

Dell Wyse Management Suite

Version 2.x – Schnellstarthandbuch



Anmerkungen, 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.

© 2020 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder Tochterunternehmen. Andere Markennamen sind möglicherweise Marken der entsprechenden Inhaber.

Inhaltsverzeichnis

1 Einführung	5
2 Erste Schritte mit der Wyse Management Suite	6
Anmelden bei der Wyse Management Suite in einer öffentlichen Cloud	6
Voraussetzungen für Wyse Management Suite in einer privaten Cloud	7
3 Installieren von Wyse Management Suite in privater Cloud	8
Anmelden bei der Wyse Management Suite	15
Funktionsbereiche der Verwaltungskonsole	15
Konfigurieren und Verwalten von Thin Clients	15
Erstellen von Richtliniengruppe und aktualisieren der Konfiguration	16
Registrieren eines neuen Thin Clients	17
ThinOS Gerät manuell registrieren	17
Registering devices by using DHCP option tags	19
Geräte mit DNS-SRV-Eintrag registrieren	20
4 Bereitstellen von Anwendungen auf Thin Clients	22
Hochladen und Bereitstellen von ThinOS-Firmware-Image-Beständen	22
Erstellen und Bereitstellen von Standardanwendungsrichtlinie für Thin Clients	22
5 Deinstallieren der Wyse Management Suite	24
6 Beheben von Fehlern in der Wyse Management Suite	25
7 Wyse-Geräte-Agent	27
8 Weitere Ressourcen	28
Anhang A: Remote-Datenbank	29
Configure Mongo database	29
Configure Maria database	30
Anhang B: Benutzerdefinierte Installation	31
Anhang C: Wyse Management Suite-Funktionsmatrix	36
Anhang D: Zugreifen auf Wyse Management Suite Datei-Repository	38
Anhang E: Erstellen und Konfigurieren von DHCP-Options-Tags	40
Anhang F: Erstellen und Konfigurieren von DNS-SRV-Einträgen	46
Anhang G: Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients	53

Anhang H: Windows Embedded Standard-Gerät manuell registrieren.....	54
Anhang I: ThinOS 8.x-Gerät manuell registrieren.....	55
Anhang J: ThinOS 9.x-Gerät manuell registrieren.....	56
Anhang K: Linux Gerät manuell registrieren.....	57
Anhang L: Begriffe und Definitionen.....	58

Einführung

Die Wyse Management Suite ist die Verwaltungslösung der nächsten Generation, mit der Sie Ihre Dell Wyse Thin Clients zentral konfigurieren, überwachen, verwalten und optimieren können. Die neue Suite macht es einfacher, Thin Clients mit hoher Funktionalität und Leistung sowie Bedienungsfreundlichkeit zu implementieren und zu verwalten. Sie bietet außerdem erweiterte Funktionsoptionen, z. B. Cloud versus lokale Bereitstellung, von überall mit einer mobilen Anwendung verwalten, erweiterte Sicherheit wie die BIOS-Konfiguration und Port-Sperrung. Zu den weiteren Funktionen gehören die Suche nach Geräten und Registrierung, Bestands- und Lagerverwaltung, Konfigurationsverwaltung, Bereitstellung von Betriebssystemen und Anwendungen, Echtzeitbefehle, Überwachung, Warnungen, Berichterstellung und Fehlerbehebung von Endpunkten.

Editionen

Wyse Management Suite ist in den folgenden Editionen erhältlich:

- **Standard (Kostenlos)** – Die Standard-Edition der Wyse Management Suite ist nur für eine lokale Bereitstellung verfügbar. Sie benötigen zur Verwendung der Standardedition keinen Lizenzschlüssel. Die Standardedition eignet sich für kleine und mittelständische Unternehmen.
- **Pro (kostenpflichtig)** – Die Pro-Edition der Wyse Management Suite kann sowohl in der privaten als auch in der öffentlichen Cloud bereitgestellt werden. Die Pro-Edition verwendet abonnementbasierte Lizenzierungen und erfordert einen Lizenzschlüssel. Mit der Pro-Lösung können Organisationen ein Hybridmodell annehmen und ihre Lizenzen sowohl lokal als auch in der Cloud verwenden. Die lokale Pro-Edition eignet sich für kleine, mittelständische und große Unternehmen. Für eine Cloud Bereitstellung kann die Pro-Edition Ihre Geräte auf nicht-Firmennetzwerken (Home-Office, Drittanbieter, Partnern, mobile Thin Clients usw.) verwalten. Die Pro-Edition der Wyse Management Suite bietet außerdem:
 - Eine mobile Anwendung, um in Echtzeit kritische Warnungen und Benachrichtigungen zu sehen und Befehle zu senden.
 - Verbesserte Sicherheit durch Zweifaktor-Authentifizierung und Active Directory-Authentifizierung für rollenbasierte Verwaltung.
 - Erweiterte App-Richtlinie und -Berichterstellung

ANMERKUNG:

- **Cloud-Dienste 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.**

Weitere Informationen zu den in der Standard- und Pro-Edition unterstützten Funktionen finden Sie in der [Funktionsmatrix](#).

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 öffentlichen Cloud](#)
- [Voraussetzungen für Wyse Management Suite in einer privaten Cloud](#)

Anmelden bei der Wyse Management Suite in einer öffentlichen 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 öffentliche Cloud (SaaS) Edition der Wyse Management Suite mithilfe einer der folgenden Links zu:
 - **US-Datenzentrum** –us1.wysemanagementsuite.com/ccm-web
 - **EU-Datenzentrum** –eu1.wysemanagementsuite.com/ccm-web
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
3. Klicken Sie auf **Anmelden**.

ANMERKUNG: Wenn Sie sich zum ersten Mal bei der Wyse Management Suite Konsole anmelden, wenn ein neuer Benutzer hinzugefügt wird oder wenn eine Benutzerlizenz erneuert wird, wird die Seite Geschäftsbedingungen angezeigt. Lesen Sie die Geschäftsbedingungen, 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 öffentlichen Cloud installiert werden. Zudem muss der vollständig qualifizierte Domainname (FQDN) des Servers im öffentlichen DNS registriert werden.

Ändern Ihres Kennworts

Zum Ändern des Anmeldekennworts klicken Sie auf den Link "Konto" in der oberen rechten Ecke der Verwaltungskonsole und klicken Sie dann auf **Kennwort ändern**.

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

Abmelden bei der Wyse Management Suite

Zum Abmelden von der Verwaltungskonsole klicken Sie auf den Link "Konto" in der oberen rechten Ecke der Verwaltungskonsole und klicken Sie dann auf **Abmelden**.

Voraussetzungen für Wyse Management Suite in einer privaten Cloud

Tabelle 1. Vorbedingungen

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. 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	<p>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.</p> <ul style="list-style-type: none"> • TCP 443 – HTTPS-Kommunikation • TCP 1883 – MQTT-Kommunikation • TCP 3306 – MariaDB (optional, wenn Remote) • TCP 27017 – MongoDB (optional, wenn Remote) • TCP 11211 – Memcache • TCP 5172, 49159 – End-User Management Software Development Kit (EMSDK) – optional und nur für Teradici Geräte erforderlich <p>Die Standardschnittstellen, die vom Installationsprogramm verwendet werden, können im Rahmen der Installation zu einem alternativen Port geändert werden.</p>			<p>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.</p>
Unterstützte Browser	<p>Internet Explorer Version 11</p> <p>Google Chrome, Version 58.0 und höher</p> <p>Mozilla Firefox ,Version 52.0 und höher</p> <p>Edge-Browser unter Windows – nur in englischer Sprache</p>			

- 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.

i ANMERKUNG: WMS.exe und WMS_Repo.exe müssen auf zwei verschiedenen Servern installiert werden. Sie müssen das Wyse Management Suite Remote-Repository für die öffentliche 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. Weitere Informationen finden Sie unter [Zugriff auf das Datei-Repository](#).

Installieren von Wyse Management Suite in privater Cloud

Um die Wyse Management Suite in einer privaten Cloud einrichten zu können, müssen die folgenden Anforderungen erfüllt werden:

- 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 Anmeldeinformationen 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.

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/.

So installieren Sie die Wyse Management Suite in einer privaten Cloud:

1. Doppelklicken Sie auf das Installationspaket.
2. Lesen Sie auf dem **Willkommen**-Bildschirm die Lizenzvereinbarung und klicken Sie auf **Weiter**.
3. 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 Benutzerinteraktion und installiert eingebettete Datenbanken.
 - Benutzerdefiniert – erfordert maximale Benutzerinteraktion und wird für fortgeschrittene Benutzer empfohlen. Weitere Informationen finden Sie unter [Benutzerdefinierte 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 IE-Konfiguration Erhöhte Sicherheit 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.

4. Wählen Sie **Typisch** als **Setup-Typ** aus. Geben Sie die neuen **Datenbank-Anmeldeinformationen** für die eingebetteten Datenbanken an. Geben Sie darüber hinaus auch die neuen **Administrator-Anmeldeinformationen** ein und klicken Sie auf **Weiter**.

ANMERKUNG: Die Administrator-Anmeldeinformationen sind erforderlich, um sich nach der Installation in der Wyse Management Suite-Webkonsole anmelden zu können.
5. Auf der Seite **Konfiguration** 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 die Teradici EM SDK Option auf der Setup-Typ Seite aktiviert ist, können Sie den Port für den Teradici-Server auf der Seite Konfiguration konfigurieren.
6. Wählen Sie einen Pfad aus, um die Software zu installieren, einen Pfad zum Installieren des lokalen Mandanten-Datei-Repositorys und klicken Sie dann auf **Weiter**.

Der Standardpfad des Zielordners für die Installation der Software ist C:\Program Files\DELL\WMS.

7. Klicken Sie auf **Weiter**.

Die Seite **Vorinstallations-Zusammenfassung** wird angezeigt.

8. Klicken Sie auf **Weiter**, um die Software zu installieren.

Das Installationsprogramm benötigt etwa 4–5 Minuten, um die Installation abzuschließen. Es kann jedoch länger dauern, wenn abhängige Komponenten, wie VC-Runtime, nicht auf dem System installiert sind.

