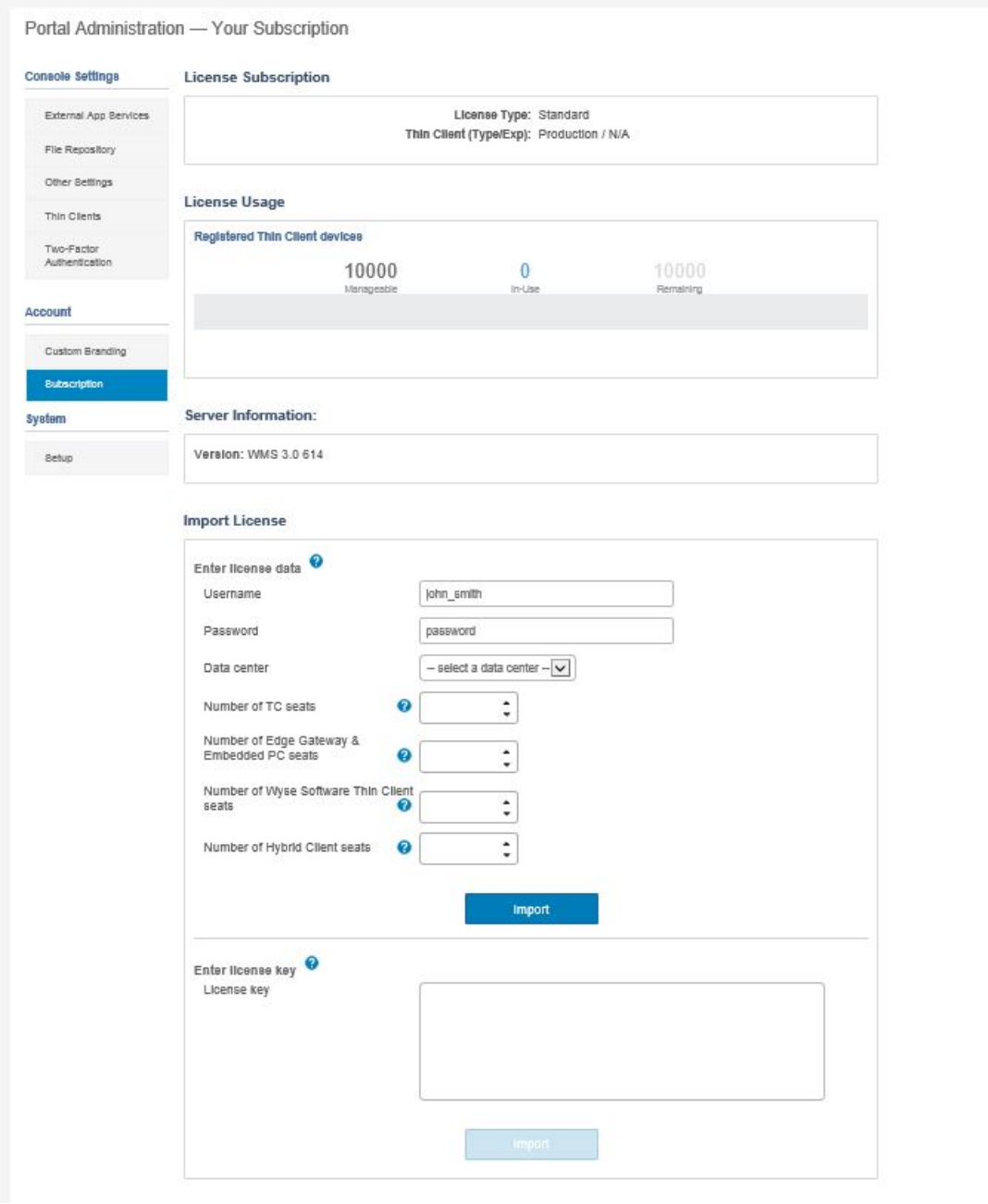


**Abbildung 4. Portalverwaltung**

c. Geben Sie die Anzahl der Thin Client Plätze an.

d. Klicken Sie auf **Exportieren**.

Wählen Sie zum Exportieren der Lizenz **WMS 1.1** oder **WMS 1.0** aus der Drop-down-Liste aus.

Die Seite "Zusammenfassung" zeigt die Details der Lizenz an, sobald die Lizenz erfolgreich importiert wurde.

16. Geben Sie Ihre SMTP-Serverinformationen ein und klicken Sie dann auf **Speichern**.

**ANMERKUNG:** Sie können diesen Bildschirm überspringen und Änderungen später in der Konsole vornehmen.

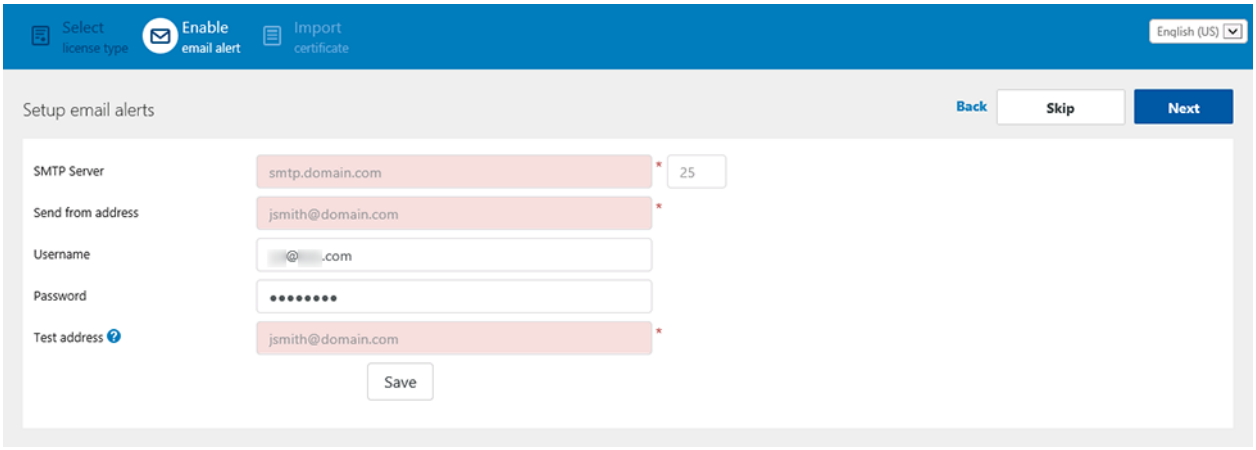


**Abbildung 5. E-Mail-Warnung**

**ANMERKUNG:** Sie müssen gültige SMTP-Serverinformationen für den Empfang von E-Mail-Benachrichtigungen von der Wyse Management Suite eingeben.

17. Importieren Sie Ihr SSL-Zertifikat, um die Kommunikation mit dem Wyse Management Suite-Server sicherzustellen. Geben Sie das öffentliche, private und Apache-Zertifikat ein und klicken Sie auf die Schaltfläche **Importieren**. Das Importieren des Zertifikats dauert drei Minuten bis die Konfiguration und der Neustart der Tomcat-Dienste abgeschlossen ist. Sie können diesen Bildschirm überspringen und dieses Setup bzw. Änderungen später in der Konsole ausführen, indem Sie sich bei der privaten Wyse Management Suite-Cloud anmelden und aus der **Portalverwaltung**-Seite importieren.

**ANMERKUNG:**

Standardmäßig importiert die Wyse Management Suite das selbstsignierte SSL-Zertifikat, das während der Installation für die sichere Kommunikation zwischen dem Client und dem Wyse Management Suite-Server erstellt wird. Wenn Sie für Ihren Wyse Management Suite-Server kein gültiges Zertifikat importieren, wird eine Sicherheitswarnmeldung angezeigt, wenn Sie die Wyse Management Suite von einer anderen Maschine als dem Server, auf dem sie installiert ist, aufrufen. Diese Warnmeldung wird angezeigt, weil das selbstsignierte Zertifikat während der Installation generiert wurde und nicht von einer Zertifizierungsstelle wie z. B. geotrust.com signiert wurde. Sie können entweder ein .pem oder .pfx-Zertifikat importieren.

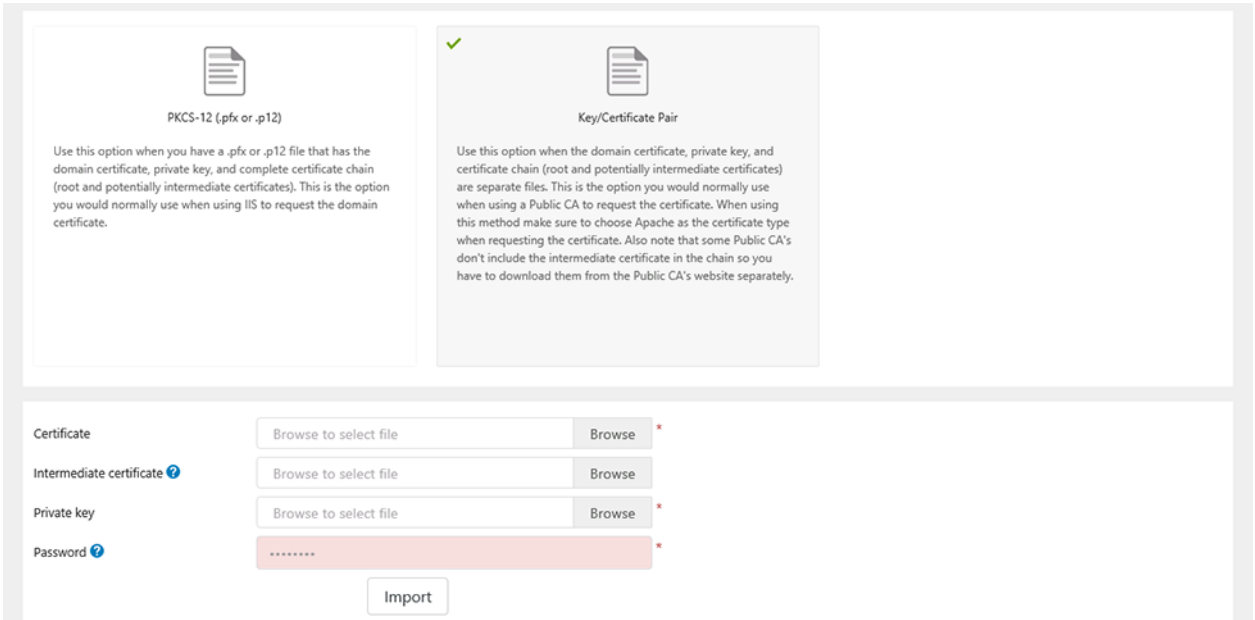


**Abbildung 6. Schlüssel- oder Zertifikatswertpaar**

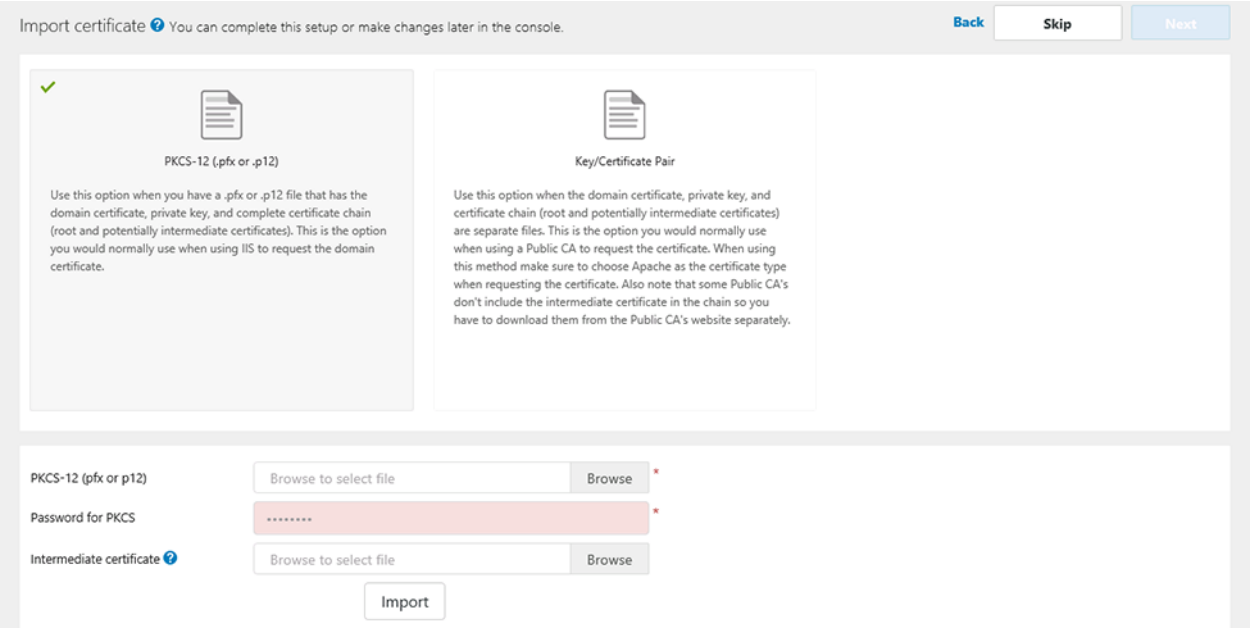


**Abbildung 7. PKCS-12**

18. Auf der Seite **Gerät** können Sie **Anmeldungsvalidierung** aktivieren, damit Administratoren die manuelle und automatische Registrierung von Thin Clients in einer Gruppe steuern können.

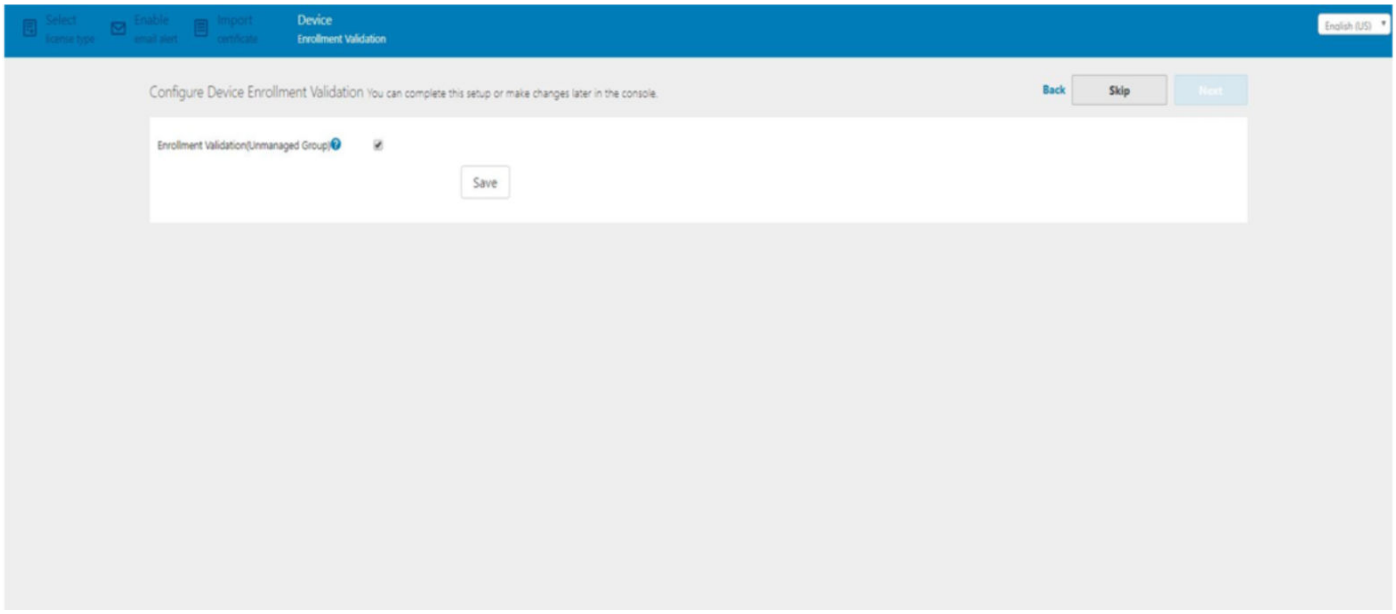


**Abbildung 8. Registrierungsvalidierung**

19. Klicken Sie auf **Speichern** und dann auf **Weiter**.
20. Klicken Sie auf **Bei WMS anmelden**.
    Die Anmeldeseite **Dell Management Portal** wird angezeigt.

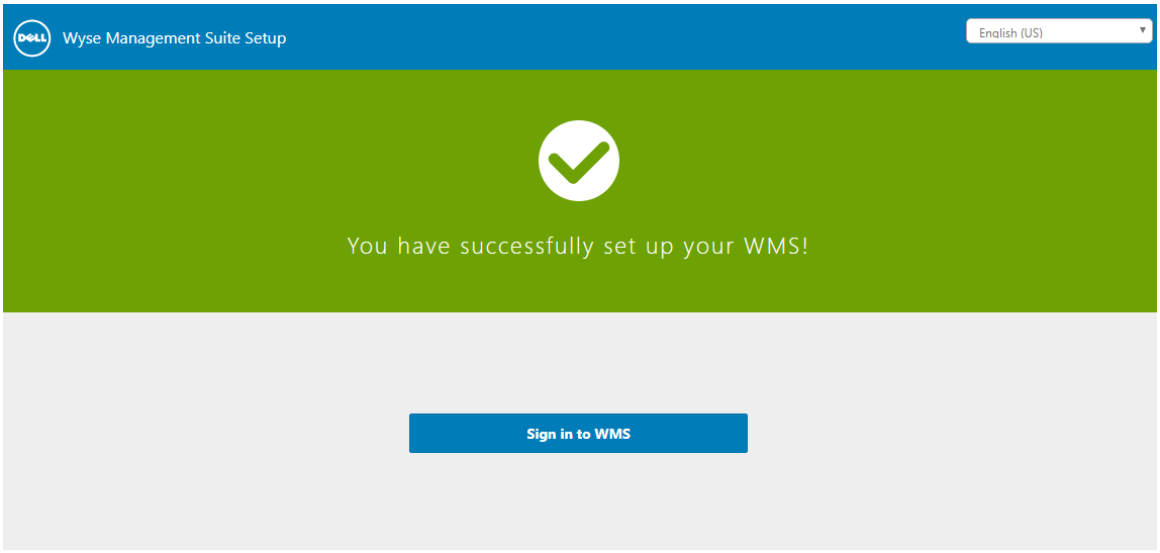


**Abbildung 9. Anmeldeseite**

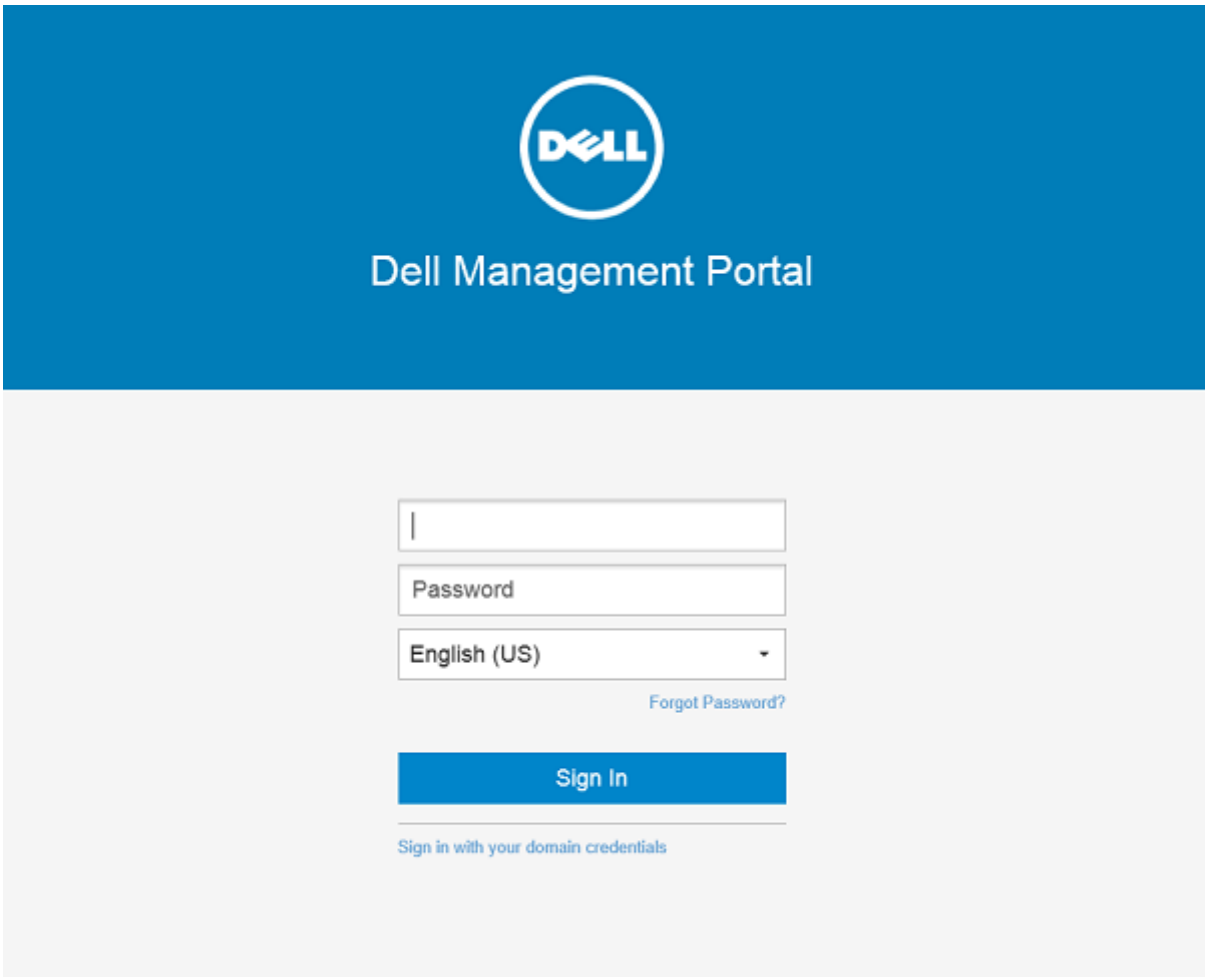


**Abbildung 10. Dell Management Portal**

**ANMERKUNG:** Lizenzen können über die Seite **Portalverwaltung** zu einem späteren Zeitpunkt aktualisiert oder erweitert werden.