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

10. Klicken Sie auf der Webkonsole auf **Erste Schritte**.

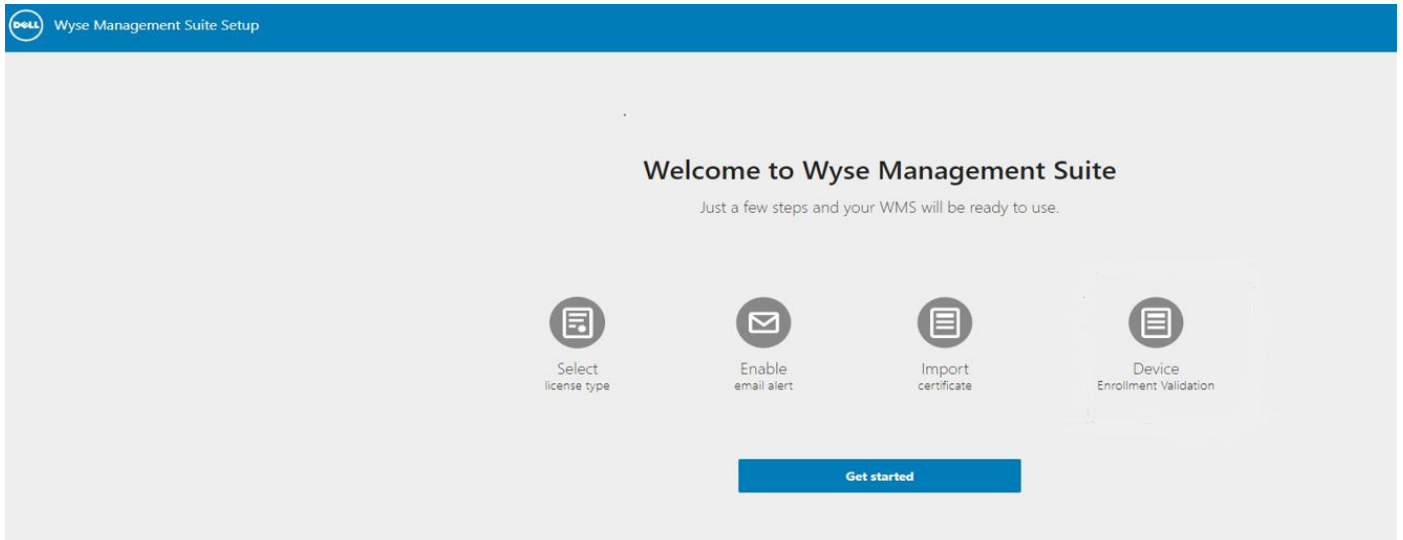


Abbildung 1. Startseite

11. Wählen Sie Ihre bevorzugte Lizenz aus.

- Wenn Sie den Lizenztyp als **Standard** auswählen und dann auf **Weiter** klicken, um mit der Standard Wyse Management Suite Installation fortzufahren.
- 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 Öffentliche-Cloud-Portal der Wyse Management Suite anmelden und den Schlüssel in das Feld "Lizenzschlüssel" eingeben.

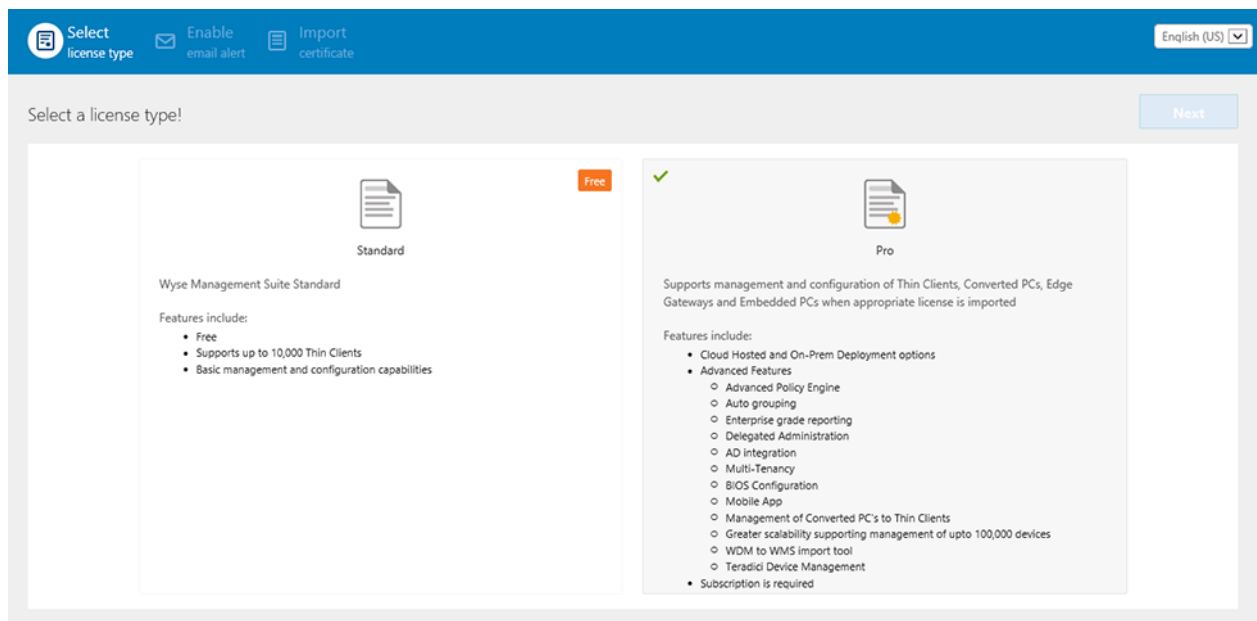


Abbildung 2. Lizenztyp

Enter license information ?

Enter your credentials to import licensing information ?

Username

Password

Data center

Number of TC seats ?

Number of Edge Gateway & Embedded PC seats ?

Number of Wyse Software Thin Client seats ?

Input your WMS Pro license key

License Key ?

OR

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**.

Console Settings

- Active Directory (AD)
- Alert Classification
- Edge Gateway & Embedded PC Registration
- External App Services
- File Repository
- Other Settings
- Thin Clients
- Two-Factor Authentication
- Reports

Account

- Custom Branding
- Subscription

License Subscription

License Type: Production
 Thin Client (Type/Exp): Production / Jun 1, 2019
 Wyse Software Thin Client (Type/Exp): Production / Jan 1, 2020
 Edge Gateway & Embedded PC (Type/Exp): Production / Dec 1, 2019

License Usage

Registered Thin Client devices

50
Manageable

24
In-Use

45
Used in Public Cloud
WMS

5
Used in Private Cloud
WMS

Registered Edge Gateways & Embedded PC devices

50
Manageable

0
In-Use

50
Used in Public Cloud
WMS

0
Used in Private Cloud
WMS

Registered Wyse Software Thin Client devices

50
Manageable

0
In-Use

50
Used in Public Cloud
WMS

0
Used in Private Cloud
WMS

Server Information:

Version: WMS 1.3.0 40874

Export License For Private Cloud

		Private Cloud	Public Cloud	Manageable
Number of TC seats	?	<input type="text"/>	45	50
Number of Edge Gateway & Embedded PC seats	?	<input type="text"/>	50	50
Number of Wyse Software Thin Client seats	?	<input type="text"/>	50	50

Export
WMS 1.1+ ▼

Abbildung 4. Portalverwaltung

- c. Geben Sie die Anzahl der Thin Client Plätze an.
- d. Klicken Sie auf **Exportieren**.

ANMERKUNG: Wählen Sie zum Exportieren der Lizenz WMS 1.1 oder WMS 1.0 aus der Dropdownliste aus.

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

- 12. 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.

- 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](https://www.geotrust.com) signiert wurde. Sie können entweder ein .pem oder .pfx-Zertifikat importieren.