**Themen:**

- Anmelden bei der Wyse Management Suite
- Funktionsbereiche der Verwaltungskonsole
- Konfigurieren und Verwalten von Thin Clients
- Erstellen von Richtliniengruppe und aktualisieren der Konfiguration
- Registrieren eines neuen Thin Clients

# Anmelden bei der Wyse Management Suite

**Info über diese Aufgabe**

So melden Sie sich bei der Verwaltungskonsole an:

**Schritte**

1. Wenn Sie Internet Explorer verwenden, deaktivieren Sie den **Internet Explorer erhöhte Sicherheit** und die Einstellungen für die **Kompatibilitätsansicht**.
2. Verwenden Sie einen unterstützten Webbrowser auf einer beliebigen Maschine mit Zugriff auf das Internet und greifen Sie auf die Private-Cloud-Edition der Wyse Management Suite über https://<FQDN>/ccm-web zu. Zum Beispiel https://wmsserver.domain.com/ccm-web, wobei wmsserver.domain.com der qualifizierte Domänennamen des Servers ist.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
4. Klicken Sie auf **Anmelden**.

# Funktionsbereiche der Verwaltungskonsole

Die Wyse Management Suite ist in die folgenden Funktionsbereiche organisiert:

**Info über diese Aufgabe**

- Die **Dashboard**-Seite enthält Informationen zu jedem Funktionsbereich des Systems.
- Die **Gruppen und Konfigurationen**-Seite nutzt eine hierarchische Gruppenrichtlinienverwaltung für die Gerätekonfiguration. Optional können Untergruppen der globalen Gruppenrichtlinien erstellt werden, um Geräte entsprechend den Unternehmensstandards zu kategorisieren. Beispielsweise können Geräte nach Berufsfunktion, Gerätetyp, BYOD usw. gruppiert werden.
- Die **Geräte**-Seite ermöglicht das Anzeigen und Verwalten von Geräten, Gerätetypen und gerätespezifischen Konfigurationen.
- Über die **Apps & Daten**-Seite können Geräteanwendungen, Betriebssystemimages, Richtlinien, Zertifikatdateien, Logos und Hintergrundbilder verwaltet werden.
- Die **Regeln**-Seite ermöglicht Ihnen das Hinzufügen, Bearbeiten und Aktivieren oder Deaktivieren von Regeln wie z. B. die automatische Gruppierung und Warnmeldungen.
- Die **Jobs**-Seite ermöglicht Ihnen das Erstellen von Jobs für Tasks z. B. Neustart, WOL und Anwendungs- oder Imagerichtlinien, die registrierten Geräten bereitgestellt werden müssen.
- Die **Ereignisse**-Seite ermöglicht das Anzeigen und Überprüfen von Systemereignissen und Warnungen.
- Die **Benutzer**-Seite ermöglicht lokalen Benutzern und aus dem Active Directory importierten Benutzern zum Anmelden bei der Wyse Management Suite Rollen als globaler Administrator, Gruppenadministrator und Viewer zugewiesen zu bekommen. Benutzer erhalten die Berechtigungen zum Ausführen von Vorgängen basierend auf den ihnen zugewiesenen Rollen.
- Die Seite **Portalverwaltung** ermöglicht Administratoren das Konfigurieren verschiedener Systemeinstellungen, wie die Konfiguration des lokalen Repositorys, das Lizenzabonnement, die Active Directory-Konfiguration und die Zweifaktor-Authentifizierung. Weitere Informationen finden Sie im *Administratorhandbuch zu Dell Wyse Management Suite* unter support.dell.com.

# Konfigurieren und Verwalten von Thin Clients

**Konfigurationsverwaltung** – Wyse Management Suite unterstützt eine Hierarchie von Gruppen und Untergruppen. Gruppen können manuell oder automatisch basierend auf vom Systemadministrator definierten Regeln erstellt werden. Sie können basierend auf den funktionalen Gruppen organisieren, zum Beispiel nach Marketing, Vertrieb und Entwicklung oder basierend auf der Standorthierarchie, z. B. Land, Bundesland und Stadt.

**ANMERKUNG:**

In der Pro-Edition können Systemadministratoren Regeln hinzufügen, um Gruppen zu erstellen. Sie können auch Geräte zu einer vorhandenen Gruppe zuordnen, je nach Gerätattributen wie Subnetz, Zeitzone und Standort.

Sie können auch Folgendes konfigurieren:

- Einstellungen oder Richtlinien, die für alle Geräte im Tenantkonto gelten und die in der Standardrichtliniengruppe festgelegt werden. Diese Einstellungen und Richtlinien sind der globale Parametersatz, der für alle Gruppen und Untergruppen gilt.
- Einstellungen oder Parameter, die in Gruppen auf niedrigeren Ebenen konfiguriert werden, haben vor den Einstellungen, die in übergeordneten oder Gruppen in höheren Ebenen konfiguriert wurden, Vorrang.
- Parameter, die spezifisch für ein bestimmtes Gerät sind und die über die Seite **Gerätedetails** konfiguriert werden können. Diese Parameter haben, wie auch untergeordnete Gruppen, Vorrang vor den Einstellungen, die in übergeordneten Gruppen konfiguriert wurden.

Konfigurationsparameter werden für alle Geräte in dieser Gruppe und alle Untergruppen bereitgestellt, wenn der Administrator die Richtlinie erstellt und veröffentlicht.

Sobald eine Konfiguration veröffentlicht und an das Gerät ausgegeben wurde, werden die Einstellungen so lange nicht erneut zu den Geräten gesendet, bis der Administrator eine Änderung vornimmt. Neue Geräte, die registriert sind, erhalten die Konfigurationsrichtlinie, die für die Gruppe gilt, für die sie registriert wurde. Dies umfasst die Parameter, die von der globalen Gruppe und den Gruppen auf mittleren Ebenen kommen.

Konfigurationsrichtlinien werden unmittelbar veröffentlicht und können nicht für einen späteren Zeitpunkt geplant werden. Einige Richtlinienänderungen, z. B. Anzeigeeinstellungen, erfordern möglicherweise einen Neustart.

**Anwendungs- und Betriebssystemimagebereitstellung** – Anwendungen und Betriebssystemimageupdates können über die Registerkarte **Apps & Daten** bereitgestellt werden. Anwendungen werden basierend auf den Richtliniengruppen bereitgestellt.

**ANMERKUNG:** Erweiterte Anwendungsrichtlinien ermöglichen das Bereitstellen einer Anwendung für die aktuellen und alle Untergruppen basierend auf Ihren Anforderungen. Betriebssystem-Images können nur für die aktuelle Gruppe bereitgestellt werden.

Wyse Management Suite unterstützt die Standard- und die erweiterten Anwendungsrichtlinien. Ein Standardanwendungsrichtlinie ermöglicht Ihnen die Installation eines einzigen Anwendungspakets. Sie müssen das Gerät vor und nach jeder Anwendungsinstallation neu starten. Bei einer erweiterten Anwendungsrichtlinie können mehrere Anwendungspakete mit nur zwei Neustarts installiert werden. Diese Funktion ist nur in der Pro-Edition verfügbar. Erweiterte Anwendungsrichtlinien unterstützen auch die Ausführung von Vor- und Nach-Installationsskripts, die möglicherweise zur Installation einer bestimmten Anwendung benötigt werden.

Sie können Standard- und erweiterte Anwendungsrichtlinien so konfigurieren, dass sie automatisch angewandt werden, wenn ein Gerät in der Wyse Management Suite registriert wird oder wenn ein Gerät in eine neue Gruppe verschoben wird.

Die Bereitstellung von Anwendungsrichtlinien und Betriebssystemimages für Thin Clients kann basierend auf der Zeitzone des Geräts oder anderen spezifischen Zeitzonen zur sofortigen oder späteren Ausführung geplant werden.

**Inventarisieren von Geräten** – Diese Option erscheint durch Klicken auf die Registerkarte **Geräte**. Standardmäßig zeigt diese Option zeigt eine paginierte Liste aller Geräte im System an. Der Administrator kann eine Teilmenge der Geräte mithilfe von verschiedenen Filterkriterien aufrufen, z. B. Gruppen oder Untergruppen, Gerätetypen, Art des Betriebssystems, Status, Subnetz und Plattform oder Zeitzone.

Um für dieses Gerät zur **Gerätedetails**-Seite zu navigieren, klicken Sie auf den Geräteeintrag, der auf dieser Seite aufgelistet ist. Alle Details für das Gerät werden angezeigt.

Die **Gerätedetails**-Seite zeigt auch alle Konfigurationsparameter, die für dieses Gerät gelten, sowie die Gruppenebene, auf der einzelne Parameter angewendet werden.

Diese Seite ermöglicht außerdem den Administratoren das Einstellen von Konfigurationsparametern, die sich speziell auf das Gerät beziehen, indem sie die Schaltfläche **Geräteausnahmen** aktiviert. Parameter, die in diesem Abschnitt konfiguriert sind, überschreiben jeden Parameter, der auf Gruppen- und/oder globaler Ebene konfiguriert wurde.

**Berichte** – Administratoren können vordefinierte Berichte auf der Grundlage der voreingestellten Filter erstellen und aufrufen. Klicken Sie zum Erzeugen von vordefinierten Berichten auf der Seite **Portalverwaltung** auf die Registerkarte **Berichte**.

**Mobile Anwendung** – Der Administrator kann Warnmeldungen erhalten und Geräte mit der mobilen Anwendung verwalten, die für Android-Geräte verfügbar ist. Klicken Sie zum Herunterladen der mobilen Anwendung und des Schnellstarthandbuchs auf der Seite **Portalverwaltung** auf die Registerkarte **Warnungen und Klassifizierung**.

# Erstellen von Richtliniengruppe und aktualisieren der Konfiguration

So erstellen Sie eine Richtlinie und aktualisieren die Konfiguration:

1. Melden Sie sich als Administrator an.
2. So erstellen Sie eine Richtliniengruppe:
   a. Wählen Sie **Gruppen und Konfigurationen** aus und klicken Sie auf die Schaltfläche **+** auf der linken Seite.
   b. Geben Sie den Gruppennamen und die Beschreibung an.
   c. Markieren Sie das Kontrollkästchen **Aktiviert**.
   d. Geben Sie das Gruppentoken ein.
   e. Klicken Sie auf **Speichern**.
3. So aktualisieren oder bearbeiten Sie eine Richtliniengruppe:
   a. Klicken Sie auf **Richtlinien bearbeiten** und wählen Sie das Betriebssystem aus, das die Richtlinie verwalten soll.
   b. Wählen Sie die zu ändernden Richtlinien aus und schließen Sie die Konfiguration ab.
   c. Klicken Sie auf **Speichern und Veröffentlichen**.

**ANMERKUNG:**
- Weitere Informationen zu den verschiedenen Konfigurationsrichtlinien, die von der Wyse Management Suite unterstützt werden, finden Sie im *Administratorhandbuch zu Dell Wyse Management Suite* unter support.dell.com.
- Sie können eine Regel zum automatischen Erstellen einer Gruppe und/oder Zuweisen eines Geräts zu einer Gruppe basierend auf bestimmten Attributen erstellen, z. B. Subnetz, Zeitzone und Standort.

# Registrieren eines neuen Thin Clients

**ANMERKUNG:** Weitere Informationen zur Sicherheitsumgebung für Kunden finden Sie unter Wyse-Geräte-Agent.

Ein Thin Client kann mit der Wyse Management Suite manuell über den Wyse Device Agent (WDA) registriert werden. Sie können einen Thin Client auch automatisch registrieren, indem Sie entsprechende Options-Tags auf dem DHCP-Server konfigurieren oder entsprechende DNS-SRV-Einträge auf dem DNS-Server konfigurieren.

Wenn Sie möchten, dass Geräte in unterschiedlichen Subnetzen automatisch in verschiedene Wyse Management Suite-Gruppen mit mehreren Subnetzen einchecken, verwenden Sie die DHCP-Option-Tags, um einen Thin Client zu registrieren. Beispielsweise können Geräte in TimeZone_A in ProfileGroup einchecken, die für TimeZoneA konfiguriert wurde.

Wenn Sie die Wyse Management Suite-Serverinformationen unter TLD eingeben möchten und wenn Sie die Wyse Management Suite Pro für die automatische Gruppenzuweisung basierend auf Geräteregeln installiert haben, verwenden Sie die DNS-SRV-Einträge auf dem DNS-Server, um einen Thin Client zu registrieren. Wenn zum Beispiel das Gerät über TimeZoneA eincheckt, weisen Sie es der für TimeZoneA konfigurierten ProfileGroup zu.

Für die Wyse Management Suite auf einer privaten Cloud mit selbstsignierten Zertifikaten müssen die Thin Clients die folgenden Versionen von Wyse Geräte-Agenten oder die Firmware für die sichere Kommunikation installiert haben:

- Windows Embedded Systems – 13.0 oder spätere Versionen
- Thin Linux – 2.0.24 oder spätere Versionen
- ThinOS – 8.4 Firmware oder spätere Versionen
- Sie können ein Gerät mit einer älteren Agentenversion über HTTP-URL anstatt HTTPS registrieren. Nachdem der Agent oder die Firmware auf die neueste Version aktualisiert wurde, wird die Kommunikation mit der Wyse Management Suite automatisch auf HTTPS geschaltet.
- Sie können die neueste Version von WDA hier herunterladen: downloads.dell.com/wyse/wda.
- Gehen Sie für die auf einer privaten Cloud installierten Wyse Management Suite zu **Administration-Portal** > **Setup** und wählen Sie das Kontrollkästchen **Zertifikatvalidierung** aus, wenn Sie Zertifikate von einer Zertifizierungsstelle wie www.geotrust.com importiert haben. Dieses Kontrollkästchen sollte nicht ausgewählt werden, wenn Sie Zertifikate nicht von einer bekannten Zertifizierungsstelle

importiert haben. Diese Option ist nicht für Wyse Management Suite in einer öffentlichen Cloud verfügbar, da die Zertifikatsvalidierung in der öffentlichen Cloud immer aktiviert ist.

# ThinOS Gerät manuell registrieren

So registrieren Sie ThinOS Geräte manuell:

### Schritte

1. Klicken Sie auf dem Desktopmenü auf **System-Setup Zentrale Konfiguration**.
   Das Fenster **Zentrale-Konfiguration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **WDA**.

   **WMS** ist standardmäßig ausgewählt.

   **ANMERKUNG:** Der WDA-Dienst wird automatisch ausgeführt, sobald der Client-Startprozess abgeschlossen ist.

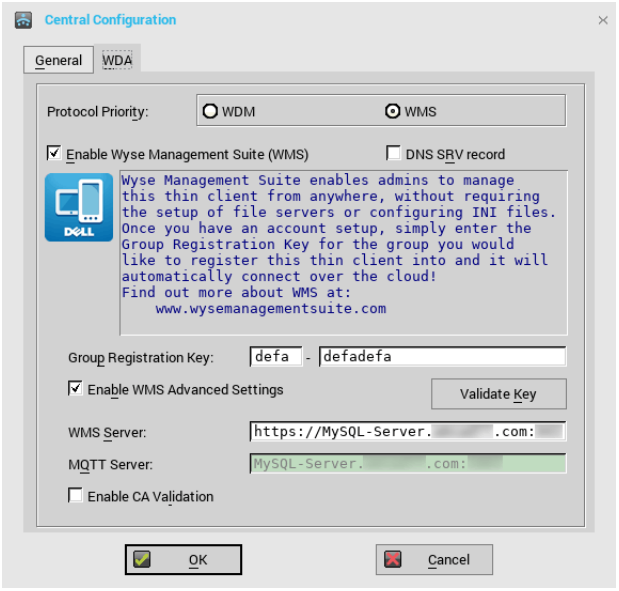


**Abbildung 11. Zentrale Konfiguration**

3. Wählen Sie das Kontrollkästchen **Wyse Management Suite aktivieren** zum Aktivieren der Wyse Management Suite aus.
4. Geben Sie den für die gewünschte Gruppe von Ihrem Administrator konfigurierten **Gruppenregistrierungsschlüssel** ein.
5. Wählen Sie die Option **Erweiterte WMS-Einstellungen aktivieren** aus und geben Sie die Details für den WMS-Server oder MQTT-Server ein.
6. Aktivieren oder deaktivieren Sie die CA-Validierung je nach Ihrem Lizenztyp – öffentliche Cloud oder private Cloud.
   - Öffentliche Cloud – Wählen Sie das Kontrollkästchen **CA-Validierung aktivieren** aus, wenn das Gerät in der öffentlichen Cloud in der Wyse Management Suite registriert ist.
   - Private Cloud – Wählen Sie das Kontrollkästchen **CA-Validierung aktivieren** aus, wenn Sie Zertifikate von einer bekannten Zertifizierungsstelle in Ihren Wyse Management Suite-Server importiert haben.

   **ANMERKUNG:**

   Nehmen Sie an der Pro-Cloud-Version von Wyse Management Suite in den USA keine Änderungen an den Standarddetails des WMS-Servers und MQTT-Servers vor. Verwenden Sie für die Pro-Cloud-Version von Wyse Management Suite in Europa Folgendes:
   - CCM-Server – eu1.wysemanagementsuite.com
   - MQTT-Server – *eu1-pns.wysemanagementsuite.com:1883*
7. Klicken Sie auf **Schlüssel validieren**, um das Setup zu überprüfen. Das Gerät startet automatisch neu, nachdem der Schlüssel validiert wurde.

**ANMERKUNG:** Wenn der Schlüssel nicht validiert wird, überprüfen Sie die Anmeldeinformationen, die Sie angegeben haben. Stellen Sie sicher, dass Port 443 und Port 1883 nicht durch das Netzwerk blockiert sind.

8. Klicken Sie auf **OK**.
   Das Gerät wird in der Wyse Management Suite-Konsole registriert.

**Nächste Schritte**

Informationen zum Registrieren von Windows Embedded Standard Geräten und Linux Geräten finden Sie in Windows Embedded Standard-Gerät manuell registrieren und Linux Gerät manuell registrieren.

## Registrieren von ThinOS-Geräten unter Verwendung von INI-Dateien

Wenn Sie die ThinOS-Geräte mithilfe von wnos.ini, oder xen.ini konfigurieren möchten, können die zusätzlichen Informationen in den .ini-Dateien veröffentlicht werden, um die Geräte darüber zu informieren, bei einem Wyse Management Suite-Server einzuchecken.

Beispiele:

- Beispiel für ThinOS 8.5:

  WDAService=yes \

  Priority=WMS

  WMSEnable=yes \

  Server=<Server-URL> \

  CAValidation=no \

  Override=yes

- Beispiel für ThinOS 8.4:

  WDAService=yes \

  Priority=CCM

  CCMEnable=yes \

  CCMServer=<Server-URL> \

  GroupPrefix=< Präfix > \

  GroupKey=< Schlüssel > \

  MQTTServer=<Server-URL> \

  Override=yes \

  CAValidation=no

Weitere Informationen finden Sie im neuesten *Dell Wyse ThinOS INI-Handbuch* unter support.dell.com.

**ANMERKUNG:**

- Bei ThinOS 8.3 (ThinOS Lite 2.3 ) und neueren Versionen ermöglicht Ihnen ein `WDA-Dienstpriorität`-Befehl die Angabe eines Verwaltungsprotokolls. Dieser Befehl wird zur Ermittlung des Verwaltungsservers verwendet.
- Die CCM-Tags für ThinOS Versionen 8.3, 8.4 und 8.5 sind unterschiedlich.

## Registering devices by using DHCP option tags

**ANMERKUNG:**

- Ausführliche Informationen zum Hinzufügen von DHCP-Option-Tags auf dem Windows Server finden Sie unter Erstellen und Konfigurieren von DHCP-Options-Tags. Weitere Informationen über die Sicherheitsumgebung für Kunden finden Sie unter Wyse-Geräte-Agent.