Abbildung 6. Schlüssel- oder Zertifikatswertpaar

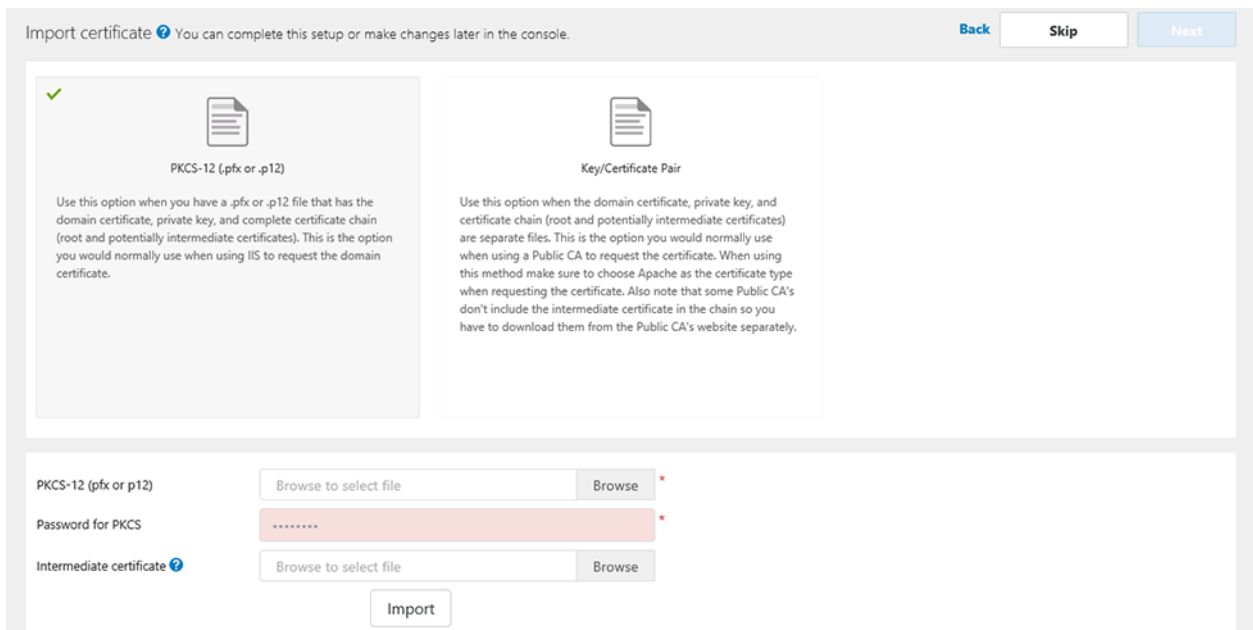


Abbildung 7. PKCS-12

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

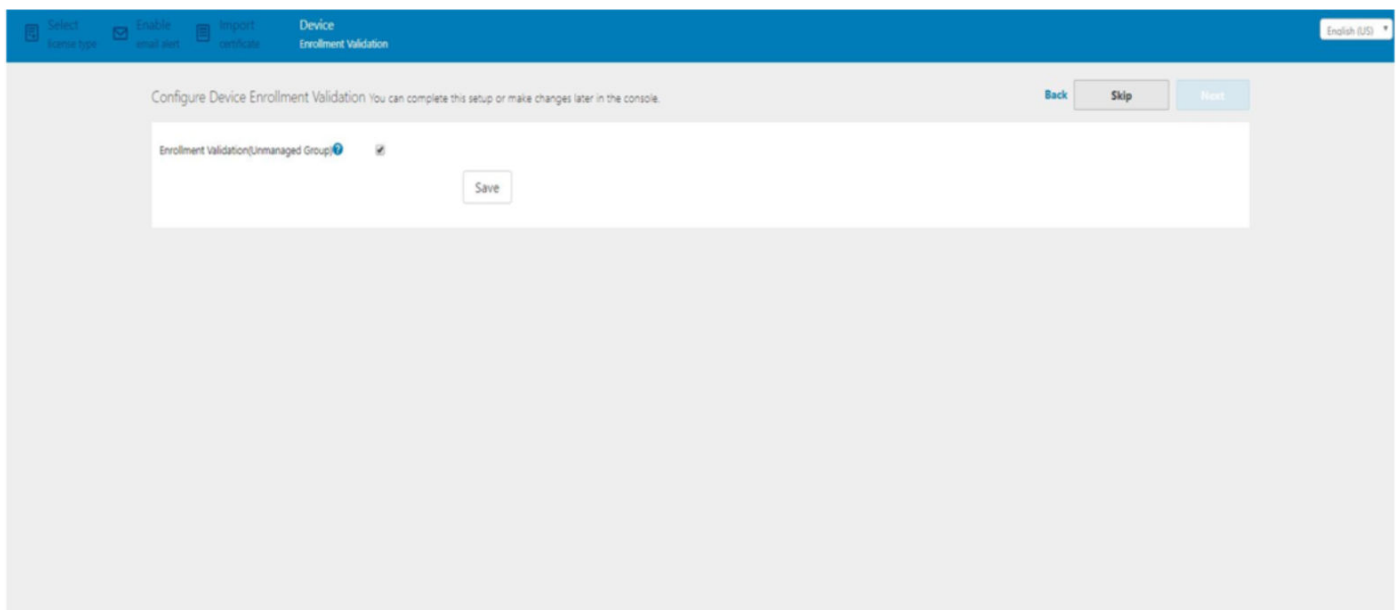


Abbildung 8. Anmeldungsvalidierung

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

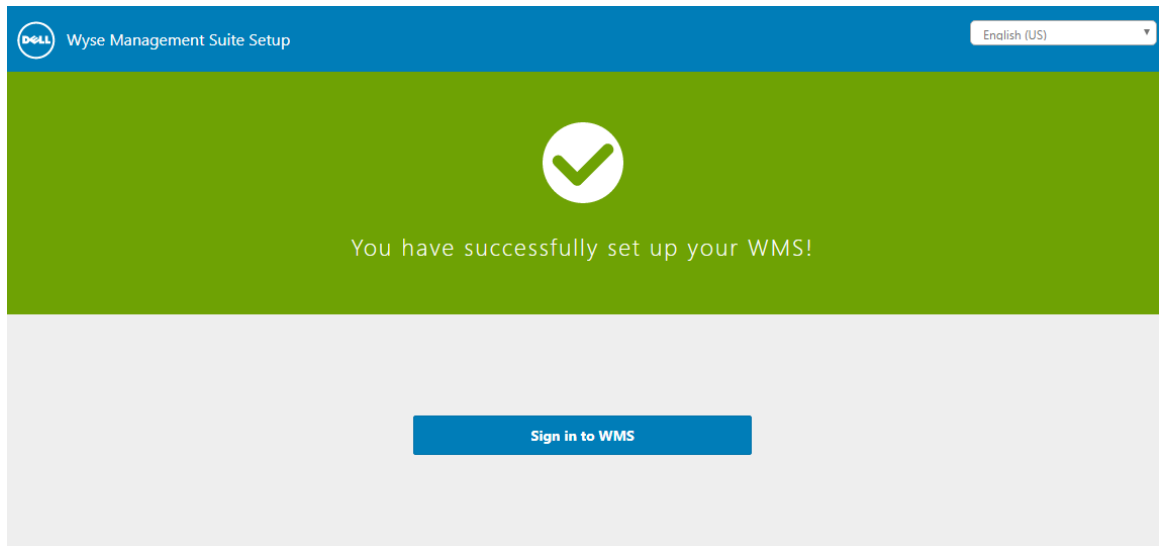


Abbildung 9. Anmeldeseite

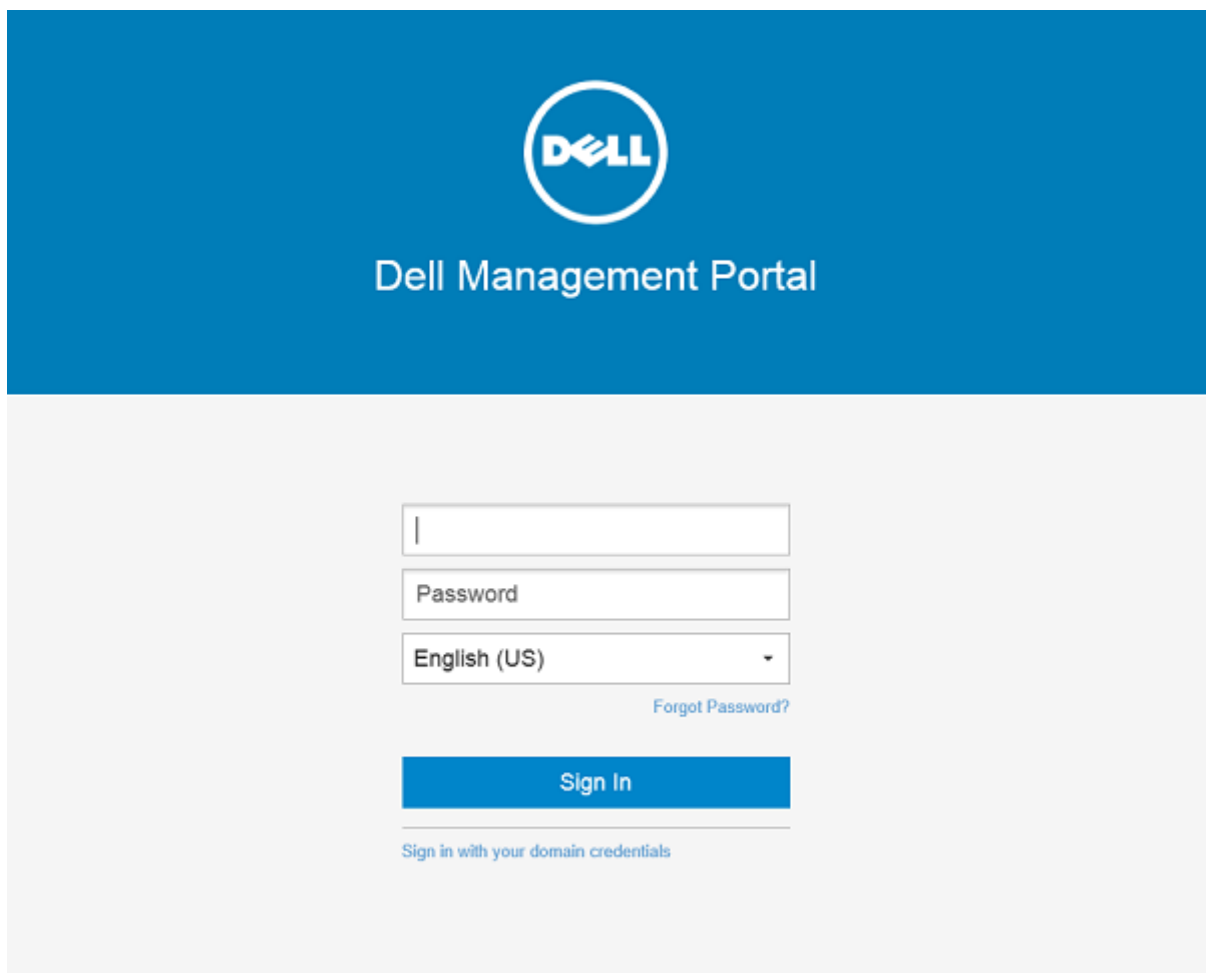


Abbildung 10. Dell Management Portal

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

So melden Sie sich bei der Verwaltungskonsole an:

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://wmserver.domain.com/ccm-web>, wobei [wmserver.domain.com](https://wmserver.domain.com/ccm-web) der qualifizierte Domänenname 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:

- 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 Repositories, 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 Geräteattributen 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-Installationskripten, 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:

- Melden Sie sich als Administrator an.
- So erstellen Sie eine Richtliniengruppe:
 - Wählen Sie **Gruppen und Konfigurationen** aus und klicken Sie auf die Schaltfläche **+** auf der linken Seite.
 - Geben Sie den Gruppennamen und die Beschreibung an.
 - Markieren Sie das Kontrollkästchen **Aktiviert**.
 - Geben Sie das Gruppentoken ein.
 - 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**.

i 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

i 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:

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.

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

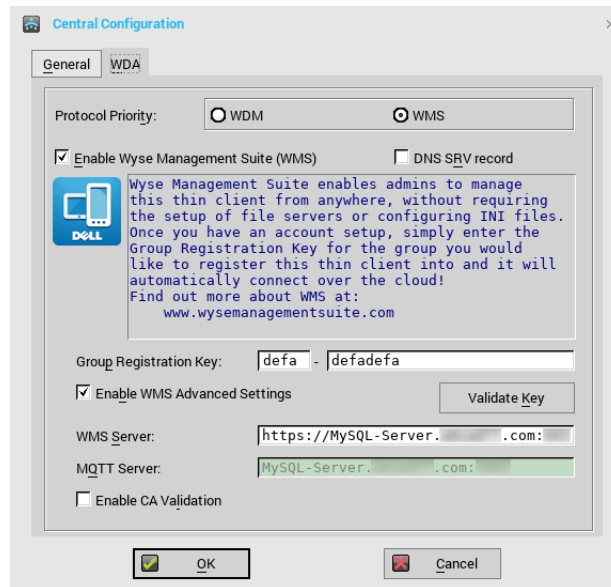


Abbildung 11. Zentrale Konfiguration

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.