Sie können Geräte mithilfe der folgenden DHCP-Options-Tags registrieren:

**Tabelle 5. Registrieren von Geräten mithilfe von DHCP-Options-Tags**

| Options-Tag | Beschreibung |
|---|---|
| **Name** – WMS<br>**Datentyp** – Zeichenfolge<br>**Code** – 165<br>**Beschreibung** – WMS-Server-FQDN | Dieses Tag verweist auf die Wyse Management Suite-Server-URL. Beispiel: `wmsserver.acme.com:443`, wobei wmsserver.acme.com der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist. Links zum Registrieren Ihrer Geräte in der Wyse Management Suite in einer öffentlichen Cloud finden Sie unter Erste Schritte mit der Wyse Management Suite in einer öffentlichen Cloud.<br>**ANMERKUNG:** Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird. Verwenden Sie https://, wenn Sie das ThinOS 9.x Gerät nicht für Wyse Management Suite registrieren können. |
| **Name** – MQTT<br>**Datentyp** – Zeichenfolge<br>**Code** – 166<br>**Beschreibung** – MQTT-Server | Dieses Tag leitet das Gerät zum Wyse Management Suite-Pushbenachrichtigungsserver (PNS) weiter. Bei einer Installation in einer privaten Cloud wird das Gerät an den MQTT-Dienst auf dem Wyse Management Suite-Server weitergeleitet. Beispiel: `wmsservername.domain.com:1883`.<br>Zum Registrieren Ihrer Geräte in der öffentlichen Cloud der Wyse Management Suite sollte das Gerät auf die PNS-(MQTT-)Server in der öffentlichen Cloud verweisen. Beispiel:<br>US1:us1-pns.wysemanagementsuite.com<br>EU1:eu1-pns.wysemanagementsuite.com<br>Sie müssen die MQTT-Serverdetails eingeben, wenn Sie Wyse Agent-Details in der älteren Version von ThinOS und Windows eingebetteten Geräten konfigurieren. MQTT ist eine Komponente von WMS, die erforderlich ist, um die Thin Clients zu benachrichtigen. Die URLs – mit und ohne MQTT-Details – müssen zur Zulassungsliste in der Wyse Management Suite Public-Cloud-Umgebung hinzugefügt werden.<br>**ANMERKUNG:** Sie können die MQTT-URLs nicht verwenden, um sich bei Wyse Management Suite anzumelden. |
| **Name** – CA-Validation<br>**Datentyp** – Zeichenfolge<br>**Code** – 167<br>**Beschreibung** – Zertifizierungsstellenprüfung | Dieses Tag ist erforderlich, wenn die Wyse Management Suite auf Ihrem System in Ihrer privaten Cloud installiert ist. Fügen Sie dieses optionale Tag nicht hinzu, wenn Sie die Registrierung Ihrer Geräte bei der Wyse Management Suite in einer öffentlichen Cloud vornehmen.<br>Geben Sie **Wahr** ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server von einer bekannten Zertifizierungsstelle importiert haben.<br>Geben Sie **Falsch** ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server nicht von einer bekannten Zertifizierungsstelle importiert haben. |
| **Name** – GroupToken<br>**Datentyp** – Zeichenfolge<br>**Code** – 199<br>**Beschreibung** – Gruppentoken | Dieser Tag ist erforderlich, um ThinOS-Geräte in der Wyse Management Suite in einer öffentlichen oder privaten Cloud zu registrieren.<br>Dieser Tag ist optional zum Registrieren des Windows Embedded Standard oder von ThinLinux-Geräten in der Wyse Management Suite in einer privaten Cloud. Wenn der Tag nicht verfügbar ist, werden die Geräte während der Installation vor Ort automatisch in der unverwalteten Gruppe registriert. |

# Geräte mit DNS-SRV-Eintrag registrieren

**ANMERKUNG:** Weitere Informationen über die Sicherheitsumgebung für Kunden finden Sie unter Wyse-Geräte-Agent.

DNS-basierte Geräteregistrierung wird von den folgenden Versionen des Wyse Geräte-Agenten unterstützt:

- Windows Embedded Systems – 13.0 oder spätere Versionen

- Thin Linux – 2.0.24 oder spätere Versionen
- ThinOS – 8.4 Firmware oder spätere Versionen

Sie können Geräte mit dem Wyse Management Suite-Server registrieren, falls für die DNS-SRV-Eintragsfelder gültige Werte eingegeben wurden.

**ANMERKUNG:** Ausführliche Informationen zum Hinzufügen von DNS-SRV-Einträgen im Windows Server finden Sie unter Erstellen und Konfigurieren eines DNS-SRV-Eintrags.

Die folgende Tabelle listet die gültigen Werte für die DNS-SRV-Einträge auf:

### Tabelle 6. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags

| URL/Tag | Beschreibung |
|---|---|
| **Eintragsname** – _WMS_MGMT<br>**Eintrags-FQDN** – _WMS_MGMT._tcp.<Domänenname><br>**Eintragstyp** – SRV | Dieser Eintrag verweist auf die Wyse Management Suite Server-URL. Beispiel: `wmsserver.acme.com:443`, wobei wmsserver.acme.com der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist. Links zum Registrieren Ihrer Geräte in der Wyse Management Suite in einer öffentlichen Cloud finden Sie unter Erste Schritte mit der Wyse Management Suite in einer öffentlichen Cloud.<br>**ANMERKUNG:** Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird. Verwenden Sie https://, wenn Sie das ThinOS 9.x Gerät nicht für Wyse Management Suite registrieren können. |
| **Eintragsname** – _WMS_MQTT<br>**Eintrags-FQDN** – _WMS_MQTT._tcp.<Domänenname><br>**Eintragstyp** – SRV | Dieser Eintrag leitet das Gerät zum Wyse Management Suite-Pushbenachrichtigungsserver (PNS) weiter. Bei einer Installation in einer privaten Cloud wird das Gerät an den MQTT-Dienst auf dem Wyse Management Suite-Server weitergeleitet. Beispiel: `wmsservername.domain.com:1883`.<br>**ANMERKUNG:** MQTT ist bei der neuesten Version der Wyse Management Suite optional.<br>Zum Registrieren Ihrer Geräte in der öffentlichen Cloud der Wyse Management Suite sollte das Gerät auf die PNS-(MQTT-)Server in der öffentlichen Cloud verweisen. Beispiel:<br>US1 –us1-pns.wysemanagementsuite.com<br>EU1 –eu1-pns.wysemanagementsuite.com<br>Sie müssen die MQTT-Serverdetails eingeben, wenn Sie Wyse Agent-Details in der älteren Version von ThinOS und Windows eingebetteten Geräten konfigurieren. MQTT ist eine Komponente von WMS, die erforderlich ist, um die Thin Clients zu benachrichtigen. Die URLs – mit und ohne MQTT-Details – müssen zur Zulassungsliste in der Wyse Management Suite Public-Cloud-Umgebung hinzugefügt werden.<br>**ANMERKUNG:** Sie können die MQTT-URLs nicht verwenden, um sich bei Wyse Management Suite anzumelden. |
| **Eintragsname** –_WMS_GROUPTOKEN<br>**Eintrags-FQDN** – _WMS_GROUPTOKEN.<Domain><br>**Eintragstyp** – TEXT | Dieser Datensatz ist erforderlich, um ThinOS-Geräte in der Wyse Management Suite in einer öffentlichen oder privaten Cloud zu registrieren.<br>Dieser Datensatz ist optional zum Registrieren des Windows Embedded Standard oder von ThinLinux-Geräten in der Wyse Management Suite in einer privaten Cloud. Wenn der Eintrag nicht verfügbar ist, werden die Geräte während der Installation vor Ort automatisch in der unverwalteten Gruppe registriert. |

**Tabelle 6. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags (fortgesetzt)**

| URL/Tag | Beschreibung |
|---|---|
| | **ANMERKUNG:** Das Gruppentoken ist optional für die neueste Version von Wyse Management Suite in einer privaten Cloud. |
| **Eintragsname** – _WMS_CAVALIDATION<br>**Eintrags-FQDN** – _WMS_CAVALIDATION.<Domain><br>**Eintragstyp** – TEXT | Dieser Eintrag ist erforderlich, wenn die Wyse Management Suite auf Ihrem System in Ihrer privaten Cloud installiert ist. Fügen Sie diesen optionalen Eintrag nicht hinzu, wenn Sie die Registrierung Ihrer Geräte bei der Wyse Management Suite in einer öffentlichen Cloud vornehmen.<br>Geben Sie **Wahr** ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server von einer bekannten Zertifizierungsstelle importiert haben.<br>Geben Sie **Falsch** ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server nicht von einer bekannten Zertifizierungsstelle importiert haben.<br>**ANMERKUNG:** CA Validation ist bei der neuesten Version der Wyse Management Suite optional. |

# Registrieren von Geräten mithilfe sicherer DNS-Datensatzfelder oder sicherer DHCP-Bereichsoptionen

Ab Wyse Management Suite 3.5 können Sie Geräte mithilfe sicherer DNS-Datensatzfelder oder DHCP-Bereichsoptionen registrieren.

### Info über diese Aufgabe

Sie können Geräte mit dem Wyse Management Suite-Server registrieren, falls die DNS-Eintragsfelder oder DHCP-Scope-Optionen anhand der folgenden Werte festgelegt wurden:

- DNS-SRV-Eintragsfelder:
  - _WMS_MGMTV2
  - _WMS_GROUPTOKENV2
- DHCP Scope-Optionen:
  - WMS-URL - 201
  - Gruppentoken – 202

### Schritte

1. Navigieren Sie zu **Portalverwaltung** > **Konsoleneinstellungen** > **WMS-Ermittlung**.
2. Geben Sie das Gruppentoken ein.
3. Wählen Sie den Ermittlungstyp aus der Drop-down-Liste **Ermittlungstyp** aus.
4. Klicken Sie auf **Details generieren**.
   Die verschlüsselten WMS-URL-Details und das Gruppentoken werden angezeigt.
   **ANMERKUNG:** Wenn das Wyse Management Suite-Zertifikat geändert wird, müssen der sichere DNS- und DHCP-Code neu erstellt werden, um ein neues Gerät zu registrieren.

# 4

# Bereitstellen von Anwendungen auf Thin Clients

Die Standardanwendungsrichtlinie ermöglicht die Installation eines einzigen Anwendungspakets und erfordert einen Neustart vor und nach der Installation jeder Anwendung. Mithilfe der erweiterten Anwendungsrichtlinie können Sie mehrere Anwendungspakete mit nur zwei Neustarts installieren. Die erweiterte Anwendungsrichtlinie unterstützt auch die Ausführung von Installationsskripts vor und nach der Installation, die Sie möglicherweise zur Installation einer bestimmten Anwendung benötigen. Weitere Informationen finden Sie in Anhang B.

**Themen:**



## Hochladen und Bereitstellen von ThinOS-Firmware-Image-Beständen

So fügen Sie eine Datei zum ThinOS-Image-Bestand hinzu:

**Schritte**

1. Klicken Sie in der Registerkarte **Apps & Daten** unter **OS-Abbild-Repository** auf **ThinOS**.
2. Klicken Sie auf **Firmware-Datei hinzufügen**.
   Der Bildschirm **Datei hinzufügen** wird angezeigt.
3. Um eine Datei auszuwählen, klicken Sie auf **Durchsuchen** und wechseln Sie zum Speicherort, an dem sich die Datei befindet.
4. Geben Sie die Beschreibung für Ihre Datei ein.
5. Wählen Sie das Kontrollkästchen aus, wenn Sie eine vorhandene Datei überschreiben möchten.
6. Klicken Sie auf **Hochladen**.

   **ANMERKUNG:** Die Datei wird zum Repository hinzugefügt, wenn Sie das Kontrollkästchen auswählen. Sie ist jedoch keiner Gruppe und keinem Gerät zugewiesen. Gehen Sie, um die Datei zuzuweisen, zu der entsprechenden Gerätekonfigurationsseite.

## Erstellen und Bereitstellen von Standardanwendungsrichtlinie für Thin Clients

So stellen Sie Thin Clients eine Standardanwendungsrichtlinie zur Verfügung:

1. Gehen Sie im lokalen Repository zu **thinClientApps** und kopieren Sie die Anwendung in den Ordner.
2. Stellen Sie sicher, dass die Anwendung registriert ist, indem Sie zu **Apps & Daten** navigieren und **Thin Client** unter **App-Bestand** auswählen.

   **ANMERKUNG:** Die App-Bestand-Benutzeroberfläche benötigt etwa zwei Minuten, um alle kürzlich hinzugefügten Programme zu generieren.
3. Klicken Sie in den **App-Richtlinien** auf **Thin Client**.
4. Klicken Sie auf **Richtlinie hinzufügen**.
5. Geben Sie zum Erstellen einer Anwendungsrichtlinie die entsprechenden Informationen in das Fenster **Standard-App-Richtlinie hinzufügen** ein.
   a. Wählen Sie **Richtlinienname**, **Gruppe**, **Task**, **Gerätetyp** und **TC-Anwendung** aus.

b. Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.

   Zeitüberschreitung zeigt eine Meldung auf dem Client an, die Ihnen vor der Installation Zeit zum Speichern der Änderungen verschafft. Geben Sie an, wie viele Minuten lang das Meldungsdialogfeld auf dem Client angezeigt werden soll.

c. Um diese Richtlinie automatisch auf einem Gerät anzuwenden, das in der Wyse Management Suite registriert ist, wählen Sie **Richtlinie auf neue Geräte anwenden** aus der Dropdownliste **Richtlinie automatisch anwenden** aus.

**ANMERKUNG:**

- Die App-Richtlinie wird angewendet, wenn ein beliebiges Gerät in die definierte Gruppe verschoben oder direkt in der Gruppe registriert wird.
- Wenn Sie **Richtlinie beim Check-In-Vorgang auf Geräte anwenden** auswählen wird die Richtlinie automatisch beim Einchecken in den Wyse Management Suite-Server auf das Gerät angewendet.

6. Um eine Verzögerung bei der Ausführung der Richtlinie zuzulassen, markieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Dropdownmenüs aktiviert:
   - Wählen Sie aus dem Dropdownmenü **Max. Anzahl an Stunden pro Verzögerung** die maximale Anzahl an Stunden aus (1 bis 24 Stunden), für die die Richtlinienausführung verzögert werden kann.
   - Wählen Sie aus dem Dropdownmenü **Max. Verzögerungen** die maximale Anzahl an Stunden aus (1 bis 3 Stunden), für die die Richtlinienausführung verzögert werden kann.
7. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an.
8. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.

   Eine Meldung wird angezeigt, um den Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu gewähren.
9. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.

   Die App/Image-Richtlinienjob kann dann ausgeführt werden:

   a. **Sofort** – Der Server führt den Job sofort aus.

   b. **Nach Zeitzone des Geräts** – Der Server erstellt einen Job für jede Gerätezeitzone und plant den Job für das ausgewählte Datum bzw. die Uhrzeit der Zeitzone des Geräts.

   c. **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.
10. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
11. Sie können den Status des Jobs durch Navigation zur Seite **Jobs** überprüfen.

# 5

# Upgrade der Wyse Management Suite von Version 2.x auf 3.x

**Voraussetzungen**

- Stellen Sie sicher, dass genügend Speicherplatz auf dem Laufwerk vorhanden ist, auf dem Wyse Management Suite installiert ist, und das lokale Repository konfiguriert ist.
- Wenn Sie Antiviren- oder andere Überwachungstools auf dem Wyse Management Suite-Setup installiert oder konfiguriert haben, empfiehlt Dell Technologies, die Tools vorübergehend zu deaktivieren, bis das Upgrade abgeschlossen ist. Sie können auch einen entsprechenden Ausschluss zum Installationsverzeichnis, temporären Verzeichnis und lokalen Repository von Wyse Management Suite hinzufügen.

**Schritte**

1. Doppelklicken Sie auf das Installationspaket der Wyse Management Suite 3.x.
2. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
   Die EULA-Details werden angezeigt.
   **ANMERKUNG:** Dieser Bildschirm wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite 3.0 auf 3.x durchführen.
3. Lesen Sie die Lizenzvereinbarung.
4. Wählen Sie **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie anschließend auf **Weiter**.
5. Auf der Seite **Upgrade** konfigurieren Sie den freigegebenen Ordner sowie die Zugangsberechtigungen für die CIFS-Benutzer. Die verfügbaren Optionen sind:
   - Verwenden eines vorhandenen Benutzers – Wählen Sie diese Option aus, um die Anmeldeinformationen für den vorhandenen Benutzer zu validieren.
   - Einen neuen Benutzer erstellen – Wählen Sie diese Option aus und geben Sie die Anmeldeinformationen für einen neuen Benutzer ein.

   **ANMERKUNG:** Wenn das EM SDK während der vorherigen Installation der Wyse Management Suite auf dem Server installiert wurde, werden die Teradici EM SDK-Komponenten automatisch aktualisiert. Wenn das EM SDK während der vorherigen Installation nicht auf dem Gerät installiert wurde, aktivieren Sie das Kontrollkästchen "Teradici EM SDK", um die Teradici EM SDK-Komponenten zu installieren und konfigurieren.

   **ANMERKUNG:** Sie können das Teradici EM SDK auch mit dem Wyse Management Suite-Installationsprogramm installieren und aktualisieren.
6. Aktivieren Sie das Kontrollkästchen **Bind memcached to 127.0.0.1**, um den memcache an den lokalen Server (127.0.0.1) zu binden. Wenn dieses Kontrollkästchen nicht markiert ist, wird Memcache an FQDN **gebunden**.
7. Wählen Sie alle entsprechenden Versionen von TLS basierend auf den Supportkriterien der gemanagten Geräte aus.

   **ANMERKUNG:** Die WDA-Version niedriger als WDA_14.4.0.135_Unified, das Import-Tool und das 32-Bit-Merlin-Image sind nicht kompatibel mit TLSv1.1 und höher. Wählen Sie TLSv1.0 aus, wenn in der Wyse Management Suite Umgebung Geräte mit einer älteren Version von WDA, des Import-Tools oder von Geräten mit 32-Bit-Merlin-Image vorhanden sind.
8. Klicken Sie zum Öffnen der Wyse Management Suite-Webkonsole auf **Starten**.

# 6

# Upgrade der Wyse Management Suite von Version 3.x auf 3.3

**Voraussetzungen**

- Stellen Sie sicher, dass genügend Speicherplatz auf dem Laufwerk vorhanden ist, auf dem Wyse Management Suite installiert ist, und das lokale Repository konfiguriert ist.
- Wenn Sie Antiviren- oder andere Überwachungstools auf dem Wyse Management Suite-Setup installiert oder konfiguriert haben, empfiehlt Dell Technologies, die Tools vorübergehend zu deaktivieren, bis das Upgrade abgeschlossen ist. Sie können auch einen entsprechenden Ausschluss zum Installationsverzeichnis, temporären Verzeichnis und lokalen Repository von Wyse Management Suite hinzufügen.

**Schritte**

1. Doppelklicken Sie auf das Installationspaket der Wyse Management Suite 3.2.
2. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
   Die EULA-Details werden angezeigt.
   **ANMERKUNG:** Dieser Bildschirm wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite 3.0 auf 3.x durchführen.
3. Lesen Sie die Lizenzvereinbarung.
4. Wählen Sie **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie anschließend auf **Weiter**.
5. Auf der Seite **Upgrade** konfigurieren Sie den freigegebenen Ordner sowie die Zugangsberechtigungen für die CIFS-Nutzer. Die verfügbaren Optionen sind:
   - Verwenden eines vorhandenen Nutzers – Wählen Sie diese Option aus, um die Anmeldeinformationen für den vorhandenen Nutzer zu validieren.
   - Einen neuen Nutzer erstellen – Wählen Sie diese Option aus und geben Sie die Anmeldeinformationen für einen neuen Nutzer ein.

   **ANMERKUNG:** Wenn das EM SDK während der vorherigen Installation der Wyse Management Suite auf dem Server installiert wurde, werden die Teradici EM SDK-Komponenten automatisch aktualisiert. Wenn das EM SDK während der vorherigen Installation nicht auf dem Gerät installiert wurde, aktivieren Sie das Kontrollkästchen "Teradici EM SDK", um die Teradici EM SDK-Komponenten zu installieren und konfigurieren.

   **ANMERKUNG:** Sie können das Teradici EM SDK auch mit dem Wyse Management Suite-Installationsprogramm installieren und aktualisieren.
6. Aktivieren Sie das Kontrollkästchen **Bind memcached to 127.0.0.1**, um den memcache an den lokalen Server (127.0.0.1) zu binden. Wenn dieses Kontrollkästchen nicht markiert ist, wird Memcache an FQDN **gebunden**.
7. Wählen Sie einen Port für die sichere MQTT-Kommunikation aus. Der Standard-Port ist 8443.
   **ANMERKUNG:** Die Portnummer für die sichere MQTT-Kommunikation darf nicht 0 sein. Die Option zum Auswählen von Ports wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite Version 3.1 und 3.1.1 auf Version 3.3 durchführen.

   Das Fenster **Update der MQTT-Konfiguration** wird angezeigt, wenn eine Nichtübereinstimmung des Hostnamens zwischen MQTT-URLs in der Datenbank vorliegt.
8. Aktivieren Sie das Kontrollkästchen **Empfohlene Änderungen anwenden**, wenn Sie die URLs ändern möchten.
   **ANMERKUNG:** Das Fenster **Update der MQTT-Konfiguration** wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite von Version 3.2 und 3.2.1 auf Version 3.3 durchführen.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie zum Öffnen der Wyse Management Suite-Webkonsole auf **Starten**.

# 7

# Upgrade der Wyse Management Suite von Version 3.x auf 3.5

**Voraussetzungen**

- Stellen Sie sicher, dass genügend Speicherplatz auf dem Laufwerk vorhanden ist, auf dem Wyse Management Suite installiert ist, und das lokale Repository konfiguriert ist.
- Wenn Sie Antiviren- oder andere Überwachungstools auf dem Wyse Management Suite-Setup installiert oder konfiguriert haben, empfiehlt Dell Technologies, die Tools vorübergehend zu deaktivieren, bis das Upgrade abgeschlossen ist. Sie können auch einen entsprechenden Ausschluss zum Installationsverzeichnis, temporären Verzeichnis und lokalen Repository von Wyse Management Suite hinzufügen.

**Schritte**

1. Doppelklicken Sie auf das Installationspaket der Wyse Management Suite 3.5.
2. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
   Die EULA-Details werden angezeigt.

   **ANMERKUNG:** Dieser Bildschirm wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite 3.0 auf 3.x durchführen.
3. Lesen Sie die Lizenzvereinbarung.
4. Wählen Sie **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie anschließend auf **Weiter**.
5. Auf der Seite **Upgrade** können Sie folgende Aufgaben ausführen:
   a. Konfigurieren Sie den freigegebenen Ordner sowie die Zugangsberechtigungen für die CIFS-Nutzer. Die verfügbaren Optionen sind:
      - **Verwenden eines bestehenden Nutzers** – Wählen Sie diese Option aus, um die Zugangsdaten für den vorhandenen Nutzer zu validieren.
      - **Einen neuen Nutzer erstellen** – Wählen Sie diese Option aus und geben Sie die Zugangsdaten für einen neuen Nutzer ein.

      Das Kennwort muss mindestens 8 Zeichen enthalten.
   b. Klicken Sie auf **Weiter**.
   c. Der Bildschirm **Servicekonto-Zugangsdaten** wird angezeigt. Ein lokaler Nutzer mit den geringsten Berechtigungen wird mit den Zugangsdaten erstellt, die in diesem Bildschirm eingegeben werden. Die Dell Wyse Management Suite-Services werden auf diesem Nutzerkonto ausgeführt.
   d. Geben Sie die Zugangsdaten für das Servicekonto ein.

      Das Kennwort muss zwischen 9 und 127 Zeichen enthalten.
   e. Klicken Sie auf **Weiter**.
      Der Bildschirm **Software-Vault-Zugangsdaten** wird angezeigt. Software-Vault wird verwendet, um sensible Daten zu speichern, die von der Dell Wyse Management Suite-Anwendung benötigt werden.
   f. Geben Sie das Kennwort für Software-Vault ein.

      Das Kennwort muss mindestens 8 Zeichen enthalten.
   g. Klicken Sie auf **Weiter**.

   **ANMERKUNG:** Wenn das EM SDK während der vorherigen Installation der Wyse Management Suite auf dem Server installiert wurde, werden die Teradici EM SDK-Komponenten automatisch aktualisiert. Wenn das EM SDK während der vorherigen Installation nicht auf dem Gerät installiert wurde, aktivieren Sie das Kontrollkästchen **Teradici EM SDK**, um die Teradici EM SDK-Komponenten zu installieren und konfigurieren.

   **ANMERKUNG:** Sie können das Teradici EM SDK auch mit dem Wyse Management Suite-Installationsprogramm installieren und aktualisieren.
6. Wählen Sie einen Port für die sichere MQTT-Kommunikation aus. Der Standard-Port ist 8443.

   **ANMERKUNG:** Die Portnummer für die sichere MQTT-Kommunikation darf nicht 0 sein. Die Option zum Auswählen von Ports wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite Version 3.1 und 3.1.1 auf Version 3.5 durchführen.

7. Aktivieren Sie das Kontrollkästchen **Empfohlene Änderungen anwenden**, wenn Sie die URLs ändern möchten.
   **ANMERKUNG:** Das Fenster **Update der MQTT-Konfiguration** wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite von Version 3.2 und 3.2.1 auf Version 3.5 durchführen.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie zum Öffnen der Wyse Management Suite-Webkonsole auf **Starten**.

# 8

# Upgrade der Wyse Management Suite von Version 3.x auf 3.6

**Voraussetzungen**

- Stellen Sie sicher, dass genügend Speicherplatz auf dem Laufwerk vorhanden ist, auf dem Wyse Management Suite installiert ist, und das lokale Repository konfiguriert ist.
- Wenn Sie Antiviren- oder andere Überwachungstools auf dem Wyse Management Suite-Setup installiert oder konfiguriert haben, empfiehlt Dell Technologies, die Tools vorübergehend zu deaktivieren, bis das Upgrade abgeschlossen ist. Sie können auch einen entsprechenden Ausschluss zum Installationsverzeichnis, temporären Verzeichnis und lokalen Repository von Wyse Management Suite hinzufügen.

**Schritte**

1. Doppelklicken Sie auf das Installationspaket der Wyse Management Suite 3.6.
2. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
   Die EULA-Details werden angezeigt.
   **ANMERKUNG:** Dieser Bildschirm wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite 3.0 auf 3.x durchführen.
3. Lesen Sie die Lizenzvereinbarung.
4. Wählen Sie **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie anschließend auf **Weiter**.
5. Auf der Seite **Upgrade** können Sie folgende Aufgaben ausführen:
   a. Konfigurieren Sie den freigegebenen Ordner sowie die Zugangsberechtigungen für die CIFS-Nutzer. Die verfügbaren Optionen sind:
      - **Verwenden eines bestehenden Nutzers** – Wählen Sie diese Option aus, um die Zugangsdaten für den vorhandenen Nutzer zu validieren.
      - **Einen neuen Nutzer erstellen** – Wählen Sie diese Option aus und geben Sie die Zugangsdaten für einen neuen Nutzer ein.

      Das Kennwort muss mindestens acht Zeichen enthalten.
   b. Klicken Sie auf **Weiter**.
      Der Bildschirm **Servicekonto-Zugangsdaten** wird angezeigt. Wählen Sie die Optionen basierend auf Ihrer vorhandenen Wyse Management Suite-Version aus.
      - Wenn Sie ein Upgrade von Wyse Management Suite Version 3.3 oder 3.3.1 auf 3.6 durchführen, werden die folgenden Optionen angezeigt:
        - **Einen neuen lokalen Nutzer erstellen** – Wählen Sie diese Option aus, um Anmeldeinformationen einzugeben und einen neuen lokalen Nutzer mit den geringsten Berechtigungen zu erstellen. Der neue Nutzer wird der Gruppe **Nutzer** hinzugefügt, aber der Nutzer verfügt nicht über Administratorrechte.
          **ANMERKUNG:** Der Nutzername, den Sie auf dem Bildschirm **Servicekonto-Anmeldeinformationen** eingeben, darf nicht mit Ihrem Teradici-Nutzernamen identisch sein. Der Nutzername muss zwischen 2 und 20 Zeichen enthalten. Ihr Kennwort muss 9 bis 127 Zeichen lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten. Leerzeichen sind im Kennwort nicht zulässig.
        - **Einen vorhandenen lokalen Nutzer verwenden** – Wählen Sie diese Option aus, um die Anmeldeinformationen eines vorhandenen lokalen Nutzers einzugeben. Wenn Sie diese Option auswählen, wird eine Meldung angezeigt. Stellen Sie sicher, dass der Nutzer bereits vorhanden ist, über Serviceanmeldungsrechte (**SeServiceLogonRight**) verfügt und sich mindestens einmal erfolgreich beim System angemeldet hat. Dell Technologies empfiehlt, sicherzustellen, dass der Nutzer keine Administratorrechte hat.
          **ANMERKUNG:** Wenn Sie diese Option auswählen, wird die Komplexität des Kennworts nicht überprüft und der Nutzername, den Sie eingeben, muss 2 bis 20 Zeichen lang sein.
        - **Einen vorhandenen Domainnutzer verwenden** – Wählen Sie diese Option aus, um die Anmeldeinformationen eines vorhandenen Domainnutzers einzugeben. Wenn Sie diese Option auswählen, wird eine Meldung angezeigt. Stellen Sie sicher, dass der Nutzer bereits in der Domain vorhanden ist, über Serviceanmeldungsrechte (**SeServiceLogonRight**) verfügt und sich mindestens einmal erfolgreich beim System angemeldet hat. Dell Technologies empfiehlt, sicherzustellen, dass der Nutzer keine Administratorrechte hat.

**ANMERKUNG:** Wenn Sie diese Option auswählen, wird die Komplexität des Kennworts nicht überprüft.

- Wenn Sie ein Upgrade von Wyse Management Suite Version 3.5 auf 3.6 durchführen, geben Sie die Anmeldedaten ein, um einen lokalen Nutzer mit den geringsten Berechtigungen zu erstellen. Die Dell Wyse Management Suite-Services werden auf diesem Nutzerkonto ausgeführt.

c. Klicken Sie auf **Weiter**, nachdem Sie die Anmeldeinformationen eingegeben haben.
Der Bildschirm **Software-Vault-Zugangsdaten** wird angezeigt. Software-Vault wird verwendet, um sensible Daten zu speichern, die von der Dell Wyse Management Suite-Anwendung benötigt werden.

d. Geben Sie das Kennwort für Software-Vault ein.
Das Kennwort muss mindestens acht Zeichen enthalten.

e. Klicken Sie auf **Weiter**.

**ANMERKUNG:** Wenn das EM SDK während der vorherigen Installation der Wyse Management Suite auf dem Server installiert wurde, werden die Teradici EM SDK-Komponenten automatisch aktualisiert. Wenn das EM SDK während der vorherigen Installation nicht auf dem Gerät installiert wurde, aktivieren Sie das Kontrollkästchen **Teradici EM SDK**, um die Teradici EM SDK-Komponenten zu installieren und konfigurieren.

**ANMERKUNG:** Sie können das Teradici EM SDK auch mit dem Wyse Management Suite-Installationsprogramm installieren und aktualisieren.

6. Wählen Sie einen Port für die sichere MQTT-Kommunikation aus. Der Standard-Port ist 8443.

**ANMERKUNG:** Die Portnummer für die sichere MQTT-Kommunikation darf nicht 0 sein. Die Option zum Auswählen von Ports wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite Version 3.1 und 3.1.1 auf Version 3.6 durchführen.

7. Aktivieren Sie das Kontrollkästchen **Empfohlene Änderungen anwenden**, wenn Sie die URLs ändern möchten.

**ANMERKUNG:** Das Fenster **Update der MQTT-Konfiguration** wird angezeigt, wenn Sie ein Upgrade von Wyse Management Suite von Version 3.2 und 3.2.1 auf Version 3.6 durchführen.

8. Klicken Sie auf **Weiter**.
9. Klicken Sie zum Öffnen der Wyse Management Suite-Webkonsole auf **Starten**.

# 9

# Deinstallieren der Wyse Management Suite

So deinstallieren Sie die Wyse Management Suite:

1. Doppelklicken Sie auf das Symbol **WMS**.

   Der Deinstallationsassistent wird gestartet und der Bildschirm **Wyse Management Suite-Deinstallationsprogramm** wird angezeigt.

2. Klicken Sie auf **Weiter**. Standardmäßig ist die Optionsschaltfläche **Entfernen** ausgewählt, die alle Installationskomponenten der Wyse Management Suite deinstalliert.

# 10

# Beheben von Fehlern in der Wyse Management Suite

Dieser Abschnitt enthält Informationen zum Beheben von Funktionsstörungen der Wyse Management Suite.

## Probleme mit dem Zugriff auf die Wyse Management Suite-Webkonsole

- Problem: Beim Versuch zum Herstellen einer Verbindung mit der Wyse Management Suite-Konsole, wird die Authentifizierungs-GUI nicht angezeigt und eine HTTP-Status-404-Seite wird angezeigt.

  Problemumgehung: Stoppen und starten Sie die Dienste in der folgenden Reihenfolge:
  1. Dell WMS: MariaDB
  2. Dell WMS: memcached
  3. Dell WMS: MongoDB
  4. Dell WMS: MQTT Broker Service
  5. Dell WMS: Tomcat Service

- Problem: Beim Versuch zum Herstellen einer Verbindung mit der Wyse Management Suite-Konsole, wird die Authentifizierungs-GUI nicht angezeigt und die folgende Fehlermeldung wird angezeigt:

  **Diese Seite kann nicht angezeigt werden**

  Workaround: Starten Sie Dell WMS: Tomcat Service neu

- Problem: Die Wyse Management Suite-Webkonsole reagiert nicht oder die Informationen auf der Webseite werden nicht ordnungsgemäß angezeigt, wenn Sie Internet Explorer verwenden.

  Problemumgehung:
  - Stellen Sie sicher, dass Sie die unterstützte Version von Internet Explorer verwenden.
  - Stellen Sie sicher, dass die erhöhte Sicherheit des Internet Explorer deaktiviert ist.
  - Stellen Sie sicher, dass die Einstellungen für die Kompatibilitätsansicht deaktiviert sind.

## Registrieren von Geräten mit der Wyse Management Suite

**ANMERKUNG:** Weitere Informationen zur Sicherheitsumgebung für Kunden finden Sie unter Wyse-Geräte-Agent.

- Problem: Geräte lassen sich mit der Wyse Management Suite in der öffentlichen Cloud nicht registrieren

  Problemumgehung:
  - Stellen Sie sicher, dass Port 443 und Port 1883 offen sind.
  - Überprüfen Sie Ihre Netzwerkverknüpfung und greifen Sie für die öffentliche Cloud über den Browser auf die Wyse Management-Webanwendung zu.
  - Wenn **Automatische Ermittlung** aktiviert ist, überprüfen Sie, ob DHCP- oder DNS-SVR-Einträge korrekt konfiguriert sind. Prüfen Sie auch die Server-URL und die Gruppentoken.
  - Überprüfen Sie, ob Sie das Gerät manuell registrieren können.

- Problem: Geräte lassen sich mit der Wyse Management Suite in der privaten Cloud nicht registrieren.

  Problemumgehung:

- Stellen Sie sicher, dass Port 443 und Port 1883 offen sind.
- Überprüfen Sie die Internetverbindung und testen Sie, ob Sie über den Browser auf die Wyse Management-Webanwendung zugreifen können.
- Wenn die automatische Ermittlung aktiviert ist, überprüfen Sie, ob DHCP- oder DNS-SRV-Einträge korrekt konfiguriert sind. Prüfen Sie auch die Server-URL und die Gruppentoken.
- Überprüfen Sie, ob Sie das Gerät manuell registrieren können.
- Überprüfen Sie, ob Sie selbstsignierte oder bekannte Zertifikate verwenden.

  **ANMERKUNG:** Standardmäßig installiert die Wyse Management Suite selbstsignierte Zertifikate. Die CA-Validierung muss deaktiviert sein, damit Geräte mit dem Wyse Management Suite-Server kommunizieren können.

# Fehler beim Senden von Befehlen an das Gerät

Problem: Befehle wie Paket aktualisieren, erneut auf Gerät starten usw. können nicht gesendet werden.

Problemumgehung:

- Stellen Sie sicher, dass der Dell WMS: Broker Service auf dem Wyse Management Suite-Server ausgeführt wird.
- Prüfen Sie, ob Port 1883 geöffnet ist.
- Stellen Sie vor dem Senden eines Befehls sicher, dass das Gerät nicht heruntergefahren ist oder sich im Energiesparmodus befindet.

# 11

# Wyse-Geräte-Agent

Der Wyse-Geräte-Agent (WDA) ist ein einheitlicher Agent für alle Lösungen zur Thin Client-Verwaltung. Durch die Installation des WDA können Sie Thin Clients mit der Wyse Management Suite verwalten.

Die folgenden drei Arten von Kundensicherheitsumgebungen werden vom Wyse-Geräte-Agenten unterstützt:

- **Hochsichere Umgebungen**: Um das Risiko von nicht autorisierten DHCP- oder DNS-Servern für die Erkennung neuer Geräte zu minimieren, müssen sich Administratoren bei jedem Gerät einzeln anmelden und die Server-URL der Wyse Management Suite konfigurieren. Sie können entweder CA-signierte oder selbst signierte Zertifikate verwenden. Dell empfiehlt jedoch, ein CA-signiertes Zertifikat zu verwenden. In der privaten Cloud-Lösung der Wyse Management Suite mit selbst signiertem Zertifikat sollte das Zertifikat in jedem Gerät manuell konfiguriert werden. Außerdem muss das Zertifikat in den Ordner `Agent Configuration` kopiert werden, um das Zertifikat zu bewahren und das Risiko eines nicht autorisierten DHCP- oder DNS-Servers auch nach dem Aufspielen eines neuen Abbilds auf das Gerät zu minimieren.

  Der Ordner `Agent Configuration` ist an folgendem Speicherort verfügbar:
  - Windows Embedded Standard-Geräte: `%SYSTEMDRIVE%\\Wyse\\WCM\\ConfigMgmt\\Certificates`
  - ThinLinux-Geräte: `/etc/addons.d/WDA/certs`
  - ThinOS-Geräte: `wnos/cacerts/`

  **ANMERKUNG:** Sie müssen das Zertifikat über ein USB-Laufwerk oder FTP-Pfade auf einen Thin Client mit ThinOS-Betriebssystem importieren.
- **Gesicherte Umgebungen**: Um das Risiko von nicht autorisierten DHCP- oder DNS-Servern für die Erkennung neuer Geräte zu minimieren, müssen Administratoren den Wyse Management Suite-Server mit CA-signierten Zertifikaten konfigurieren. Das Gerät kann die Server-URL der Wyse Management Suite aus den DHCP/DNS-Einträgen abrufen und die CA-Validierung durchführen. Die private Cloud-Lösung der Wyse Management Suite mit selbst signiertem Zertifikat erfordert, dass das Zertifikat nach der ersten Registrierung auf das Gerät übertragen wird, wenn das Gerät vor der Registrierung nicht über das Zertifikat verfügt. Dieses Zertifikat bleibt auch nach einem Neuimage oder Neustart des Geräts erhalten, um das Risiko nicht autorisierter DHCP- oder DNS-Server zu minimieren.
- **Normale Umgebungen**: Das Gerät bezieht die Server-URL der Wyse Management Suite aus den DHCP/DNS-Einträgen für die private Cloud der Wyse Management Suite, die mit einem CA- oder selbst signierten Zertifikat konfiguriert ist. Wenn die Option CA-Validierung auf dem Gerät deaktiviert ist, wird der Administrator der Wyse Management Suite benachrichtigt, nachdem Sie das Gerät zum ersten Mal registrieren. In diesem Szenario empfiehlt Dell Administratoren, das Zertifikat auf das Gerät zu übertragen, auf dem der Server mit selbst signiertem Zertifikat konfiguriert ist. Diese Umgebung ist für die öffentliche Cloud nicht verfügbar.

# 12

# Weitere Ressourcen

Video-Lehrgänge über:

- Installieren der Wyse Management Suite finden Sie unter Installation der Wyse Management Suite.
- automatische Konfiguration von ThinOS-Clients mit der Wyse Management Suite vor Ort mit DHCP-Options-Tags finden Sie unter Konfigurieren von ThinOS-Geräten mit der Wyse Management Suite.

# A

# Remote-Datenbank

Eine Remote- oder Cloud-Datenbank (DB) ist eine Datenbank, die für eine virtualisierte Umgebung erstellt wurde, zum Beispiel für eine Hybrid Cloud, eine öffentliche Cloud oder eine private Cloud. In der Wyse Management Suite können Sie entweder die Mongo-Datenbank (MongoDB) oder die Maria-Datenbank (MariaDB) bzw. beide Datenbänke basierend auf Ihren Anforderungen konfigurieren.

**Themen:**



## Konfigurieren der Mongo-Datenbank

### Voraussetzungen

Mongo-Datenbank (MongoDB) arbeitet auf dem Transmission Control Protocol (TCP) mit der Portnummer 27017.

**ANMERKUNG:** Ersetzen Sie je nach Bedarf alle Wert, die Ihre Umgebungsvariablen in Fettschrift enthalten.

### Schritte

1. Installieren Sie die MongoDB Version 4.2.16.
2. Kopieren Sie die MongoDB-Dateien auf Ihr lokales System: `C:\Mongo`.
3. Erstellen Sie die folgenden Verzeichnisse, wenn sie nicht existieren.
   - `C:\data`
   - `C:\data\db`
   - `C:\data\log`
4. Gehen Sie zum Mongo-Ordner (`C:\Mongo`) und erstellen Sie eine Datei mit dem Namen `mongod.cfg`.
5. Öffnen Sie die Datei `mongod.cfg` in einem Editor und fügen Sie das folgende Skript hinzu:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
```

6. Speichern und schließen Sie die Datei `mongod.cfg`.
7. Öffnen Sie die Eingabeaufforderung als Administrator und führen Sie den folgenden Befehl aus:

   `mongod.exe --config "C:\Program Files\MongoDB\Server\4.2\mongod.cfg" -install` oder `sc.exe create MongoDB binPath= "\"C:\ProgramFiles\MongoDB\Server\3.2\bin\mongod.exe\"--service --config=\"C:\ProgramFiles\MongoDB\Server\4.2\mongod.cfg\"" DisplayName= "Dell WMS: MongoDB" start="auto"`

   MongoDB ist installiert.
8. Führen Sie zum Starten des MongoDB-Dienstes den folgenden Befehl aus:

   `net start mongoDB`
9. Führen Sie zum Starten der Mongo-Datenbank den folgenden Befehl aus:

   `mongo.exe`
10. Führen Sie zum Öffnen der Standard-Administratordatenbank den folgenden Befehl aus:

    `use admin;`
11. Sobald die MongoDB-Tabelle angezeigt wird, führen Sie die folgenden Befehle aus:

```
db.createUser(
{
```

```
user:"wmsuser",
pwd:"PASSWORD",
roles:[{role:"userAdminAnyDatabase",db:"admin"},
{role:"dbAdminAnyDatabase",db:"admin"},
{role:"readWriteAnyDatabase",db:"admin"},
{role:"dbOwner",db:"stratus"}]
}
)
```

12. Führen Sie zum Wechseln zur Stratus-Datenbank den folgenden Befehl aus:
    `use stratus;`
13. Führen Sie zum Stoppen der MongoDB-Dienste den folgenden Befehl aus:
    `net stop mongoDB`
14. Fügen Sie eine Authentifizierungsberechtigung für die Administrator-DB hinzu. Ändern Sie die Datei `mongod.cfg` zu Folgendem:

```
systemLog:
destination:file
path:c:\data\log\mongod.log
storage:
dbPath:c:\data\db
security:
authorization:enabled
```

15. Führen Sie zum Neustarten des MongoDB-Dienstes die folgenden Schritte durch:
    `net Start mongoDB;`

### Nächste Schritte

Im Wyse Management Suite-Installationsprogramm muss der Administrator den Nutzernamen und das Kennwort verwenden, die für den Zugriff auf die Stratus-Datenbanken in MongoDB erstellt wurden. Informationen über das Festlegen der MongoDB im Wyse Management Suite-Installationsprogramm finden Sie unter Nutzerdefinierte Installation.

# Konfigurieren der Maria-Datenbank

Die Maria-Datenbank (MariaDB) arbeitet auf dem Transmission Control Protocol (TCP) mit der Portnummer 3306.

### Info über diese Aufgabe

**ANMERKUNG:**

- Die hier angezeigte IP-Adresse gehört zum Wyse Management Suite-Server, der die Webkomponenten hostet.
- Ersetzen Sie je nach Bedarf alle Wert, die Ihre Umgebungsvariablen in Fettschrift enthalten.

Zum Konfigurieren von MariaDB führen Sie folgendes durch:

### Schritte

1. Installieren Sie MariaDB Version 10.2.29.
2. Navigieren Sie zum MariaDB Installationspfad: `C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p`.
3. Geben Sie das Root-Kennwort ein, das während der Installation erstellt wurde.
4. Erstellen Sie die Stratus-Datenbank – `DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_unicode_ci;`.
5. Erstellen Sie den Nutzer `'stratus'@'localhost';`
6. Nutzer erstellen `'stratus'@'`**IP ADDRESS**`';`
7. Festlegen eines Kennworts für `'stratus'@'localhost'=password('`**PASSWORD**`');`
8. Festlegen eines Kennworts für `'stratus'@'IP ADDRESS'=password('`**PASSWORD**`');`
9. Stellen Sie alle Berechtigungen auf `*.* to 'stratus'@'`**IP ADDRESS**`'`, die durch `'`**PASSWORD**`'` mit einer Erteilungsoption identifiziert wurden, zur Verfügung.
10. Stellen Sie alle Berechtigungen auf `*.* to 'stratus'@'localhost'`, die durch `'`**PASSWORD**`'` mit einer Erteilungsoption identifiziert wurden, zur Verfügung.

### Nächste Schritte

**ANMERKUNG:** Navigieren Sie im zweiten Schritt zum Konfigurieren des benutzerdefinierten Ports für MariaDB zu `C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p -P<custom port>`.

Der Administrator muss im Wyse Management Suite-Installationsprogramm den gleichen Benutzernamen und das gleiche Kennwort verwenden, die für den Zugriff auf die Stratus-Datenbanken in MariaDB erstellt wurden. Weitere Informationen über das Einrichten der MariaDB im Wyse Management Suite-Installationsprogramm finden Sie unter Benutzerdefinierte Installation.

B

# Nutzerdefinierte Installation

Bei der nutzerdefinierten Installation können Sie zum Einrichten der Wyse Management Suite eine Datenbank auswählen. Sie müssen außerdem die grundlegenden technischen Praxiskenntnisse zur Wyse Management Suite besitzen. Dell empfiehlt die nutzerdefinierte Installation nur fortgeschrittenen Nutzern.

1. Wählen Sie als **Setup-Typ Nutzerdefiniert** aus und klicken Sie auf **Weiter**.

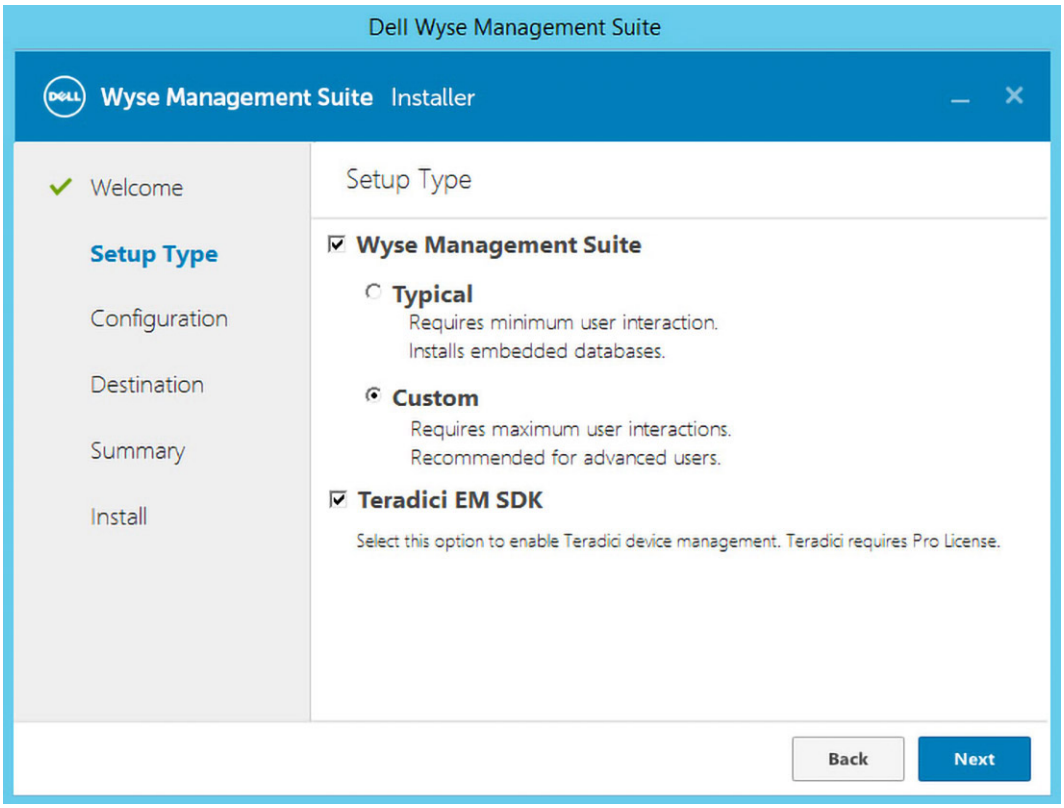


**Abbildung 12. Setup-Typ**

Die Seite **Mongo-Datenbankserver** wird angezeigt.

2. Wählen Sie als Mongo-Datenbankserver entweder **Eingebettete MongoDB** oder **Externe MongoDB** aus.
   - Wenn **Eingebettete MongoDB** ausgewählt wurde, geben Sie Ihr Kennwort ein und klicken Sie auf **Weiter**.

     **ANMERKUNG:** Das Kennwort muss zwischen 9 und 31 Zeichen lang sein.

     **ANMERKUNG:** Der Nutzername und die Datenbankserverdetails sind nicht erforderlich, wenn die integrierte Mongo-Datenbank ausgewählt wurde und die entsprechenden Felder grau hinterlegt sind.

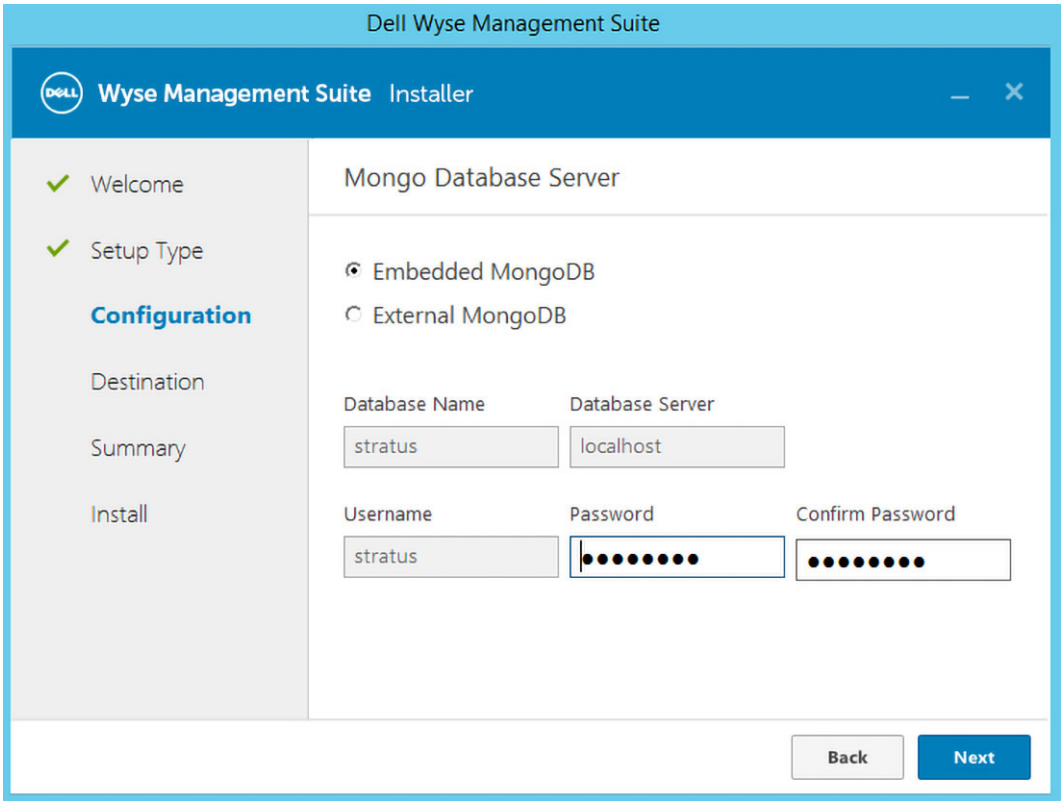


**Abbildung 13. Integrierter Mongo-Datenbankserver**

- Wenn **Externe MongoDB** ausgewählt wurde, geben Sie den Nutzernamen, das Kennwort, die Datenbankserverdetails und die Portdetails ein und klicken Sie auf **Weiter**.

  **ANMERKUNG:** Das Portfeld generiert den Standardport, der geändert werden kann.

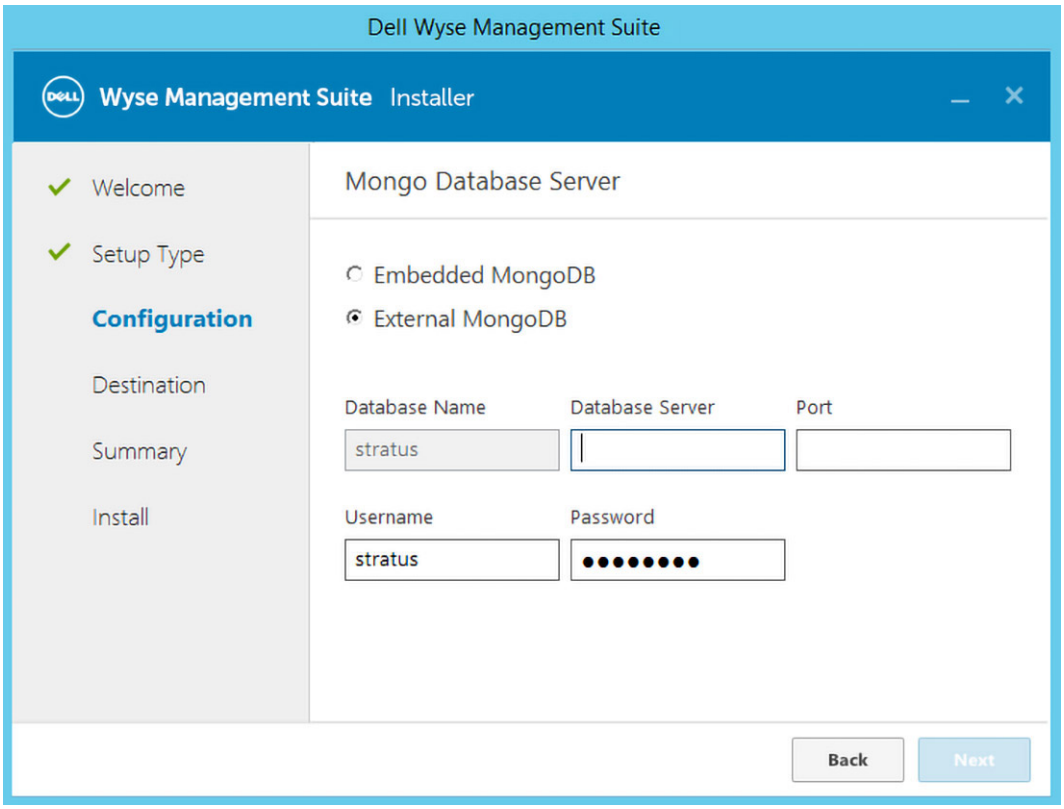


**Abbildung 14. Externe MongoDB**

Die Seite **MariaDB-Datenbankserver** wird angezeigt.

3. Wählen Sie entweder **Eingebettete MariaDB** oder **Externe MariaDB** als MariaDB-Datenbankserver aus.

- Wenn **Eingebettete MariaDB** ausgewählt wurde, geben Sie den Nutzernamen und das Kennwort ein und klicken Sie auf **Weiter**.
  **ANMERKUNG:** Das Kennwort muss zwischen 9 und 31 Zeichen lang sein.

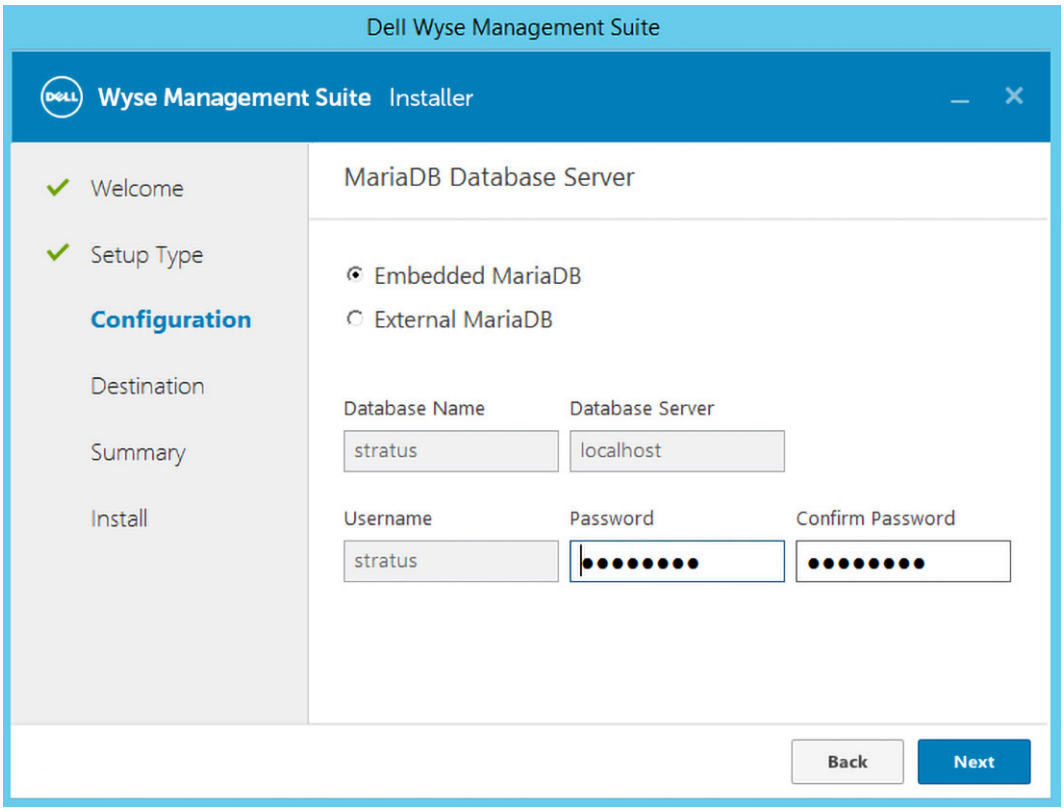


**Abbildung 15. Integrierte MariaDB**

- Wenn **Externe MariaDB** ausgewählt wurde, geben Sie den Nutzernamen, das Kennwort, die Datenbankserverdetails und die Portdetails ein und klicken Sie auf **Weiter**.

  Das Portfeld generiert den Standardport, der geändert werden kann.

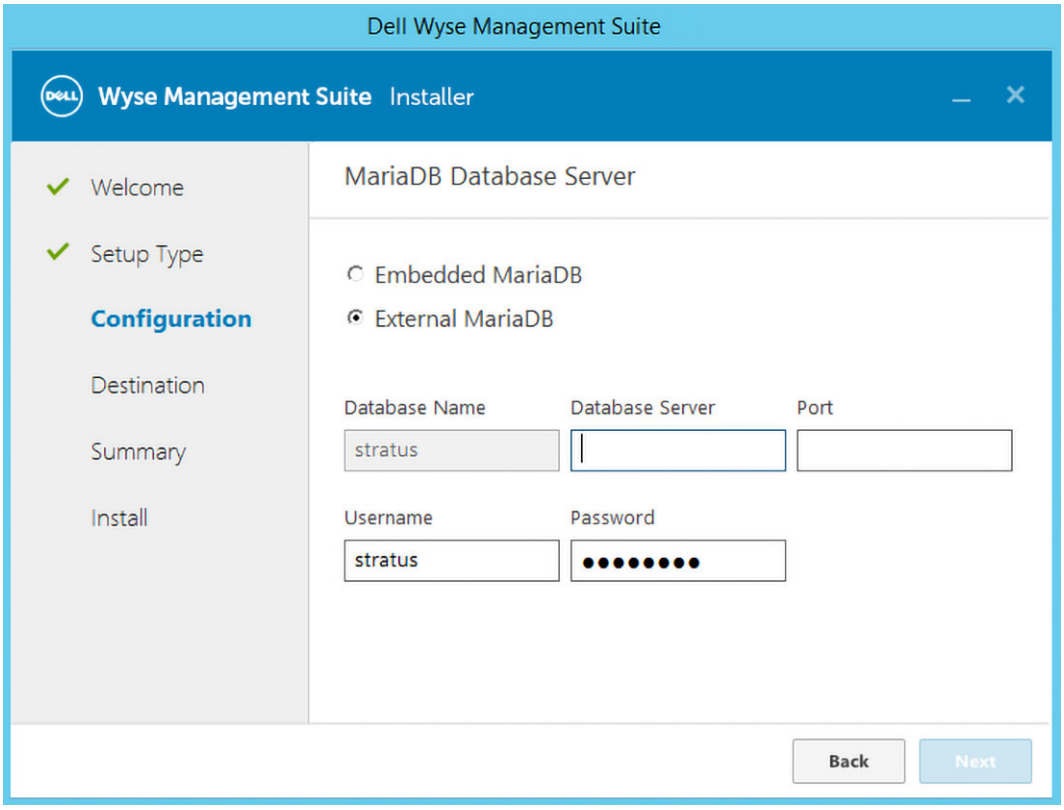


**Abbildung 16. Externe MariaDB**

4. Die Seite **Port** wird angezeigt, die es Ihnen erlaubt, die Ports für die folgenden Datenbanken anzupassen:
   - Apache Tomcat
   - MySQL-Datenbank
   - Mongo-Datenbank
   - MQTT v3.1 Broker
   - Memcached

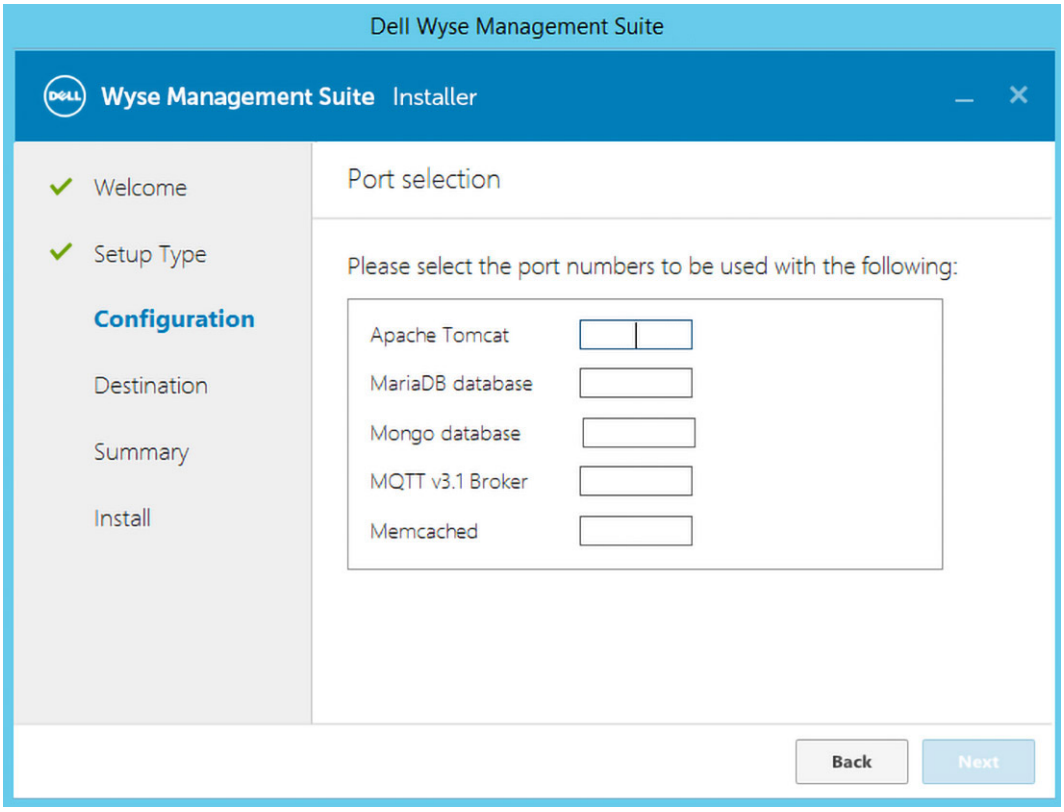


**Abbildung 17. Portauswahl**

**ANMERKUNG:** Die Wyse Management Suite verwendet die Maria-Datenbank und Mongo-Datenbank für Folgendes:

Maria Datenbank – Relationale Datenbank für Daten, die eine klar definierte Struktur und Normalisierung erfordern.

Mongo Datenbank – No-SQL-Datenbank für Leistung und Skalierbarkeit.

Befolgen Sie zur Durchführung der Installation die Anweisungen in Abschnitt Lokale Installation der WMS und erstmaliges Setup.

C

# Zugreifen auf Wyse Management Suite Datei-Repository

**Datei-Repositorys** sind Orte, an denen **Dateien** gespeichert organisiert werden. Die Wyse Management Suite verfügt über zwei Arten von Repositorys:

- **Lokales Repository** – Während der Installation der Wyse Management Suite in einer Private Cloud geben Sie den Pfad zum lokalen Repository in das Wyse Management Suite-Installationsprogramm ein. Nach der Installation, gehen Sie zu **Portaladministrator** > **Datei-Repository** und wählen Sie das lokale Repository aus. Klicken Sie auf die Option **Bearbeiten** zum Anzeigen und Bearbeiten der Einstellungen für das Repository.
- **Wyse Management Suite Repository** – Melden Sie sich bei der Wyse Management Suite in der Public Cloud an, gehen Sie zu **Portaladministrator** > **Datei-Repository** und laden Sie das Wyse Management Suite-Repository-Installationsprogramm herunter. Nach der Installation registrieren Sie das Wyse Management Suite-Repository am Wyse Management Suite-Verwaltungsserver durch Angabe der erforderlichen Informationen.

Sie können die Option **Automatische Replikation** aktivieren, um Dateien, die zu einem der Datei-Repositorys hinzugefügt wurden, in anderen Repositorys zu replizieren. Wenn Sie diese Option aktivieren, wird eine Warnmeldung angezeigt. Sie können das Kontrollkästchen **Vorhandene Dateien replizieren** aktivieren, um die vorhandenen Dateien in Ihren Datei-Repositorys zu replizieren.

Die Option **Vorhandene Dateien replizieren** ist anwendbar, wenn das Repository bereits registriert ist. Wenn ein neues Repository registriert ist, dann werden alle Dateien zum neuen Repository kopiert. Sie können den Status der Dateireplikation auf der Seite **Ereignisse** einsehen.

Die `Image Pull`-Vorlagen werden nicht automatisch in anderen Repositories repliziert. Sie müssen diese Dateien manuell kopieren.