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 2. Registrieren von Geräten mithilfe von DHCP-Options-Tags

Options-Tag	Beschreibung
<p>Name – WMS</p> <p>Datentyp – Zeichenfolge</p> <p>Code – 165</p> <p>Beschreibung – WMS-Server-FQDN</p>	<p>Dieses Tag verweist auf die Wyse Management Suite-Server-URL. Beispiel: <code>wmserver.acme.com:443</code>, wobei <code>wmserver.acme.com</code> 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.</p> <p>ANMERKUNG: Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird.</p>
<p>Name – MQTT</p> <p>Datentyp – Zeichenfolge</p> <p>Code – 166</p> <p>Beschreibung – MQTT-Server</p>	<p>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: <code>wmservername.domain.com:1883</code>.</p> <p>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:</p> <p>US1:us1-pns.wysemanagementsuite.com</p> <p>EU1:eu1-pns.wysemanagementsuite.com</p>

Options-Tag	Beschreibung
Name – CA-Validation Datentyp – Zeichenfolge Code – 167 Beschreibung – Zertifizierungsstellenprüfung	<p>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.</p> <p>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.</p> <p>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.</p>
Name – GroupToken Datentyp – Zeichenfolge Code – 199 Beschreibung – Gruppentoken	<p>Dieser Tag ist erforderlich, um ThinOS-Geräte in der Wyse Management Suite in einer öffentlichen oder privaten Cloud zu registrieren.</p> <p>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.</p>

Geräte mit DNS-SRV-Eintrag registrieren

ANMERKUNG: Weitere Informationen zur 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 3. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags

URL/Tag	Beschreibung
Eintragsname – _WMS_MGMT Eintrags-FQDN – _WMS_MGMT._tcp.<Domänenname> Eintragstyp – SRV	<p>Dieser Eintrag verweist auf die Wyse Management Suite Server-URL. Beispiel: <code>wmserver.acme.com:443</code>, wobei <code>wmserver.acme.com</code> 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.</p> <p>ANMERKUNG: Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird.</p>
Eintragsname – _WMS_MQTT Eintrags-FQDN – _WMS_MQTT._tcp.<Domänenname> Eintragstyp – SRV	<p>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: <code>wmservername.domain.com:1883</code>.</p> <p>ANMERKUNG: MQTT ist bei der neuesten Version der Wyse Management Suite optional.</p>

URL/Tag	Beschreibung
	<p>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:</p> <p>US1 –us1-pns.wysemanagementsuite.com</p> <p>EU1 –eu1-pns.wysemanagementsuite.com</p>
<p>Eintragsname – _WMS_GROUPTOKEN</p> <p>Eintrags-FQDN – _WMS_GROUPTOKEN.<Domain></p> <p>Eintragstyp – TEXT</p>	<p>Dieser Datensatz ist erforderlich, um ThinOS-Geräte in der Wyse Management Suite in einer öffentlichen oder privaten Cloud zu registrieren.</p> <p>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.</p> <p>ANMERKUNG: Das Gruppentoken ist optional für die neueste Version von Wyse Management Suite in einer privaten Cloud.</p>
<p>Eintragsname – _WMS_CAVALIDATION</p> <p>Eintrags-FQDN – _WMS_CAVALIDATION.<Domain></p> <p>Eintragstyp – TEXT</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>ANMERKUNG: CA Validation ist bei der neuesten Version der Wyse Management Suite optional.</p>

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 Installationsskripten 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](#)
- [Erstellen und Bereitstellen von Standardanwendungsrichtlinie für Thin Clients](#)

Hochladen und Bereitstellen von ThinOS-Firmware-Image-Beständen

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

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.

i 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.

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.

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.

Problemlösung:

- 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.

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 Neumage 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.

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](#).

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 Datenbanken basierend auf Ihren Anforderungen konfigurieren.

Themen:

- [Configure Mongo database](#)
- [Configure Maria database](#)

Configure Mongo database

Mongo database (MongoDB) operates on the Transmission Control Protocol (TCP) port number 27017.

 **NOTE: Replace any value that is boldfaced with your environment variables, as applicable.**

To configure MongoDB, do the following:

1. Install the MongoDB version 4.2.1.
2. Copy the MongoDB files to your local system—C:\Mongo.
3. Create the following directories if they do not exist:
 - C:\data
 - C:\data\db
 - C:\data\log
4. Go to the Mongo folder (C:\Mongo), and create a file named `mongod.cfg`.
5. Open the `mongod.cfg` file in a notepad, and add the following script:

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

6. Save and close the `mongod.cfg` file.
7. Open command prompt as an administrator, and run the following command:


```
mongod.exe --config "C:\Program Files\MongoDB\Server\4.2\mongod.cfg" -install or 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 is installed.
8. To start the MongoDB services, run the following command:


```
net start mongoDB
```
9. To start the Mongo database, run the following command:


```
mongo.exe
```
10. To open the default admin db, run the following command:


```
use admin;
```
11. After the MongoDB sheet is displayed, run the following commands:

```
db.createUser (
{
user:"wmsuser",
pwd:"PASSWORD",
roles:[{role:"userAdminAnyDatabase",db:"admin"},
{role:"dbAdminAnyDatabase",db:"admin"},
{role:"readWriteAnyDatabase",db:"admin"},
```

```
{role:"dbOwner",db:"stratus"}]
}
)
```

12. To switch to the stratus database, run the following command:

```
use stratus;
```

13. To stop the MongoDB services, run the following command:

```
net stop mongoDB
```

14. Add an authentication permission to the admin DB. Modify the `mongod.cfg` file to the following:

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

15. To restart the MongoDB service, run the following:

```
net Start mongoDB;
```

In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MongoDB. For information about setting the MongoDB on the Wyse Management Suite installer, see [Custom installation](#).

Configure Maria database

Maria database (MariaDB) operates on the Transmission Control Protocol (TCP) port number 3306.

NOTE:

- **The IP address displayed here belongs to the Wyse Management Suite server that hosts the web components.**
- **Replace any value that is boldfaced with your environment variables, as applicable.**

To configure MariaDB, do the following:

1. Install the MariaDB version 10.2.29.
2. Navigate to the MariaDB installation path—`C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p`.
3. Provide the root password which was created during installation
4. Create the database stratus—`DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_unicode_ci;`
5. Create user 'stratus'@'localhost';
6. Create user 'stratus'@'**IP ADDRESS**';
7. Set a password for 'stratus'@'localhost'=password('PASSWORD');
8. Set a password for 'stratus'@'**IP ADDRESS**'=password('PASSWORD');
9. Provide all privileges on *.* to 'stratus'@'**IP ADDRESS**' identified by 'PASSWORD' with a grant option.
10. Provide all privileges on *.* to 'stratus'@'localhost' identified by 'PASSWORD' with a grant option.

NOTE: To configure custom port for MariaDB, navigate to `C:\Program Files\MariaDB 10.2\bin>mysql.exe -u root -p -P<custom port>` in the second step.

In the Wyse Management Suite installer, the administrator must use the same user name and password that was created to access the stratus databases in MariaDB. For information about setting the MariaDB on the Wyse Management Suite installer, see [Custom installation](#).

Benutzerdefinierte Installation

Bei der benutzerdefinierten 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 benutzerdefinierte Installation nur fortgeschrittenen Benutzern.

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

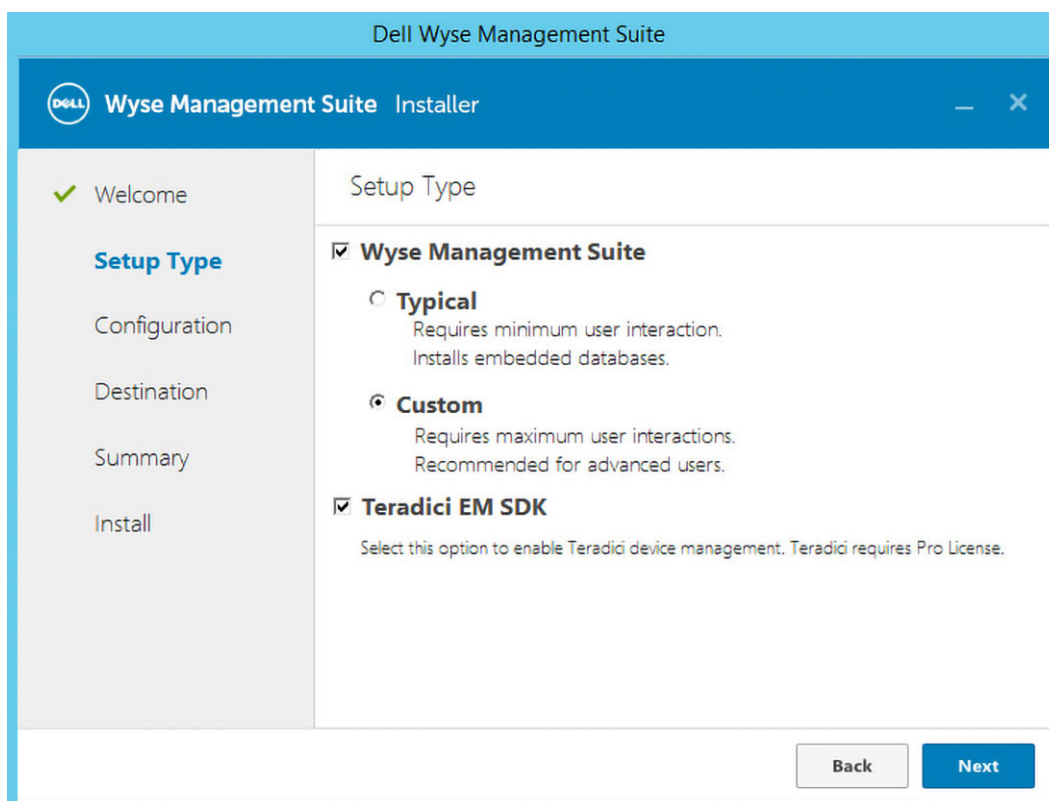


Abbildung 12. Setup-Typ

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

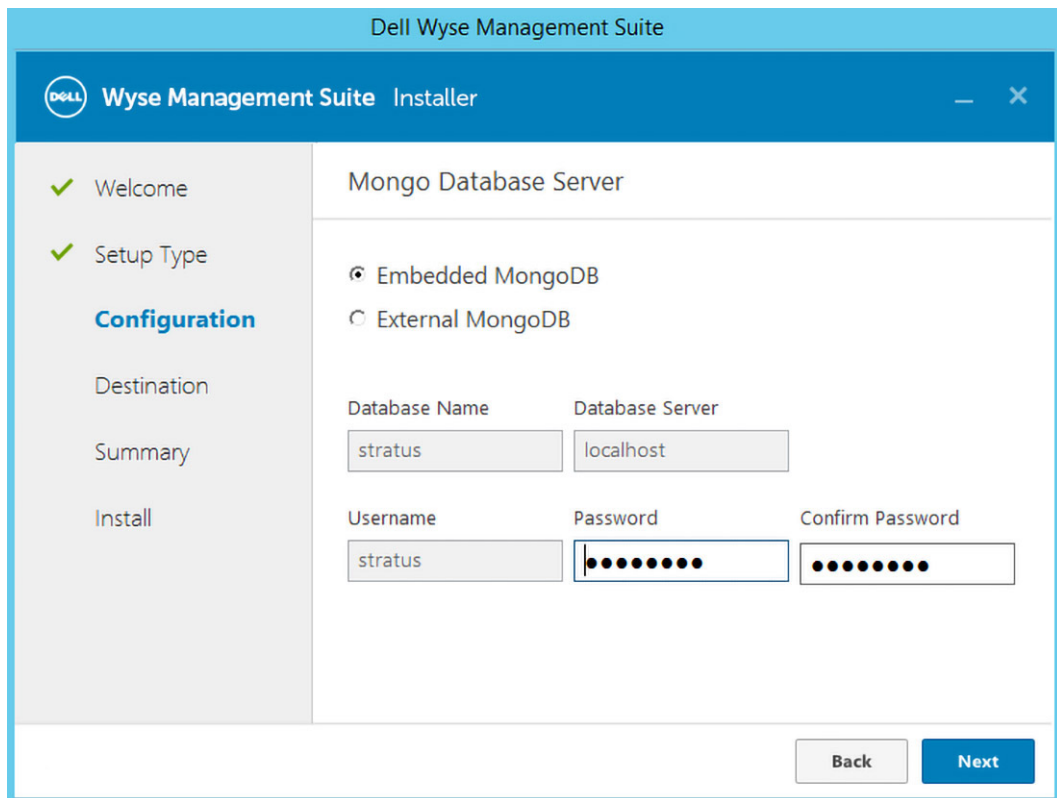


Abbildung 13. Integrierter Mongo-Datenbankserver

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

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

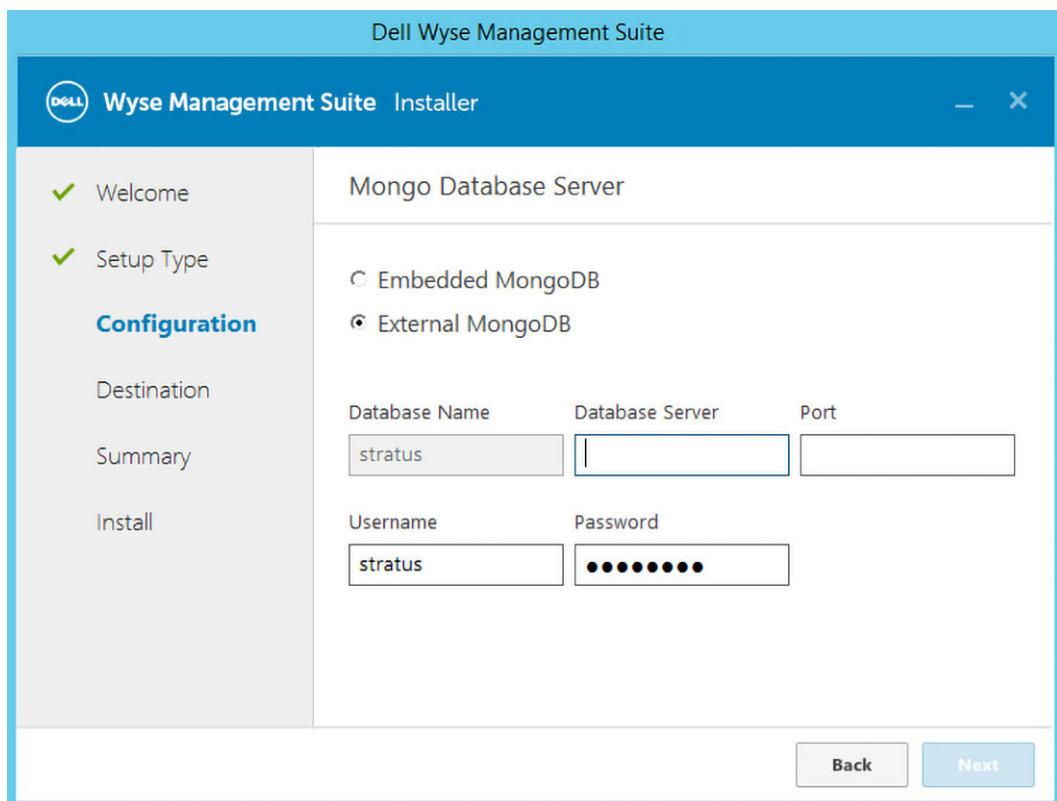


Abbildung 14. Externe MongoDB

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

3. Wählen Sie entweder **Eingebettete MariaDB** oder **Externe MariaDB** als MariaDB-Datenbankservers aus.
- Wenn **Eingebettete MariaDB** ausgewählt wurde, geben Sie den Benutzernamen und das Kennwort ein und klicken Sie auf **Weiter**.

The screenshot shows the 'Dell Wyse Management Suite' installer window. The title bar reads 'Dell Wyse Management Suite' and 'Wyse Management Suite Installer'. The main content area is titled 'MariaDB Database Server'. On the left, a navigation pane shows 'Welcome' and 'Setup Type' as completed steps, and 'Configuration' as the current step. Under 'Configuration', there are sub-steps: 'Destination', 'Summary', and 'Install'. The main configuration area has two radio buttons: 'Embedded MariaDB' (selected) and 'External MariaDB'. Below these are input fields for 'Database Name' (containing 'stratus') and 'Database Server' (containing 'localhost'). Further down are fields for 'Username' (containing 'stratus'), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). At the bottom right, there are 'Back' and 'Next' buttons.

Abbildung 15. Integrierte MariaDB

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

Das Portfeld generiert den Standardport, der geändert werden kann.

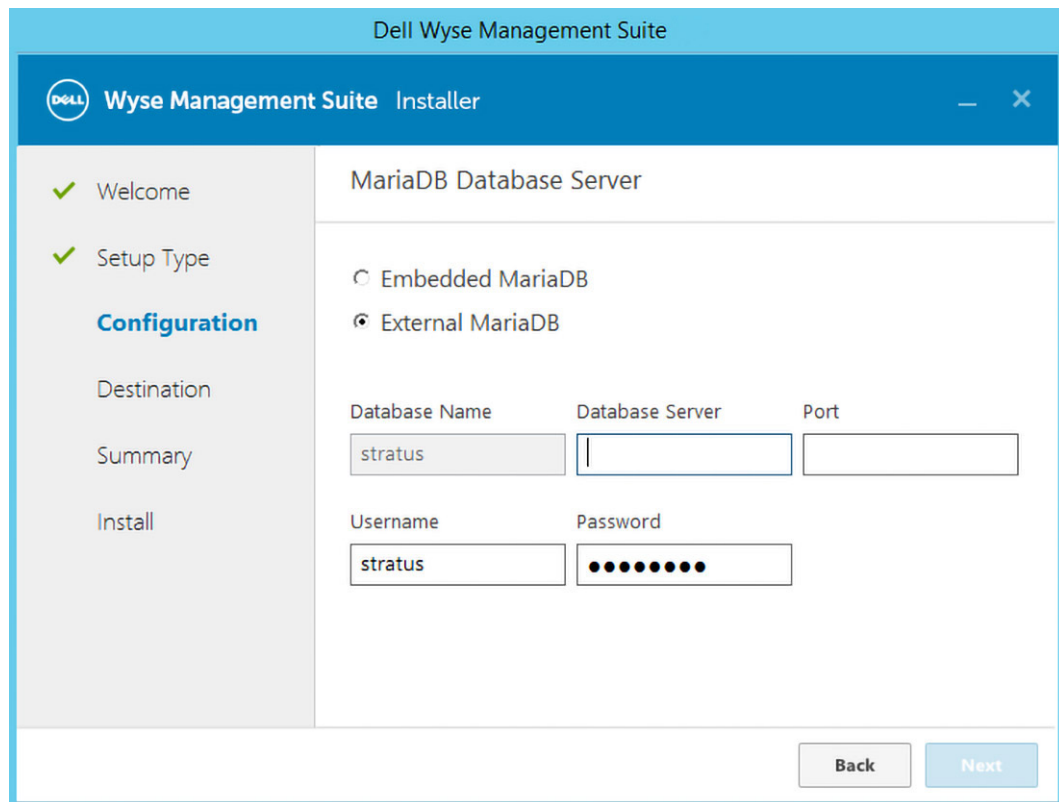


Abbildung 16. Externe MariaDB

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

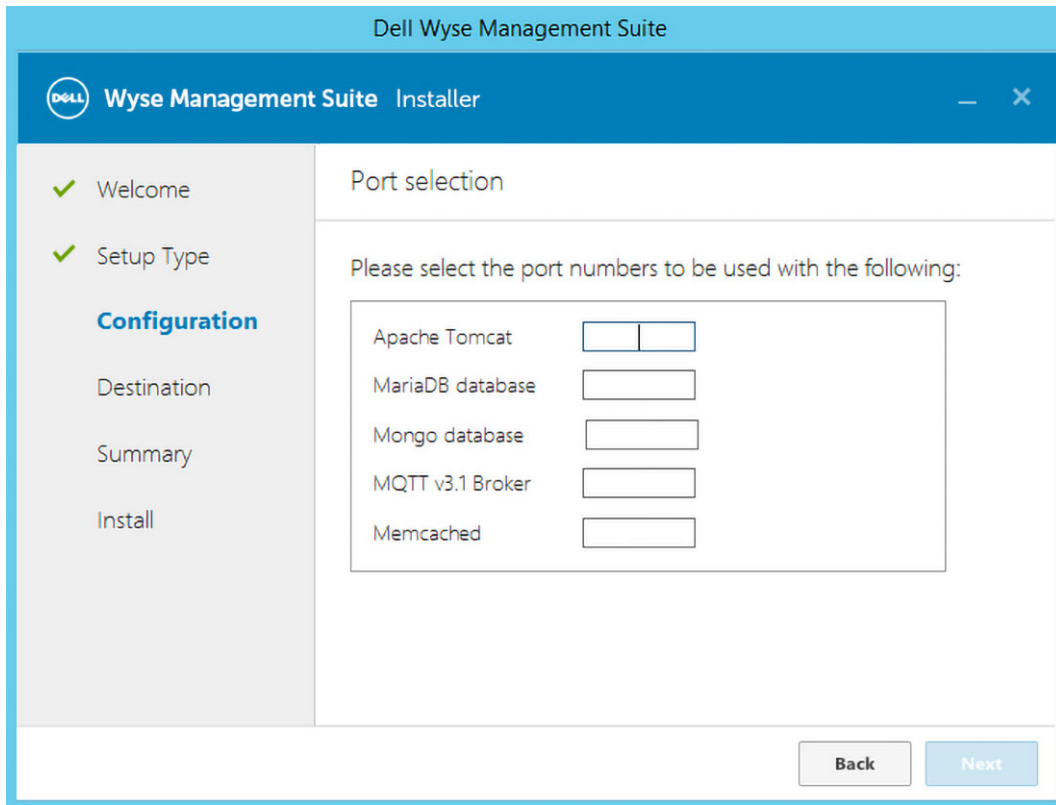


Abbildung 17. Portauswahl

- 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](#).

Wyse Management Suite-Funktionsmatrix

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

Tabelle 4. 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 freimachen	50.000 Geräte und mehr	1 Million Geräte und mehr