Die Funktion zur Dateireplikation wird nur von Repositorys der Wyse Management Suite 2.0 und späteren Versionen unterstützt.

Sie können kein selbst signiertes Zertifikat des Remote-Repositorys in den Wyse Management Suite-Server importieren. Wenn die CA-Validierung für das Remote-Repository aktiviert ist, schlägt die Replikation von Dateien aus dem Remote-Repository in das lokale Repository fehl.

Die ausgewählte TLS-Version muss identisch oder höher sein als die TLS-Version, die auf dem Wyse Management Suite Server konfiguriert ist. Stellen Sie sicher, dass Sie alle entsprechenden Versionen von TLS basierend auf den Support-Kriterien der verwalteten Geräte auswählen.

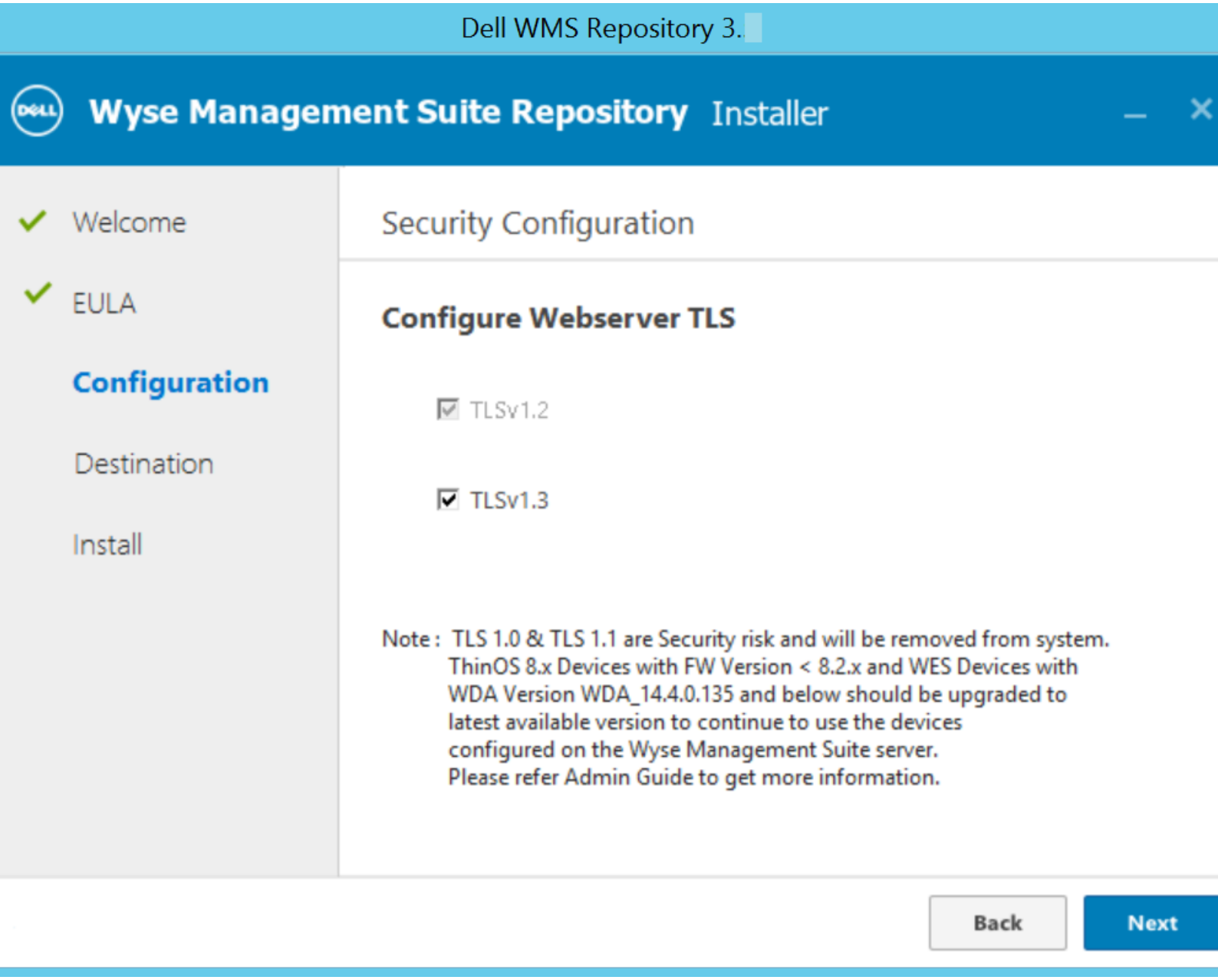


**Abbildung 18. Wyse Management Suite Repository Installer**

**ANMERKUNG:** Wählen Sie TLSv1.1 und höher nicht aus, wenn die WDA-Version auf dem Windows Embedded Standardgerät niedriger ist als 14.4.0.153_Unified und wenn Sie Merlin Imaging Agent verwenden. TLSv1.1 und höher sollte nicht ausgewählt werden, wenn Sie das Import-Tool verwenden, um vom Wyse Device Manager zur Wyse Management Suite zu migrieren.

Für die Verwendung des Wyse Management Suite-Repositorys führen Sie folgendes aus:

1. Laden Sie das Wyse Management Suite-Repository von der Public-Cloud-Konsole herunter.
2. Nach dem Installationsprozess starten Sie die Anwendung.
3. Auf der Wyse Management Suite-Repository-Seite geben Sie die Zugangsdaten zur Registrierung des Wyse Management Suite-Repositorys am Wyse Management Suite-Server an.
4. Wenn Sie die Option **Im öffentlichen WMS Management Portal registrieren** aktivieren, können Sie das Repository in der Public Cloud der Wyse Management Suite registrieren.
5. Klicken Sie auf die Option **Dateien synchronisieren** zum Senden des Dateisynchronisierungsbefehls.
6. Klicken Sie auf **Check in** und klicken Sie dann auf **Befehl senden**, um den Geräteinformationsbefehl an das Gerät zu senden.
7. Klicken Sie auf die Option **Registrierung aufheben**, um die Registrierung am vor Ort-Dienst aufzuheben.
8. Klicken Sie auf **Bearbeiten**, um die Datei zu bearbeiten.

9. Wählen Sie aus der Drop-down-Liste der Option **Gleichzeitige Dateidownloads** die Anzahl der Dateien aus.
10. Aktivieren oder deaktivieren Sie die Option **Wake-on-LAN**.
11. Aktivieren oder deaktivieren Sie die Option **Schneller Datei-Up- und Download (HTTP)**.
    - Wenn HTTP aktiviert ist, erfolgt das Hoch- und Herunterladen der Datei über HTTP.
    - Wenn HTTP nicht aktiviert ist, erfolgt das Hoch- und Herunterladen der Datei über HTTPS.
12. Wählen Sie das **Zertifikatsvalidierung** Kontrollkästchen zur Aktivierung der CA-Zertifikatüberprüfung für die Public Cloud.

    **ANMERKUNG:** Wenn die CA-Validierung des Wyse Management Suite Servers aktiviert ist, sollte das Zertifikat im Client vorhanden sein. Alle Vorgänge, wie z. B., Apps und Daten, Bildabruf, sind erfolgreich. Wenn das Zertifikat nicht im Client vorhanden ist, bietet der Wyse Management Suite Server eine generische Audit-Ereignisbenachrichtigung **Validierung der Zertifizierungsstelle fehlgeschlagen** auf der Seite **Ereignisse**. Alle Vorgänge, wie z. B., Apps und Daten, Bildabruf, waren nicht erfolgreich. Wenn die CA-Validierung von Wyse Management Suite-Server nicht aktiviert ist, findet die Kommunikation zwischen Server und Client in einem sicheren Kanal ohne Validierung der Zertifikatssignatur statt.
13. Fügen Sie einen Hinweis in dem angegebenen Feld hinzu.
14. Klicken Sie auf **Einstellungen speichern**.

D

# Erstellen und Konfigurieren von DHCP-Options-Tags

**Info über diese Aufgabe**

**ANMERKUNG:** Weitere Informationen zur Sicherheitsumgebung für Kunden finden Sie unter Wyse-Geräte-Agent.

Zum Erstellen eines DHCP-Option-Tags gehen Sie wie folgt vor:

**Schritte**

1. Öffnen Sie den Server-Manager.
2. Gehen Sie zu **Tools** und klicken Sie auf **DHCP-Option**.
3. Gehen Sie zu **FQDN** > **IPv4** und klicken Sie mit der rechten Maustaste auf **IPv4**.

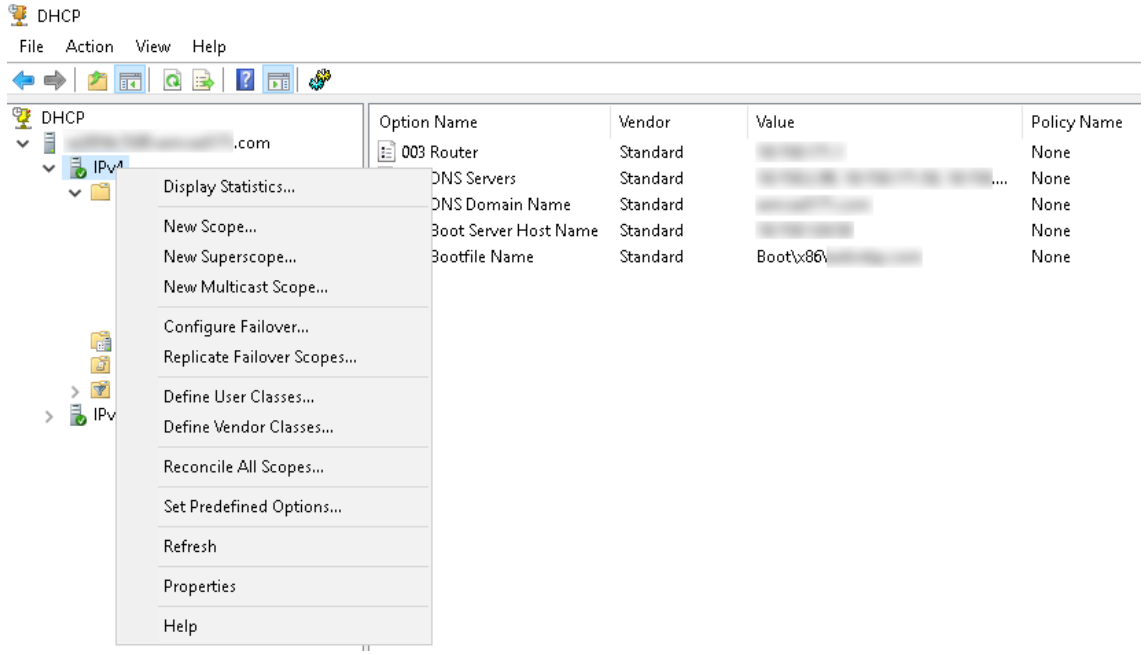


**Abbildung 19. DHCP**

4. Klicken Sie auf **Vordefinierte Optionen festlegen**.
   Das Fenster **Vordefinierte Optionen und Werte** wird angezeigt.
5. Wählen Sie aus der Dropdownliste **Optionsklasse** den Wert **DHCP-Standardoption** aus.

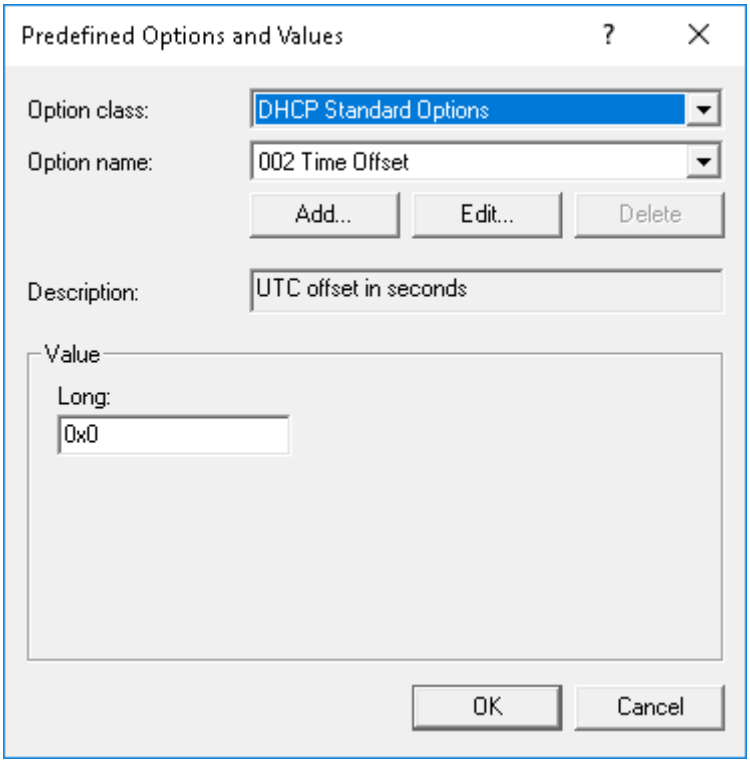


**Abbildung 20. Vordefinierte Optionen und Werte**

6. Klicken Sie auf **Hinzufügen**.
   Das Fenster **Optionstyp** wird angezeigt.

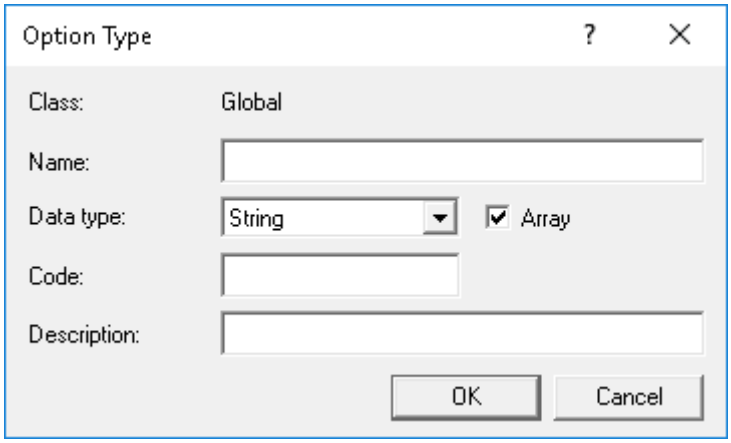


**Abbildung 21. Optionstyp**

**Beispiel**

Die Optionen müssen entweder zu den Serveroptionen des DHCP-Servers oder den Bereichsoptionen des DHCP-Bereichs hinzugefügt werden.

**Konfigurieren der DHCP-Option-Tags**

- Zum Erstellen des Option-Tags 165 Wyse Management Suite Server-URL gehen Sie wie folgt vor:
  1. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
     - Name – WMS
     - Datentyp – Zeichenfolge
     - Code – 165
     - Beschreibung – WMS_Server
  2. Geben Sie den folgenden Wert ein und klicken Sie auf **OK**.

Zeichenfolge –`WMS FQDN`

Zum Beispiel WMSServerName.YourDomain.Com:443

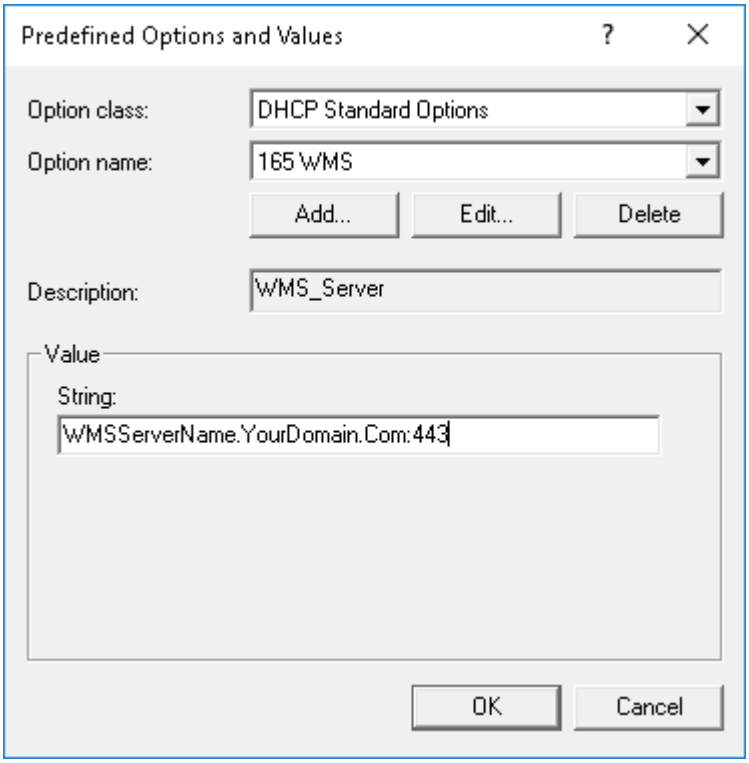


**Abbildung 22. Option-Tag 165 Wyse Management Suite Server-URL**

- Zum Erstellen des Option-Tags 166 MQTT-Server-URL gehen Sie wie folgt vor:

1. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
   - Name – MQTT
   - Datentyp – Zeichenfolge
   - Code – 166
   - Beschreibung – MQTT-Server
2. Geben Sie den folgenden Wert ein und klicken Sie auf **OK**.

   Zeichenfolge –`MQTT FQDN`

   Zum Beispiel WMSServerName.YourDomain.Com:1883

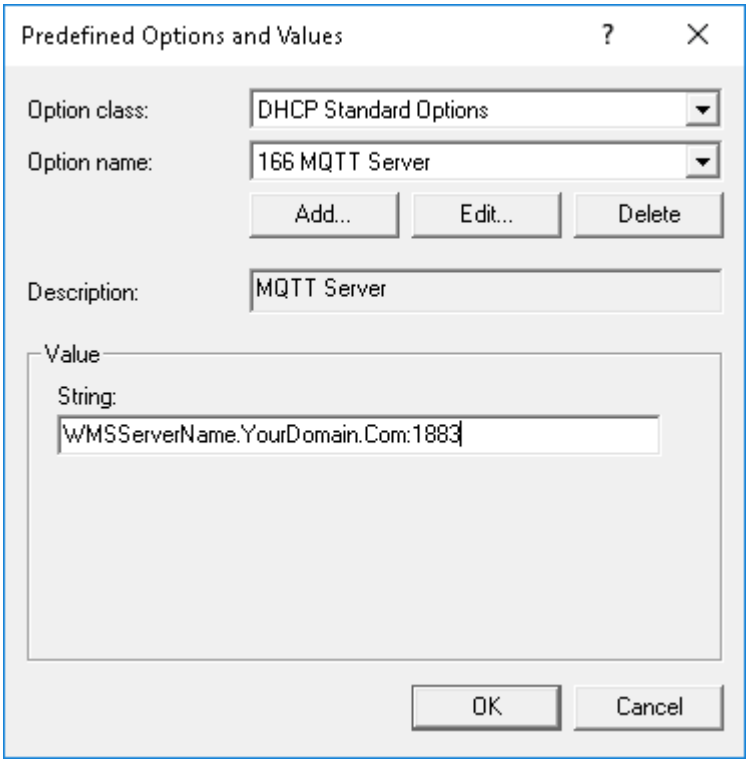


**Abbildung 23. Option-Tag 166 Wyse Management Suite Server-URL**

- Zum Erstellen des Option-Tags 167 Wyse Management Suite CA-Validation-Server-URL gehen Sie wie folgt vor:

1. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
   - Name – CA-Validation
   - Datentyp – Zeichenfolge
   - Code – 167
   - Name – CA-Validation
2. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.

   Zeichenfolge –WAHR/FALSCH

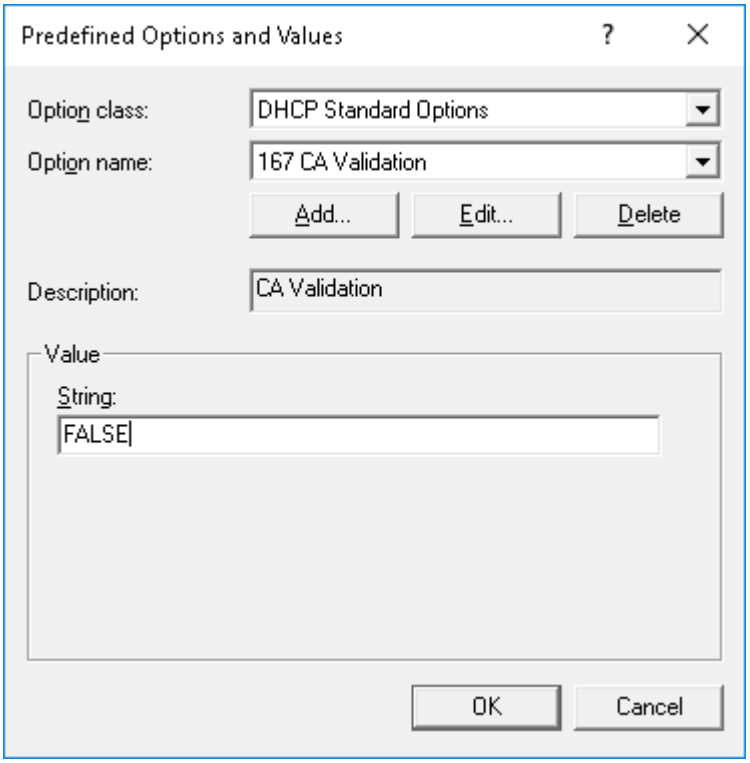


**Abbildung 24. Option-Tag 167 Wyse Management Suite Server-URL**

- Zum Erstellen des Option-Tags 199 Wyse Management Suite Gruppentoken-Server-URL gehen Sie wie folgt vor:

1. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
   - Name – Gruppentoken
   - Datentyp – Zeichenfolge
   - Code – 199
   - Beschreibung – Gruppentoken
2. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.

   Zeichenfolge – defa-Quarantäne

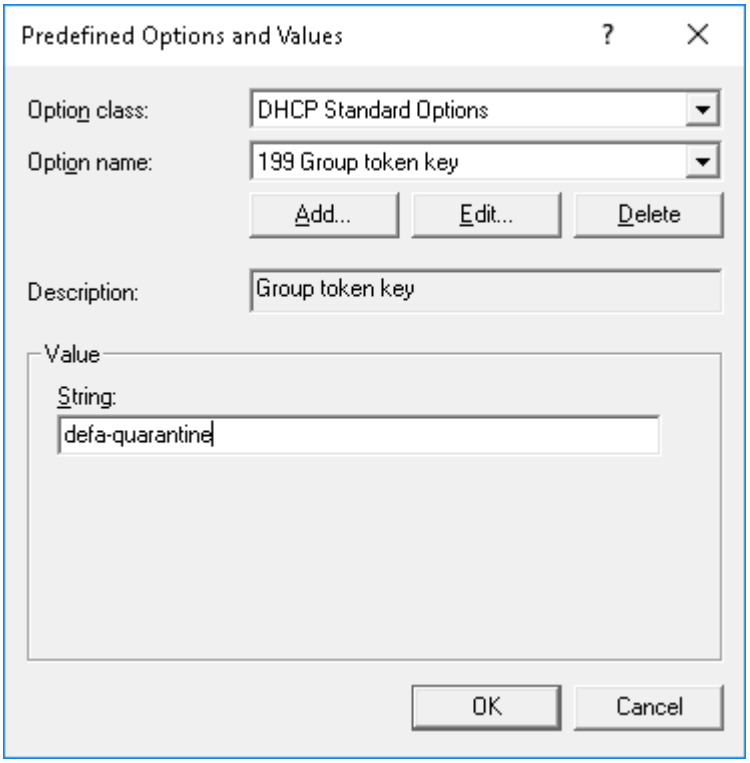


**Abbildung 25. Option-Tag 199 Wyse Management Suite Server-URL**

E

# Erstellen und Konfigurieren von DNS-SRV-Einträgen

**Info über diese Aufgabe**

**ANMERKUNG:** Weitere Informationen zur Sicherheitsumgebung für Kunden finden Sie unter Wyse-Geräte-Agent.

Um einen DNS-SRV-Eintrag zu erstellen, gehen Sie wie folgt vor:

**Schritte**

1. Öffnen Sie den Server-Manager.
2. Gehen Sie zu **Tools** und klicken Sie auf **DNS-Option**.
3. Gehen Sie zu **DNS- DNS-Server-Host-Name Forward-Lookupzonen Domain _tcp** und klicken Sie mit der rechten Maustaste auf die **_tcp-Option**.

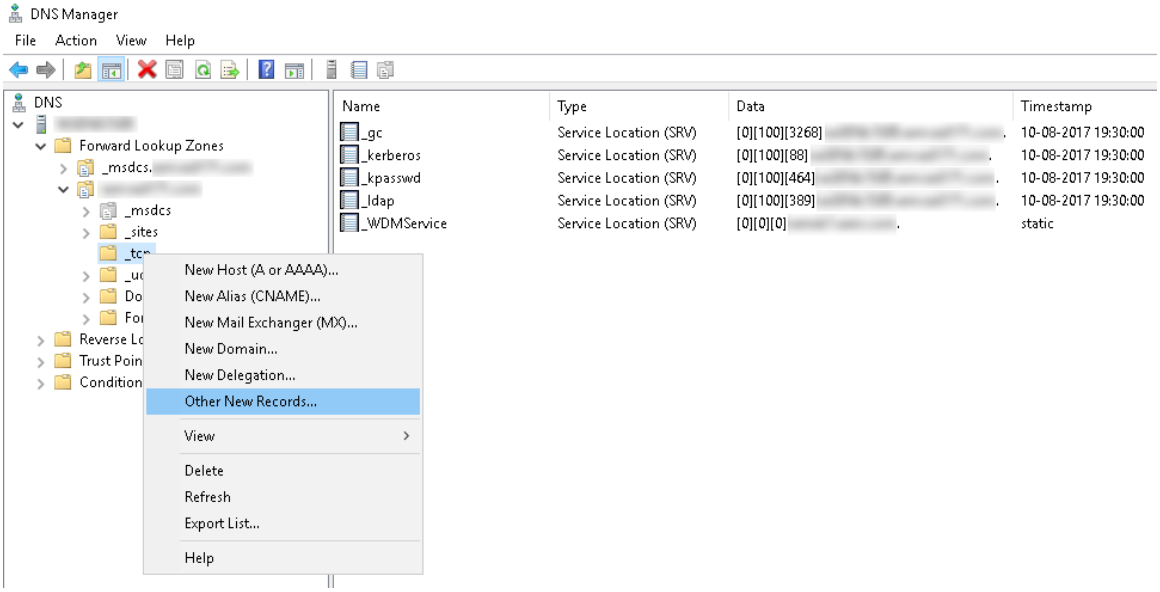


**Abbildung 26. DNS-Manager**

4. Klicken Sie auf **Andere neue Datensätze**.
   Das Fenster **Ressourcendatensatztyp** wird angezeigt.
5. Wählen Sie die **Dienstidentifizierung (SRV)**, klicken Sie auf **Datensatz erstellen** und führen Sie die folgenden Schritte aus:

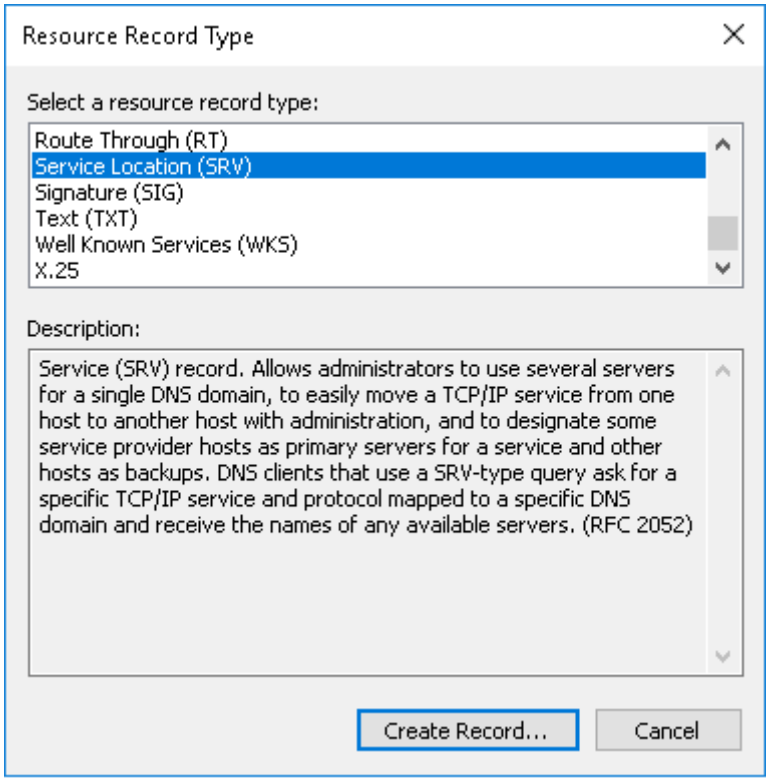


**Abbildung 27. Ressourcendatensatztyp**

a. Zum Erstellen eines Serverdatensatzes für die Wyse Management Suite, geben Sie die folgenden Informationen ein und klicken Sie auf **OK**.
   - Dienst–_WMS_MGMT
   - Protokoll–_tcp
   - Port-Nummer–443
   - Host, der diesen Dienst bietet–FQDN des WMS-Servers

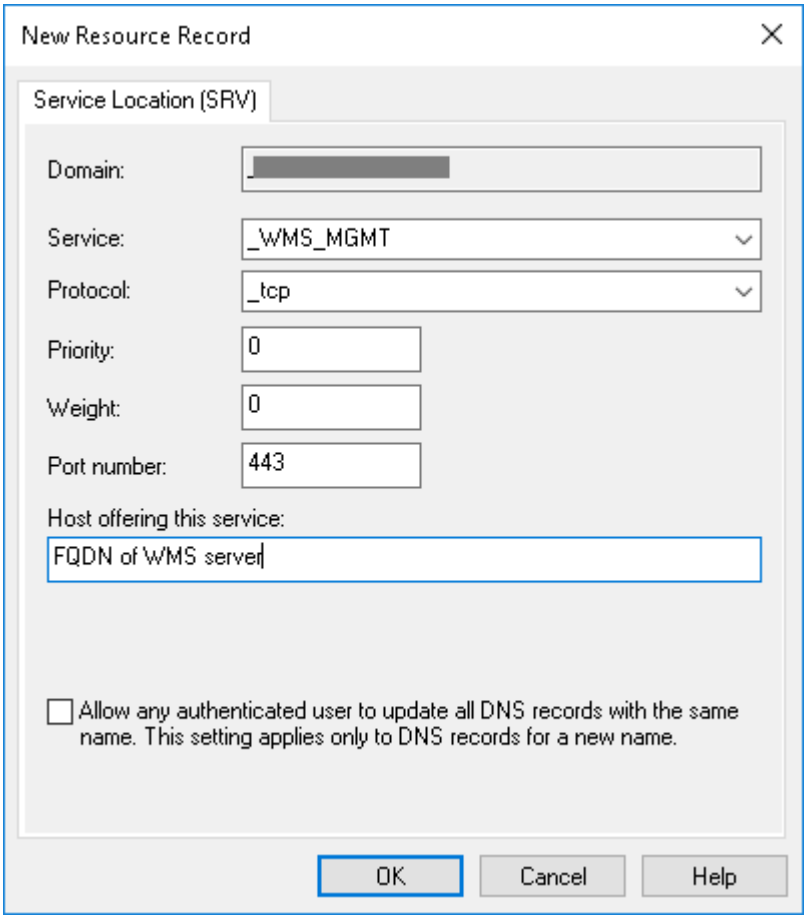


**Abbildung 28. _WMS_MGMT Service**

b. Zum Erstellen eines Serverdatensatzes für MQTT geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
   - Service-_WMS_MQTT
   - Protokoll–_tcp
   - Portnummer–1883.
   - Host, der diesen Dienst bietet–FQDN des MQTT-Servers

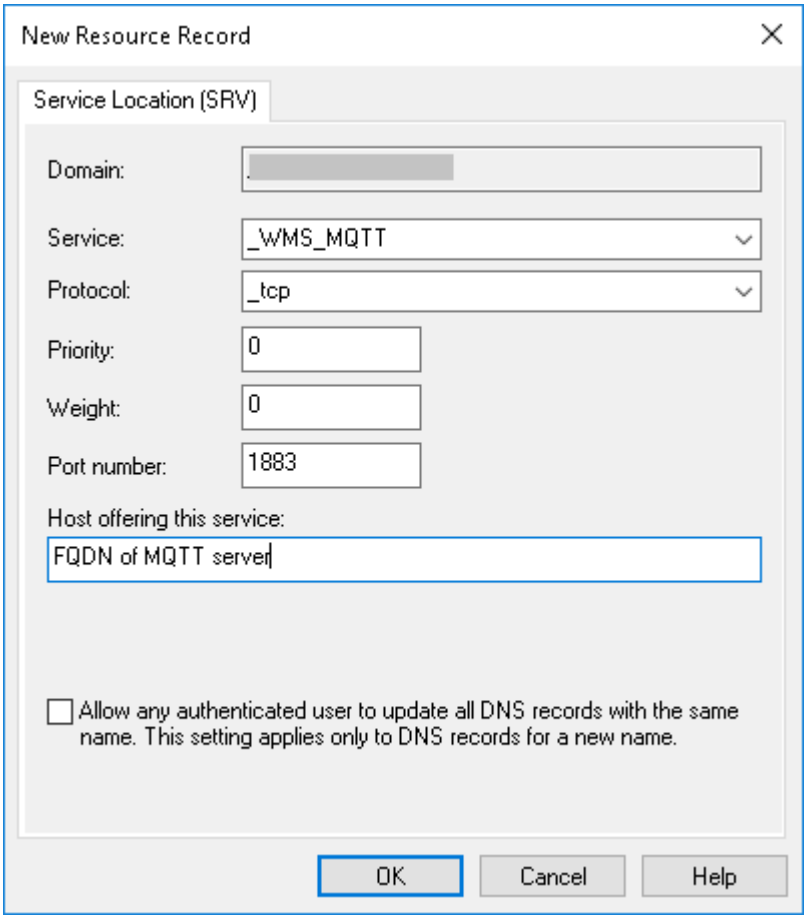


**Abbildung 29. _WMS_MQTT Service**

6. Gehen Sie zu **DNS DNS-Server-Host-Name Forward-Lookupzonen Domain** und klicken Sie mit der rechten Maustaste auf die Domain.
7. Klicken Sie auf **Andere neue Datensätze**.
8. Wählen Sie **Text (TXT)**, klicken Sie auf **Eintrag erstellen** und führen Sie die folgenden Schritte aus:

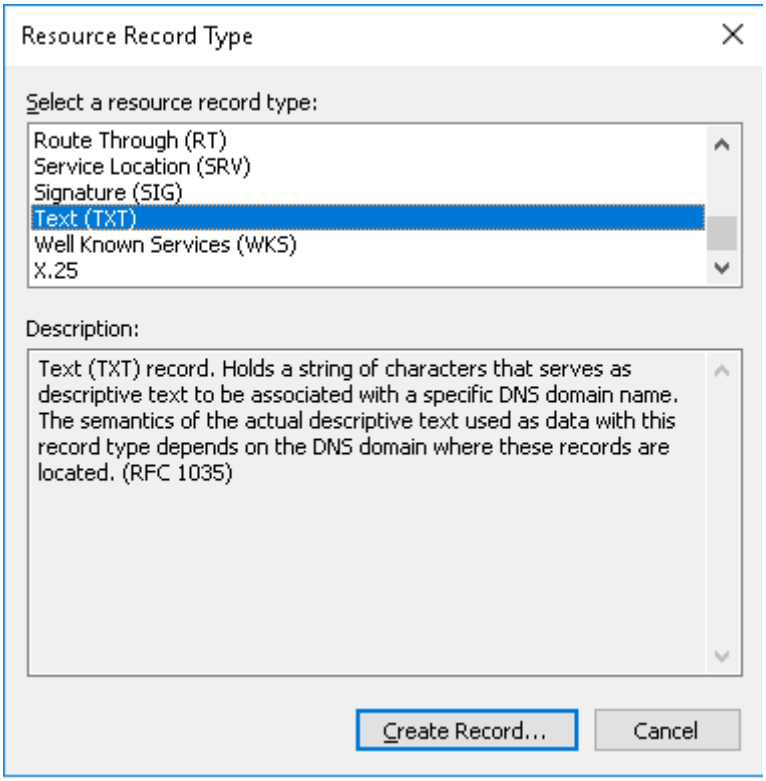


**Abbildung 30. Ressourcendatensatztyp**

a. Zum Erstellen eines Gruppentokens für die Wyse Management Suite, geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
   - Datensatzname—_WMS_GROUPTOKEN
   - Text–WMS Group token

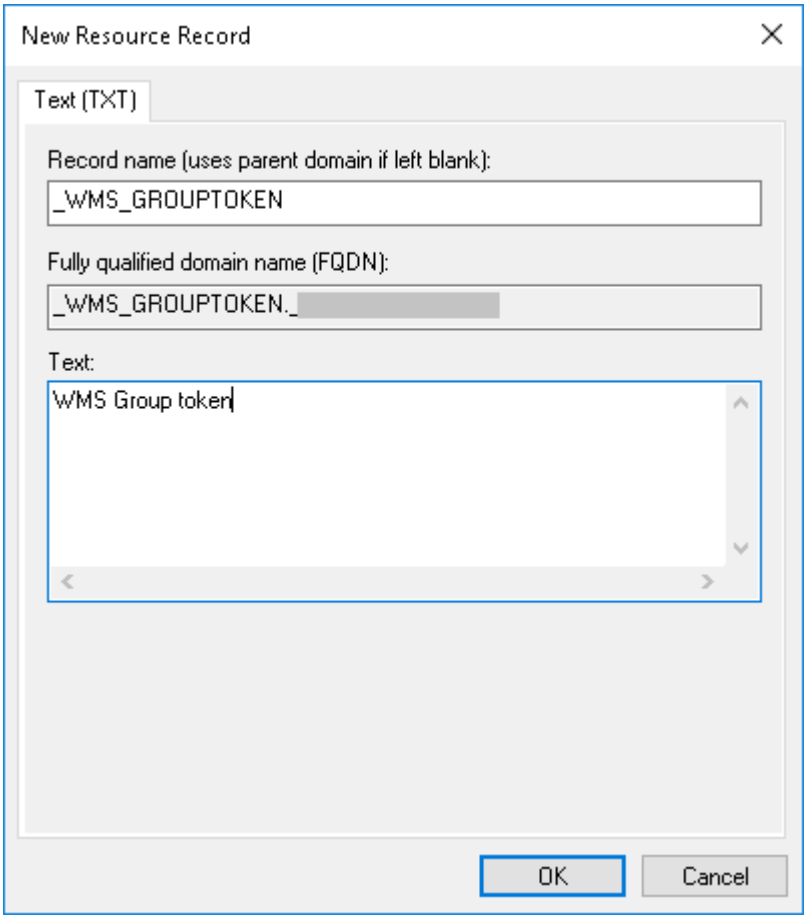


**Abbildung 31. _WMS_GROUPTOKEN Datensatzname**

b. Zum Erstellen eines CA-Validierungsdatensatzes für die Wyse Management Suite geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
   - Datensatzname–_WMS_CAVALIDATION
   - Text–TRUE/FALSE

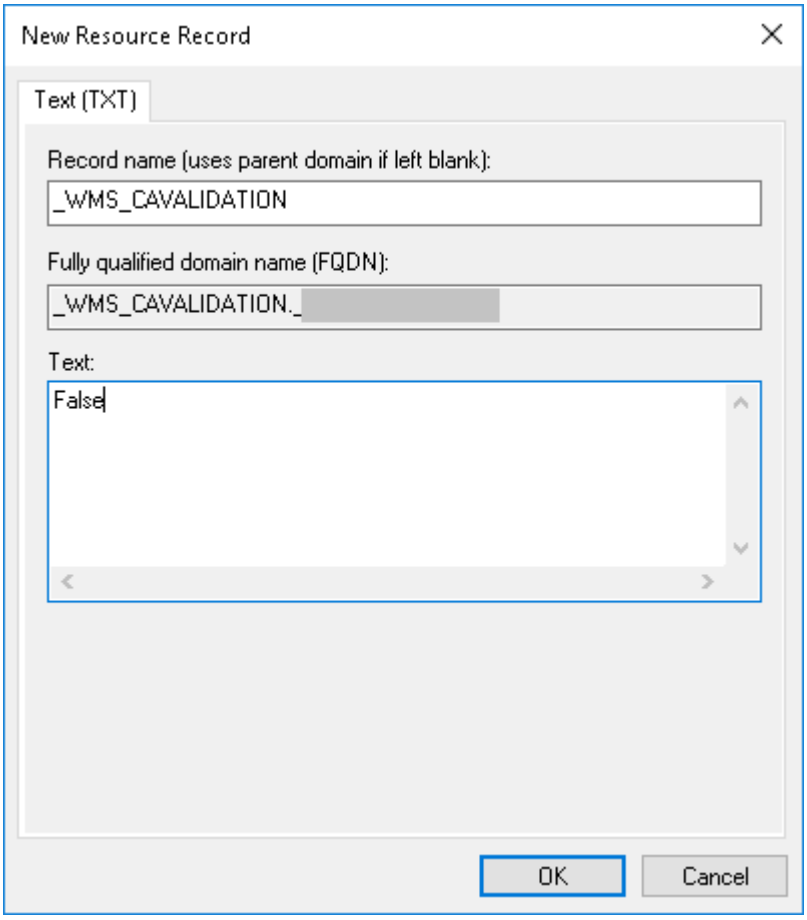


**Abbildung 32. _WMS_CAVALIDATION Datensatzname**

F

# Erstellen und Bereitstellen von Standardanwendungsrichtlinie für Thin Clients

**Info über diese Aufgabe**

So stellen Sie Thin Clients eine Standardanwendungsrichtlinie zur Verfügung:

**Schritte**

1. Gehen Sie im lokalen Repository zu **thinClientApps** und kopieren Sie die Anwendung in den Ordner.
2. Stellen Sie sicher, dass die Anwendung registriert ist, indem Sie zu **Apps & Daten** navigieren und **Thin Client** unter **App-Bestand** auswählen.

   **ANMERKUNG:** Die App-Bestand-Benutzeroberfläche benötigt etwa zwei Minuten, um alle kürzlich hinzugefügten Programme zu generieren.

3. Klicken Sie in den **App-Richtlinien** auf **Thin Client**.
4. Klicken Sie auf **Richtlinie hinzufügen**.
5. Geben Sie zum Erstellen einer Anwendungsrichtlinie die entsprechenden Informationen in das Fenster **Standard-App-Richtlinie hinzufügen** ein.
   - Wählen Sie **Richtlinienname**, **Gruppe**, **Task**, **Gerätetyp** und **TC-Anwendung** aus.
   - Um diese Policy für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter**, **Plattformfilter** oder **Herstellerfilter** aus. Das Timeout zeigt eine Meldung auf dem Client an, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt. Geben Sie an, wie viele Minuten lang das Meldungsdialogfeld auf dem Client angezeigt werden soll.
   - Um diese Richtlinie automatisch auf einem Gerät anzuwenden, das in der Wyse Management Suite registriert ist, wählen Sie **Richtlinie auf neue Geräte anwenden** aus der Drop-down-Liste **Richtlinie automatisch anwenden** aus.

   **ANMERKUNG:** Die App-Richtlinie wird angewendet, wenn ein beliebiges Gerät in die definierte Gruppe verschoben oder direkt in der Gruppe registriert wird. Wenn Sie **Richtlinie beim Check-In-Vorgang auf Geräte anwenden** auswählen wird die Richtlinie automatisch beim Einchecken in den Wyse Management Suite-Server auf das Gerät angewendet.

6. Um eine Verzögerung bei der Ausführung der Richtlinie zuzulassen, markieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Drop-down-Menüs aktiviert:
   - Wählen Sie aus dem Drop-down-Menü **Max. Anzahl an Stunden pro Verzögerung** die maximale Anzahl an Stunden aus (1 bis 24 Stunden), für die die Richtlinienausführung verzögert werden kann.
   - Wählen Sie aus dem Drop-down-Menü **Max. Verzögerungen** die maximale Anzahl an Stunden aus (1 bis 3 Stunden), für die die Richtlinienausführung verzögert werden kann.
7. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Timeout für Anwendungsinstallation** die Anzahl der Minuten an.
8. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.
   Eine Meldung wird angezeigt, um den Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu gewähren.
9. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen. Die App/Image-Richtlinienjob kann dann ausgeführt werden:
   - **Sofort** – Der Server führt den Job sofort aus.
   - **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
   - **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.
10. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
11. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

G

# Manuelles Registrieren von Dell Hybrid Clients

**Voraussetzungen**

Bevor Sie das Gerät registrieren, stellen Sie sicher, dass Ihr Gerät über eine Netzwerkverbindung verfügt, damit der Wyse Management Suite Server kontaktiert werden kann.

**ANMERKUNG:** Sie können das Gerät nur über das Gastnutzerkonto registrieren bzw. die Registrierung aufheben.

**Schritte**

1. Melden Sie sich beim Hybrid Client als Gastnutzer an.
2. Klicken Sie in der oberen Leiste auf das Symbol **Dell Client Agent**.

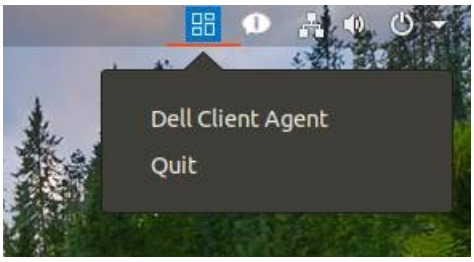


**Abbildung 33. DCA-Symbol**

3. Klicken Sie auf **Dell Client Agent**.
   Das Dialogfeld **Dell Client Agent** wird angezeigt.
4. Klicken Sie auf **Registrierung**.
   Der Standardstatus wird als **Ermittlung wird durchgeführt** angezeigt.
5. Klicken Sie zum manuellen Registrieren auf **Abbrechen**.
6. Geben Sie im Feld **WMS-Server** die URL des Wyse Management Suite Servers ein.
7. Geben Sie in das Feld **Gruppentoken** ein Gruppen-Registrierungsschlüssel ein. Das Gruppentoken ist ein eindeutiger Schlüssel für die direkte Registrierung Ihrer Geräte bei Gruppen.

   **ANMERKUNG:** Wenn die Felder für Mandant und Gruppe leer sind, wird das Gerät in der nicht verwalteten Gruppe registriert. Das Gruppentoken ist jedoch zwingend erforderlich, um das Gerät in einer öffentlichen Cloud zu registrieren.

8. Klicken Sie auf die Schaltfläche **EIN/AUS**, um die Option **Serverzertifikat-CA validieren** zu aktivieren bzw. zu deaktivieren. Aktivieren Sie diese Option, um die Validierung des Serverzertifikats für die gesamte Kommunikation zwischen Geräten und Servern durchzuführen.

   Die A-Validierungsoption wird automatisch aktiviert und kann nicht deaktiviert werden, wenn eine Public-Cloud-URL eingegeben wurde.

9. Klicken Sie auf **Registrieren**, um Ihren Hybrid Client auf dem Wyse Management Suite Server zu registrieren.

   Wenn der Hybrid-Client erfolgreich registriert wurde, wird der Status als **Registriert** angezeigt, wobei neben der Bezeichnung **Registrierungsstatus** die Option grün markiert ist. Die Beschriftung der Schaltfläche **Registrieren** ändert sich zu **Registrierung aufheben**.

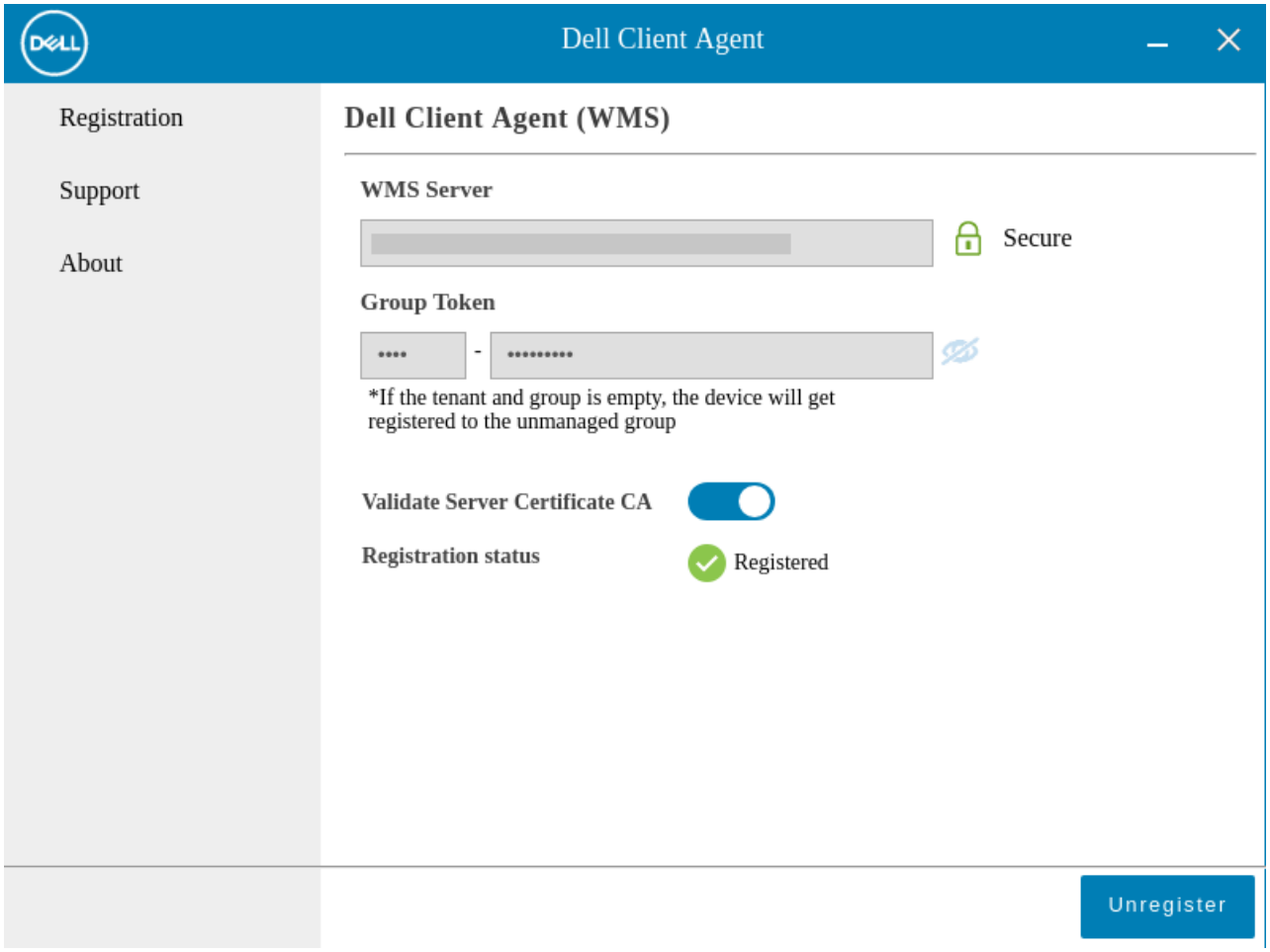


Abbildung 34. Dell Client Agent

H

# Windows Embedded Standard-Gerät manuell registrieren

Windows Embedded Standard-Geräte können manuell durch Starten des **WDA-UI** Symbols in der Taskleiste registriert werden.