Lizenzschlüssel	Nicht erforderlich	Erforderlich	Erforderlich
Gruppenbasierte Verwaltung	Unterstützt	Unterstützt	Unterstützt
Gruppen mit mehreren Ebenen und Vererbung	Unterstützt	Unterstützt	Unterstützt
Konfigurationsrichtlinienverwaltung	Unterstützt	Unterstützt	Unterstützt
Betriebssystempatch und Abbildverwaltung	Unterstützt	Unterstützt	Unterstützt
Effektive Konfiguration auf Geräteebene nach Vererbung anzeigen	Unterstützt	Unterstützt	Unterstützt
Anwendungsrichtlinienverwaltung	Unterstützt	Unterstützt	Unterstützt
Anlagen-, Bestands- und Systemverwaltung	Unterstützt	Unterstützt	Unterstützt
Automatische Geräteermittlung	Unterstützt	Unterstützt	Unterstützt
Echtzeit-Befehle	Unterstützt	Unterstützt	Unterstützt
Smart planen	Unterstützt	Unterstützt	Unterstützt
Warnungs-, Ereignis- und Überwachungsprotokolle	Unterstützt	Unterstützt	Unterstützt
Sichere Kommunikation (HTTPS)	Unterstützt	Unterstützt	Unterstützt
Verwalten von Geräten hinter einer Firewall	Eingeschränkt*	Eingeschränkt*	Unterstützt
Mobile Anwendung	Nicht unterstützt	Unterstützt	Unterstützt
Warnungen unter Verwendung von E-Mail und mobilen Anwendungen	Nicht unterstützt	Unterstützt	Unterstützt
Scripting-Support für benutzerspezifische Anwendungsinstallation	Nicht unterstützt	Unterstützt	Unterstützt
Bundle-Anwendungen zur Vereinfachung der Bereitstellung und zum Minimieren von Neustarts	Nicht unterstützt	Unterstützt	Unterstützt
Delegierte Verwaltung	Nicht unterstützt	Unterstützt	Unterstützt

Funktionen	Wyse Management Suite Standard	Wyse Management Suite Pro – private Cloud	Wyse Management Suite Pro – Cloud Edition
Dynamische Gruppenerstellung und -Zuweisung basierend auf Geräte-Attributen	Nicht unterstützt	Unterstützt	Unterstützt
Zweifaktor-Authentifizierung	Unterstützt	Unterstützt	Unterstützt
Active Directory-Authentifizierung für rollenbasierte Verwaltung	Nicht unterstützt	Unterstützt	Unterstützt
Multi-Tenancy	Nicht unterstützt	Unterstützt	Unterstützt
Berichterstellung der Unternehmensklasse	Nicht unterstützt	Unterstützt	Unterstützt
Mehrere Repositorys	Nicht unterstützt	Unterstützt	Unterstützt
Aktivieren/Deaktivieren von Hardware-Ports auf unterstützten Plattformen	Nicht unterstützt	Unterstützt	Unterstützt
BIOS-Konfiguration auf unterstützten Plattformen	Nicht unterstützt	Unterstützt	Unterstützt
Konfiguration der Export- und Importrichtlinien	Nicht unterstützt	Unterstützt	Unterstützt
Repository-Zuweisung zu einer Anwendungsrichtlinie	Nicht unterstützt	Unterstützt	Unterstützt
Befehle zum Herunterfahren für Thin Clients	Unterstützt	Unterstützt	Unterstützt
Zeitüberschreitung der Wyse Management Suite-Konsole	Nicht unterstützt	Unterstützt	Unterstützt
Richtlinien-Reihenfolge	Nicht unterstützt	Unterstützt	Unterstützt
Auswahl der Anwendung gemäß dem Betriebssystem optimiert	Unterstützt	Unterstützt	Unterstützt
Option zum Konfigurieren eines Alias	Nicht unterstützt	Unterstützt	Unterstützt

ANMERKUNG: *Das Sternchen zeigt an, dass Sie Geräte mit der Wyse Management Suite nur in einer sicheren Firewall-Umgebung verwalten können. Sie können Thin Clients nicht über den Anwendungsbereich der Firewall-Einstellungen hinaus verwalten.

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 privaten 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 öffentlichen 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.

ANMERKUNG:

- **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.**

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

1. Laden Sie das Wyse Management Suite-Repository von der öffentlichen Cloud-Konsole herunter.
2. Nach dem Installationsprozess starten Sie die Anwendung.
3. Auf der Wyse Management Suite-Repository-Seite geben Sie die Anmeldeinformationen 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 öffentlichen 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 Dropdownliste 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 öffentliche 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**.

Erstellen und Konfigurieren von DHCP-Options-Tags

ANMERKUNG: Weitere Informationen zur Sicherheitsumgebung für Kunden finden Sie unter [Wyse-Geräte-Agent](#).