1. Wählen Sie **Wyse Management Suite-WMS** als Verwaltungsserver aus.
2. Geben Sie einen geeigneten Mandanten und Gruppennamen ein. Wenn dieses Feld leer gelassen wird, werden die Geräte in einer nicht verwalteten Gruppe registriert. (Optional)
3. Klicken Sie auf **Registrieren**.

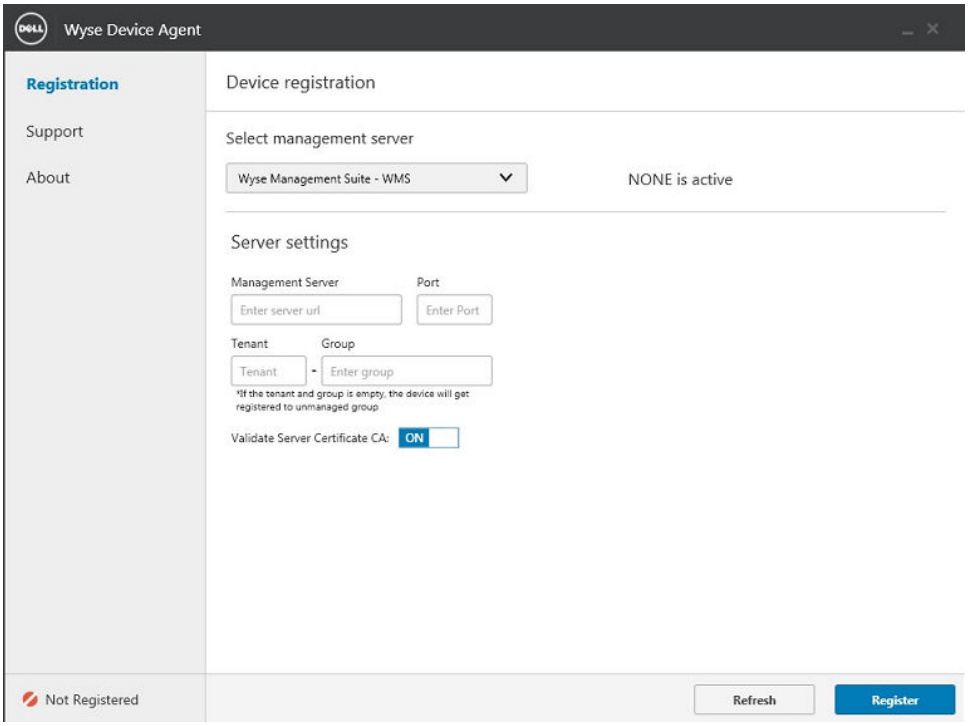


**Abbildung 35. Geräteregistrierung**

# ThinOS 8.x-Gerät manuell registrieren

**Schritte**

1. Klicken Sie im Desktopmenü auf **System-Setup** > **Zentrale Konfiguration**.
   Das Fenster **Zentrale-Konfiguration** wird angezeigt.
2. Geben Sie den für die gewünschte Gruppe von Ihrem Administrator konfigurierten **Gruppenregistrierungsschlüssel** ein.
3. Wählen Sie das Kontrollkästchen **Erweiterte WMS-Einstellungen aktivieren** aus.
4. Geben Sie im Feld **WMS-Server** die URL des Wyse Management-Servers ein.
5. Aktivieren oder deaktivieren Sie die CA-Validierung abhängig von Ihrem Lizenztyp. Aktivieren Sie für die öffentliche Cloud das Kontrollkästchen **CA-Validierung aktivieren**. Wählen Sie bei einer privaten Cloud das Kontrollkästchen **CA-Validierung aktivieren** aus, wenn Sie Zertifikate von einer bekannten Zertifizierungsstelle in Ihren Wyse Management Suite-Server importiert haben.

   Um die CA-Validierungsoption in der Private Cloud zu aktivieren, müssen Sie dasselbe selbstsignierte Zertifikat auch auf dem ThinOS Gerät installieren. Wenn Sie das selbstsignierte Zertifikat nicht auf dem ThinOS-Gerät installiert haben, wählen Sie nicht das Kontrollkästchen **CA-Validierung aktivieren** aus. Sie können das Zertifikat mithilfe der Wyse Management Suite nach der Registrierung auf dem Gerät installieren und anschließend die CA-Validierungsoption aktivieren.
6. Klicken Sie auf **Schlüssel validieren**, um das Setup zu überprüfen.

   **ANMERKUNG:** Wenn der Schlüssel nicht validiert wird, überprüfen Sie den Gruppenschlüssel und die WMS-Server-URL, den bzw. die Sie angegeben haben. Stellen Sie sicher, dass die genannten Ports nicht durch das Netzwerk blockiert werden. Die Standardports sind 443 und 1883.
7. Klicken Sie auf **OK**.

   **ANMERKUNG:** Wenn die Option zur **Anmeldungsvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Anmeldungsvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Anmeldung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben.

   Das Gerät wird in der Wyse Management Suite registriert.

J

# ThinOS 9.x-Gerät manuell registrieren

**Schritte**

1. Klicken Sie im Desktopmenü auf **System-Setup** > **Zentrale Konfiguration**.
   Das Fenster **Zentrale-Konfiguration** wird angezeigt.
2. Geben Sie den für die gewünschte Gruppe von Ihrem Administrator konfigurierten **Gruppenregistrierungsschlüssel** ein.
3. Wählen Sie das Kontrollkästchen **Erweiterte WMS-Einstellungen aktivieren** aus.
4. Geben Sie im Feld **WMS-Server** die URL des Wyse Management-Servers ein.
5. Aktivieren oder deaktivieren Sie die CA-Validierung abhängig von Ihrem Lizenztyp. Public Cloud: Wählen Sie das Kontrollkästchen **CA-Validierung aktivieren** aus. Private Cloud: Wählen Sie das Kontrollkästchen **CA-Validierung aktivieren** aus, wenn Sie Zertifikate von einer bekannten Zertifizierungsstelle in Ihren Wyse Management Suite-Server importiert haben.

   Um die CA-Validierungsoption in der Private Cloud zu aktivieren, müssen Sie dasselbe selbstsignierte Zertifikat auch auf dem ThinOS Gerät installieren. Wenn Sie das selbstsignierte Zertifikat nicht auf dem ThinOS-Gerät installiert haben, wählen Sie nicht das Kontrollkästchen **CA-Validierung aktivieren** aus. Sie können das Zertifikat mithilfe der Wyse Management Suite nach der Registrierung auf dem Gerät installieren und anschließend die CA-Validierungsoption aktivieren.
6. Klicken Sie auf **Schlüssel validieren**, um das Setup zu überprüfen.

   **ANMERKUNG:** Wenn der Schlüssel nicht validiert wird, überprüfen Sie den Gruppenschlüssel und die WMS-Server-URL, den bzw. die Sie angegeben haben. Stellen Sie sicher, dass die genannten Ports nicht durch das Netzwerk blockiert werden. Die Standardports sind 443 und 1883.

   Es wird ein Benachrichtigungsfenster angezeigt.
7. Klicken Sie auf **OK**.
8. Klicken Sie im Fenster **Zentrale Konfiguration** auf **OK**.

   **ANMERKUNG:** Wenn die Option zur **Anmeldungsvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Anmeldungsvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Anmeldung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben.

   Das Gerät wird in der Wyse Management Suite registriert.

K

# Linux Gerät manuell registrieren

Linux Geräte können manuell durch Starten des **WDA-UI** Symbols in den **Systemeinstellungen** registriert werden.

1. Geben Sie die **WMS-Server**-Informationen ein.
2. Geben Sie einen geeigneten Mandanten und Gruppennamen ein. Wenn dieses Feld leer gelassen wird, werden die Geräte in einer nicht verwalteten Gruppe registriert. (Optional)
3. Klicken Sie auf **Registrieren**.

   Das Gerät wird in der Wyse Management Suite-Konsole registriert.

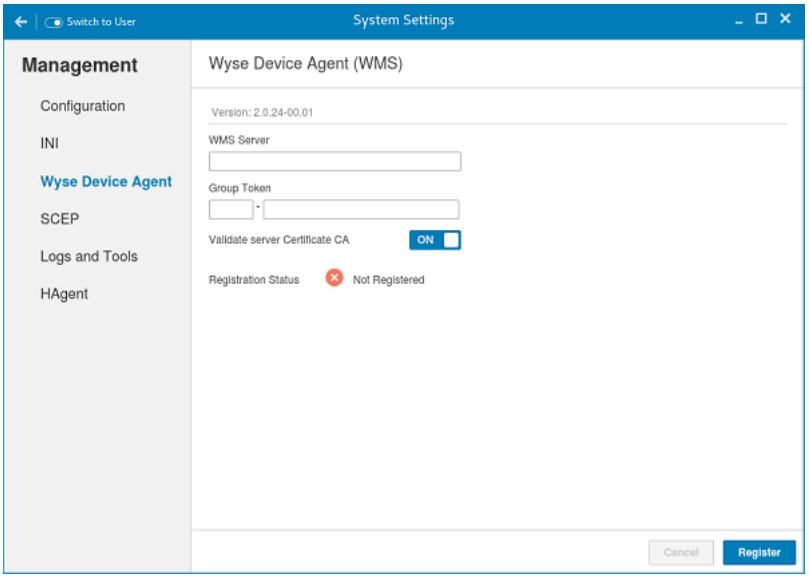


**Abbildung 36. Geräteregistrierung**

# L

# Begriffe und Definitionen

In der folgenden Tabelle sind die Begriffe aufgeführt, die in diesem Dokument verwendet werden sowie deren Definitionen.

**Tabelle 7. Begriffe und Definitionen**

| Terminologie | Definition |
|---|---|
| Private Cloud | Wyse Management Suite-Server, der in der Cloud installiert ist, die für das Datencenter Ihrer Organisation privat ist. |
| WDA | Wyse Device Agent, der im Gerät sitzt und als Agent für die Kommunikation zwischen Server und Client dient. |
| Lokales Repository | Wyse Device Agent, der im Gerät sitzt und als Agent für die Kommunikation zwischen Server und Client dient. |
| Remote-Repository | Anwendung, Betriebssystemimage und Datei-Repositorys, die optional zur Skalierbarkeit und Zuverlässigkeit über alle Standorte für Übertragungsinhalte installiert werden können. |
| Öffentliche Cloud | Wyse Management Suite, die in einer öffentlichen Cloud gehostet wird, wodurch die Infrastruktur und Software nicht eingerichtet und gewartet werden müssen, was Prozesse verschlankt und für Kosteneinsparungen sorgt. |
| Add-On/App | Eine beliebige Komponente bzw. ein beliebiges Paket, das nicht Teil des Basis-Builds ist und als eine optionale Komponente dient. Die Komponente oder das Paket kann mit der Verwaltungssoftware bereitgestellt werden. Zum Beispiel die aktuellen Verbindungsbroker von VMware und Citrix |
| Lokal | Wyse Management Suite-Server, der lokal installiert ist, die für das Datencenter Ihrer Organisation privat ist. |
| Mandant | Eine Gruppe von Benutzern, die sich einen gemeinsamen Zugriff mit spezifischen Berechtigungen für die Wyse Management Suite teilen. Es handelt sich um einen eindeutigen Schlüssel, der bestimmten Kunden für den Zugriff auf die Verwaltungssuite zugewiesen ist. |
| Benutzer | Benutzer können lokale Administratoren, globale Administratoren und Viewer sein. Gruppenbenutzer und Benutzer, die aus dem Active Directory importiert wurden, können für die Anmeldung in der Wyse Management Suite Rollen als globaler Administrator und Gruppenadministrator sowie Viewer zugewiesen werden. Benutzer erhalten Berechtigungen zum Ausführen von Vorgängen auf Basis der ihnen zugewiesenen Rollen. |