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

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**.

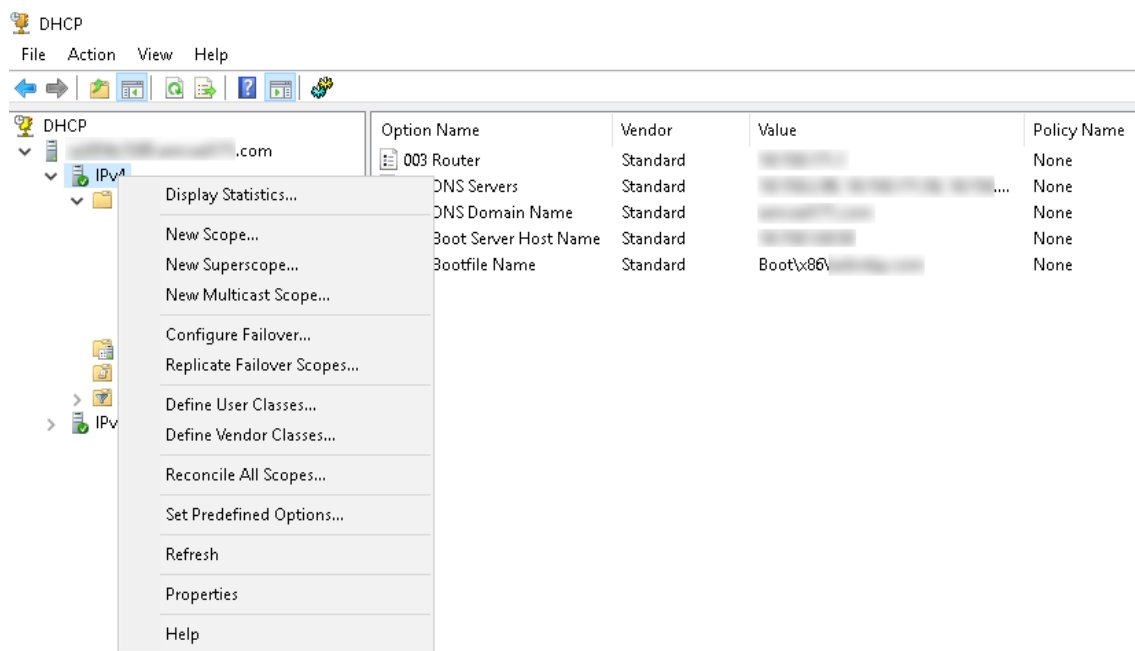


Abbildung 18. DHCP

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.

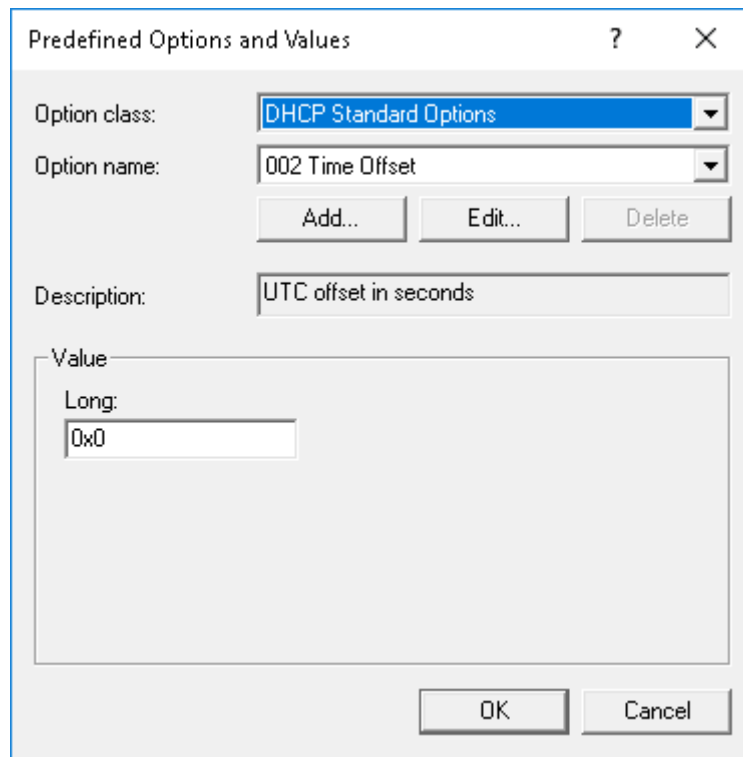


Abbildung 19. Vordefinierte Optionen und Werte

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

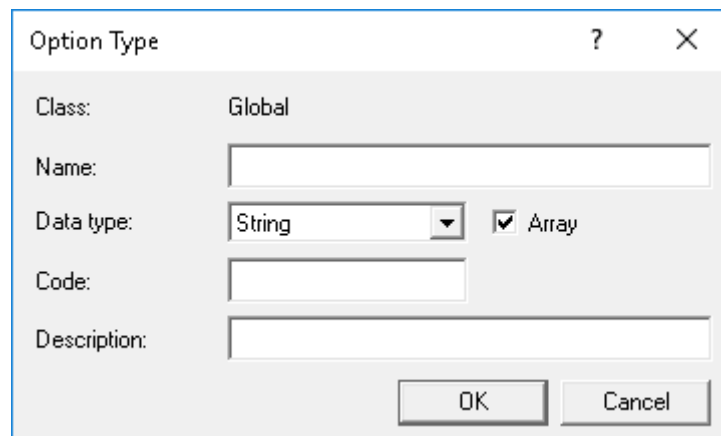


Abbildung 20. Optionstyp

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

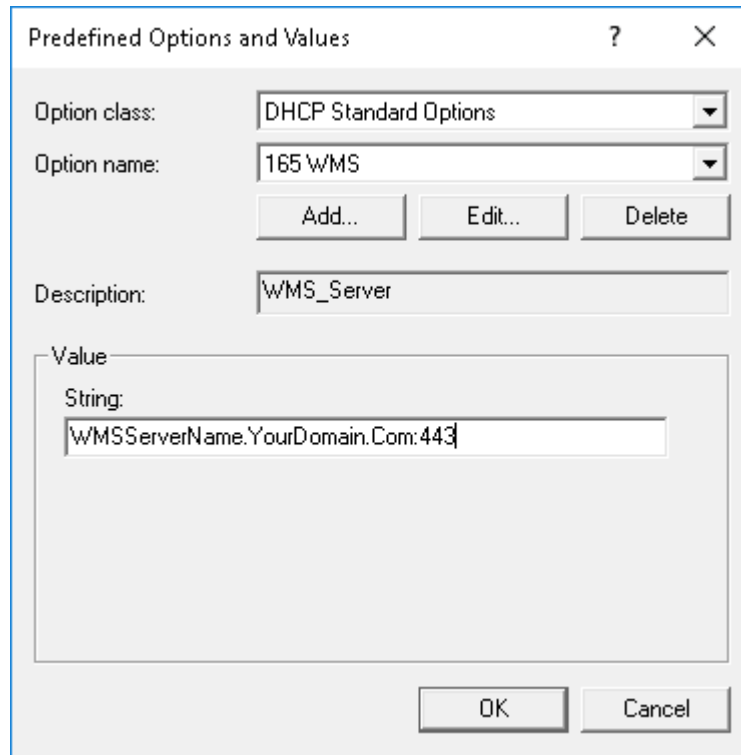


Abbildung 21. Option-Tag 165 Wyse Management Suite Server-URL

- 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

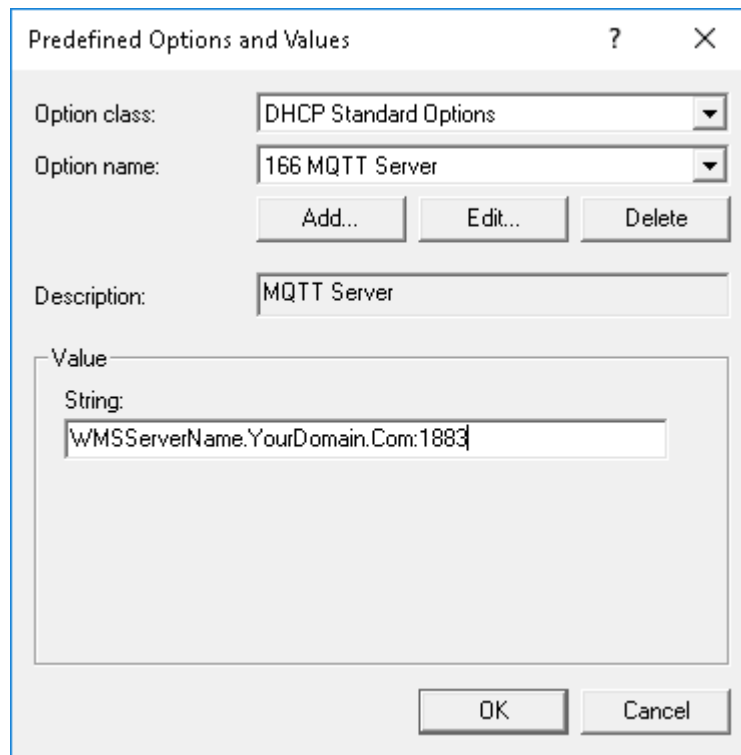


Abbildung 22. Option-Tag 166 Wyse Management Suite Server-URL

- 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

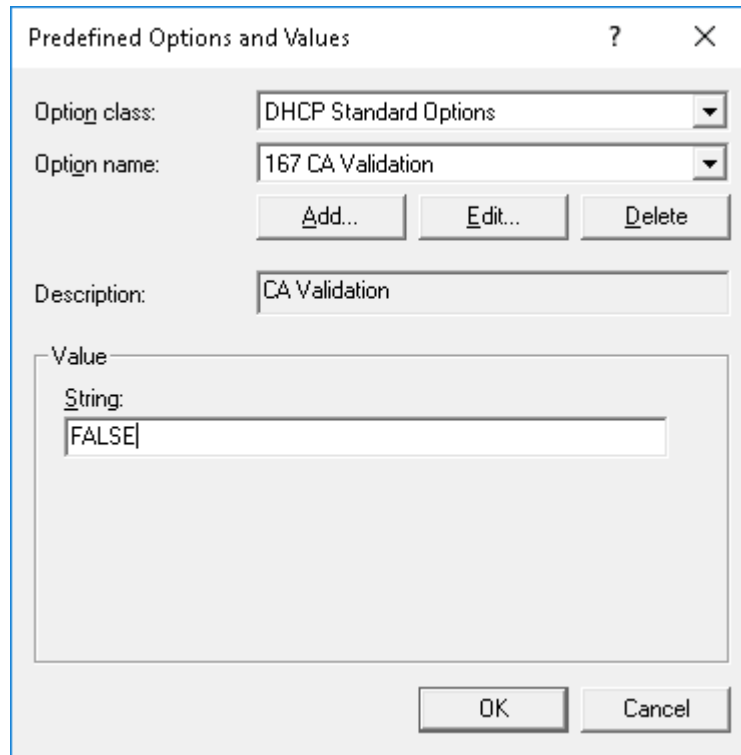


Abbildung 23. Option-Tag 167 Wyse Management Suite Server-URL

- 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

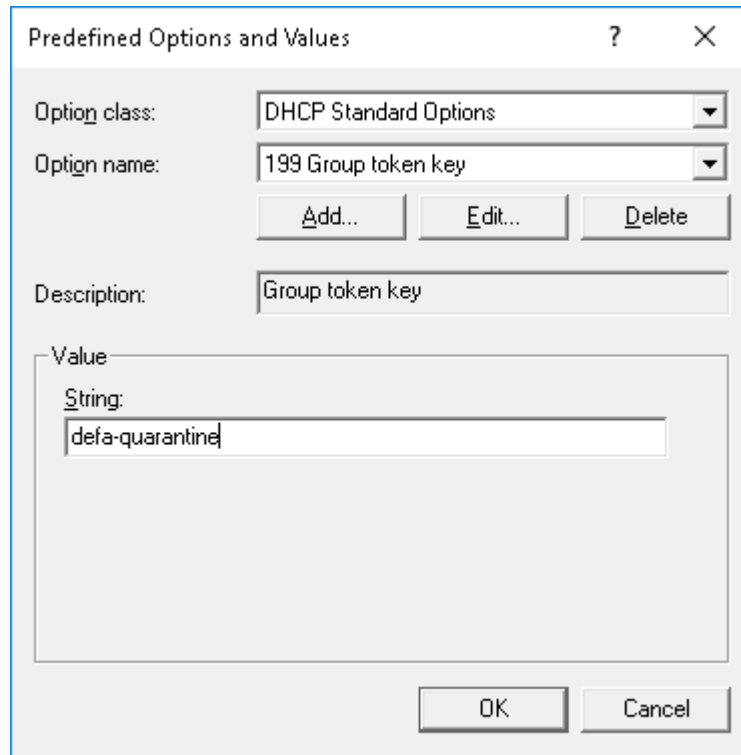


Abbildung 24. Option-Tag 199 Wyse Management Suite Server-URL

Erstellen und Konfigurieren von DNS-SRV-Einträgen

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:

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**.

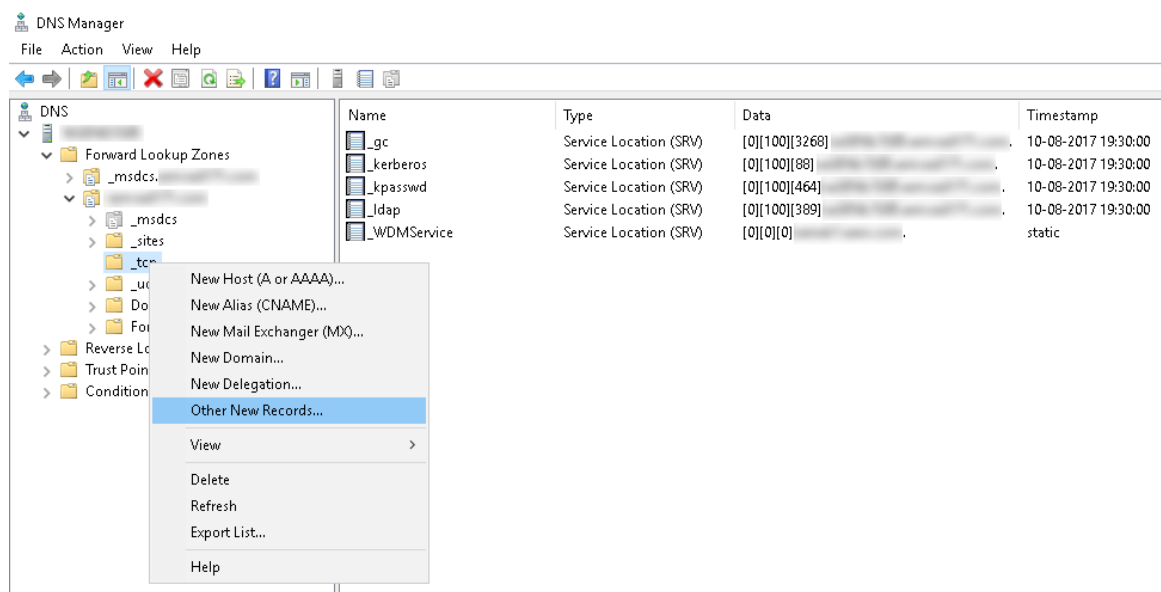


Abbildung 25. DNS-Manager

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:

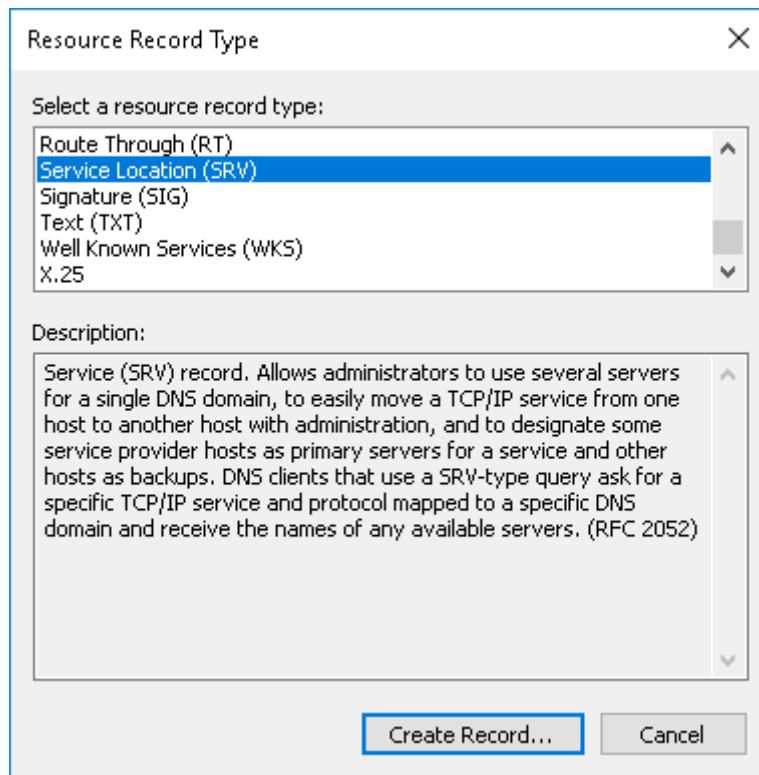


Abbildung 26. Ressourcendatensatztyp

- 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

New Resource Record

Service Location (SRV)

Domain: [Redacted]

Service: _WMS_MGMT

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 443

Host offering this service:
FQDN of WMS server

Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

Abbildung 27. _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

New Resource Record

Service Location (SRV)

Domain: []

Service: _WMS_MQTT

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 1883

Host offering this service:
FQDN of MQTT server

Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

Abbildung 28. _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:

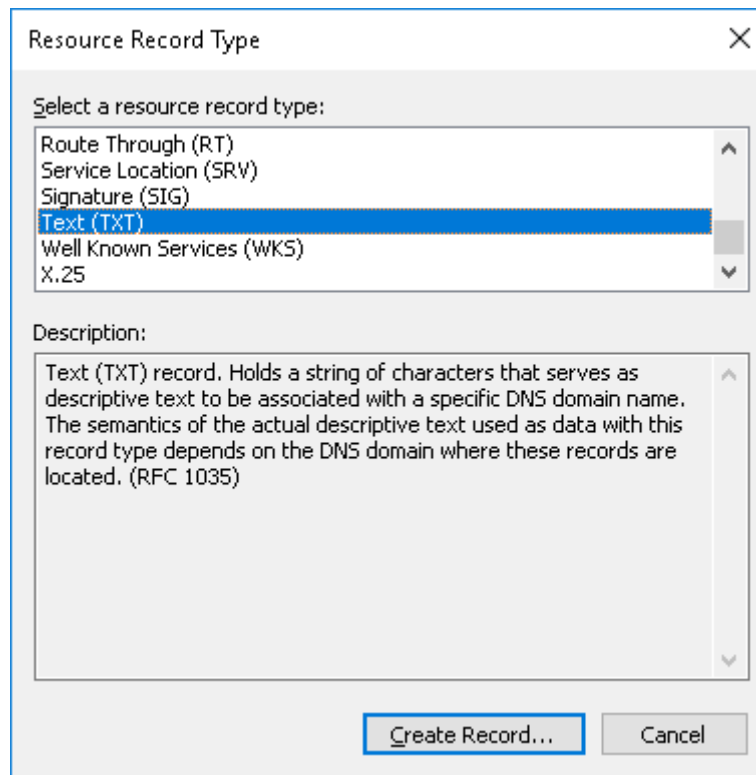


Abbildung 29. Ressourcendatensatztyp

- 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

The image shows a 'New Resource Record' dialog box with the following fields:

- Text (TXT)** (tab selected)
- Record name (uses parent domain if left blank):**
- Fully qualified domain name (FQDN):**
- Text:**

Buttons: **OK** and **Cancel**

Abbildung 30. _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_CAVVALIDATION
 - Text–TRUE/FALSE

The image shows a 'New Resource Record' dialog box with a close button (X) in the top right corner. The dialog is titled 'New Resource Record' and has a tab labeled 'Text (TXT)'. It contains three input fields and a text area:

- 'Record name (uses parent domain if left blank):' with the text '_wms_cavalidation'.
- 'Fully qualified domain name (FQDN):' with the text '_wms_cavalidation.'.
- 'Text:' with a text area containing the word 'False'.

At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

Abbildung 31. _wms_cavalidation Datensatzname

Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients

Zum Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients gehen Sie folgendermaßen vor:

1. Kopieren Sie die Anwendung und die Skripte vor/nach der Installation (falls erforderlich) zur Bereitstellung auf den Thin Clients im Ordner `thinClientApps` im lokalen Repository oder dem Wyse Management Suite-Repository.
2. Gehen Sie zu **Apps&Daten > ApplInventory** und wählen Sie **Thin Client** um zu überprüfen, ob die Anwendung registriert ist.
3. Klicken Sie auf **Thin Client** unter **App-Richtlinien**.
4. Klicken Sie auf **Erweiterte Richtlinie hinzufügen**.
5. Gehen Sie folgendermaßen vor, um eine neue Anwendungsrichtlinie zu erstellen:
 - a. Geben Sie einen **Richtliniennamen**, eine **Gruppe**, eine **Aufgabe** und einen **Gerätetyp** ein.
 - b. Klicken Sie auf **App hinzufügen** und wählen Sie einen oder mehrere Anwendungen unter **TC-Apps**. Für jede Anwendung können Sie ein Skript vor und nach der Installation unter **Vor Installation**, **Nach Installation** und **Installations-Parameter** wählen. Wenn Sie möchten, dass das System nach der erfolgreichen Installation der Anwendung neu starten soll, wählen Sie **Neustart**.
 - c. Wenn Sie wollen, dass diese Richtlinie auf alle Untergruppen angewendet wird, wählen Sie **Alle Untergruppen einschließen**.
 - d. Wenn Sie diese Richtlinie auf einem bestimmten Betriebssystem oder einer bestimmten Plattform bereitstellen möchten, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter**.
 - e. Die Zeitüberschreitung 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.
 - f. Wenn Sie die Richtlinie automatisch auf ein Gerät anwenden möchten, das in der Wyse Management Suite registriert ist und zu einer ausgewählten Gruppe gehört oder in die ausgewählte Gruppe verschoben wurde, wählen Sie **Richtlinie auf neue Geräte anwenden** aus der Dropdownliste **Richtlinie automatisch anwenden**.

ANMERKUNG: 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**.
 - g. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an.
6. Damit eine Verzögerung bei der Ausführung der Richtlinie ermöglicht wird, 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 Stunden (1 bis 24 Stunden), die die Ausführung der Richtlinie verzögert werden kann.
 - Wählen Sie aus dem Dropdownmenü **Max. Verzögerungen** wie oft Sie die Ausführung der Richtlinie verzögern können (1- bis 3-mal).
7. Zum Abbrechen der Anwendungsrichtlinie beim ersten Fehler, wählen Sie **App-Abhängigkeit aktivieren**. Wenn diese Option nicht ausgewählt ist, wirkt sich der Ausfall einer Anwendung auf die Richtlinienausführung aus.
8. Klicken Sie zum Erstellen einer neuen Richtlinie auf **Speichern**. Eine Nachricht wird angezeigt, um es Administratoren zu ermöglichen, diese Richtlinie für Geräte basierend auf der Gruppe zu planen. Wählen Sie **Ja**, um die Anwendungsrichtlinie sofort oder zu einem auf der Seite **App-Richtlinienjob** geplanten Datum und Uhrzeit auszuführen.

Die App/Image-Richtlinienjob kann dann ausgeführt werden:

 - a. **Sofort** – Der Server führt den Job sofort aus.
 - b. **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.
 - c. **Gemäß ausgewählter Zeitzone** – Der Server erstellt einen Job, der an dem Datum und zu der Uhrzeit der angegebenen Zeitzone ausgeführt wird.
9. Klicken Sie auf **Vorschau** und "Zeitplan festlegen" auf der nächsten Seite, um den Job zu erstellen.
10. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

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**.

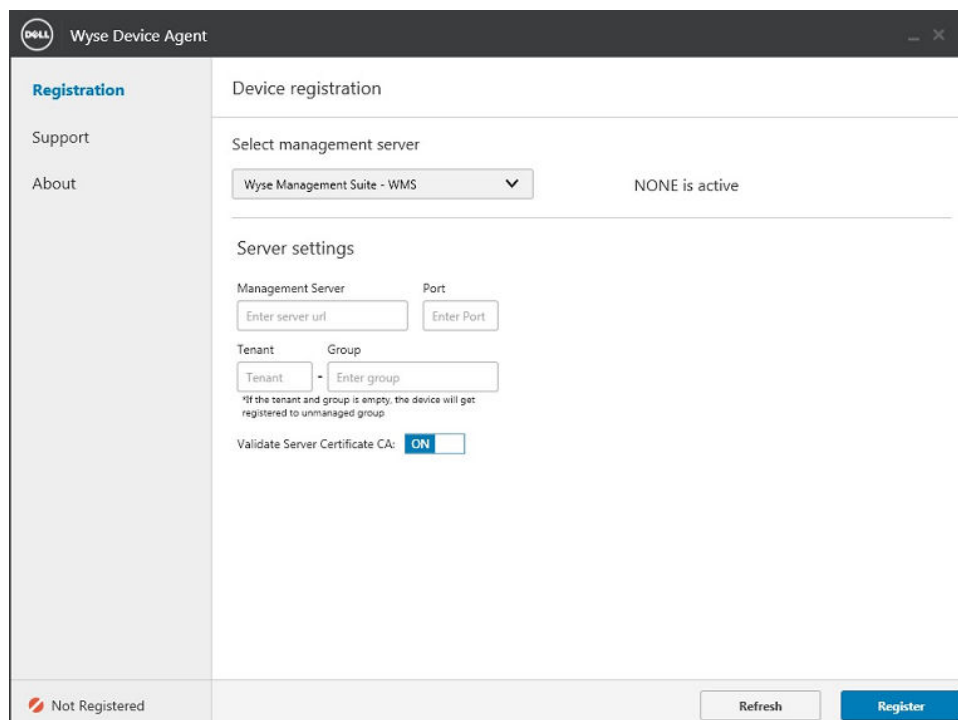


Abbildung 32. Gerätregistrierung

ThinOS 8.x-Gerät manuell registrieren

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.
i 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**.
i ANMERKUNG: Wenn die Option zur Anmeldevalidierung aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite Geräte im Status Anmeldevalidierung 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.

ThinOS 9.x-Gerät manuell registrieren

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 Anmeldevalidierung aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite Geräte im Status Anmeldevalidierung 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.

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.

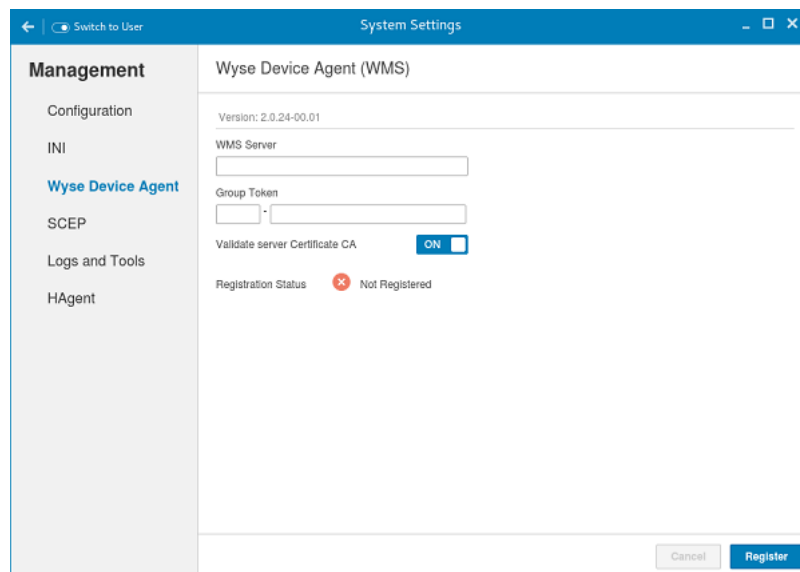


Abbildung 33. Geräteregistrierung

Begriffe und Definitionen

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

Tabelle 5. Begriffe und Definitionen

Terminologie	Definition
Private Cloud	Wyse Management Suite-Server, der in der Cloud installiert ist, die für das Datacenter 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	Anwendung, Betriebssystemimage und Datei-Repository, die bzw. das standardmäßig mit dem Wyse Management Suite-Server installiert wird.
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 Datacenter 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 die Berechtigungen zum Ausführen von Vorgängen basierend auf den ihnen zugewiesenen Rollen.