

# Dell Wyse Management Suite

Version 3.1 Administratorhandbuch



## Hinweise, Vorsichtshinweise und Warnungen

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

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

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

<b>Kapitel 1: Einführung in die Wyse Management Suite.....</b>	<b>9</b>
Was ist neu in Wyse Management Suite-Version 3.1.....	9
Editionen von Wyse Management Suite.....	9
Wyse Management Suite-Funktionsmatrix.....	10
<b>Kapitel 2: Erste Schritte mit der Wyse Management Suite.....</b>	<b>15</b>
Anmelden bei der Wyse Management Suite in einer Public Cloud.....	15
Voraussetzungen für Wyse Management Suite in einer Private Cloud.....	16
Funktionsbereiche der Managementkonsole.....	17
Konfigurieren und Verwalten von Thin Clients.....	17
Wyse-Geräte-Agent.....	18
Dell Client Agent.....	19
<b>Kapitel 3: Installieren oder Aktualisieren von Wyse Geräte-Agent.....</b>	<b>20</b>
Manuelles Installieren von Wyse Geräte-Agenten auf einem Windows-eingebetteten Gerät.....	20
Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie.....	21
Installieren oder Aktualisieren von Wyse Geräte-Agenten auf ThinLinux- und Linux-Clients.....	21
<b>Kapitel 4: Registrieren und Konfigurieren eines neuen Geräts mithilfe von Wyse Management Suite....</b>	<b>23</b>
Registrieren und konfigurieren Sie ein neues Windows-eingebettetes Standard-Gerät mithilfe von Wyse Management Suite.....	23
Registrieren und Konfigurieren eines neuen ThinOS-8.x-Geräts mithilfe von Wyse Management Suite.....	23
Registrieren und Konfigurieren eines neuen ThinOS-9.x-Geräts mithilfe von Wyse Management Suite.....	24
Registrieren und Konfigurieren eines neuen Linux- oder ThinLinux-Geräts mithilfe von Wyse Management Suite.....	25
Registrieren und Konfigurieren eines neuen Wyse Software-Thin Clients mithilfe der Wyse Management Suite.....	25
Registrieren und konfigurieren Sie den Dell Hybrid-Client mithilfe der Wyse Management Suite.....	26
<b>Kapitel 5: Wyse Management Suite-Dashboard.....</b>	<b>28</b>
Anzeigen von Warnungen.....	28
Anzeigen der Ereignisliste.....	29
Anzeigen des Gerätestatus.....	29
Aktivieren der Anmeldevalidierung.....	29
Ändern von Benutzereinstellungen.....	29
Zugriff auf die Onlinehilfe.....	30
Ändern Ihres Kennworts.....	30
Abmelden von der Verwaltungskonsole.....	30
<b>Kapitel 6: Verwalten von Gruppen und Konfigurationen.....</b>	<b>31</b>
Bearbeiten einer nicht verwalteten Gruppe.....	32
Erstellen einer Standard-Geräterichtliniengruppe.....	32
Erstellen einer ThinOS-Auswahlgruppe.....	33
Bearbeiten einer Standard-Geräterichtliniengruppe.....	33

Bearbeiten einer ThinOS-Auswahlgruppe.....	33
Entfernen einer ThinOS-Auswahlgruppe.....	33
Erstellen einer Nutzerrichtliniengruppe.....	34
Bearbeiten der Nutzerrichtliniengruppe.....	36
Konfigurieren von Richtlinien der Globalen Klasse.....	36
Importieren einer Nutzerrichtliniengruppe.....	36
Entfernen einer Gruppe.....	37
Konfigurieren von Richtlinien der Geräteklasse.....	37
Gruppenrichtlinien exportieren.....	37
Importieren von Gruppenrichtlinien.....	38
Importieren von Gruppenrichtlinien aus Gruppen- und Konfigurationen-Seite.....	38
Importieren von Gruppenrichtlinien von der Seite „Richtlinien bearbeiten“.....	38
Bearbeiten der Einstellungen für ThinOS-Richtlinien.....	39
ThinOS – Assistentenmodus.....	40
ThinOS – Erweiterter Modus.....	40
Bearbeiten der Einstellungen für ThinOS-9.x-Richtlinien.....	40
BIOS-Konfigurationen für ThinOS 9.x.....	41
Aktualisieren von ThinOS 9.x auf spätere Versionen mit der Wyse Management Suite.....	42
Hochladen und Pushen von BIOS-Paketen.....	42
Hochladen und Pushen von ThinOS 9.x-Anwendungspaketen mit Gruppen und Konfigurationen.....	43
Bearbeiten von Windows Embedded Standard-Richtlinieneinstellungen.....	43
Konfigurieren der Bereitstellungseinstellungen für Windows Embedded-Geräten.....	43
Bearbeiten der Einstellungen für die Linux-Richtlinie.....	44
Bearbeiten der Einstellungen für die ThinLinux-Richtlinie.....	44
Konfigurieren von Bereitstellungseinstellungen für ThinLinux-Geräte.....	44
Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen.....	45
Bearbeiten der Einstellungen für die Cloud Connect-Richtlinieneinstellungen.....	45
Bearbeiten der Einstellungen der Dell Hybrid Client-Richtlinien.....	45
Konfigurieren der Wyse Management Suite Clienteneinstellungen für Dell Hybrid Client.....	47
Konfigurieren von Bereitstellungseinstellungen für Dell Hybrid Client-Geräte.....	48
Erstellen und Importieren einer Ausnahmedatei für ein Massenspeichergerät.....	49
<b>Kapitel 7: Verwalten von Geräten.....</b>	<b>52</b>
Methoden zum Registrieren Geräten bei Wyse Management Suite.....	53
Manuelles Registrieren von Dell Hybrid Clients.....	53
Registrieren von Dell Hybrid Clients mithilfe der manuellen Ermittlungsmethode.....	55
Registrieren von ThinOS-Geräten mit dem Wyse Geräte-Agenten.....	55
Registrieren von Windows Embedded Standard Thin Clients bei der Wyse Management Suite über Wyse Geräte-Agent.....	56
Registrieren des Wyse Software Thin Client bei der Wyse Management Suite über den Wyse Geräte- Agenten.....	57
Registrieren von ThinLinux Thin Clients über Wyse Geräte-Agent.....	57
Registrieren von ThinOS-Geräten mithilfe der FTP-INI-Methode.....	57
Registrieren von Geräten mit ThinLinux Version 2.0 mithilfe der FTP-INI-Methode.....	58
Registrieren von Geräten mit ThinLinux Version 1.0 mithilfe der FTP-INI-Methode.....	58
Registrieren von Geräten mithilfe von DHCP-Options-Tags.....	59
Geräte mit DNS-SRV-Eintrag registrieren.....	60
Suchen nach einem Gerät mithilfe von Filtern.....	61
Filter auf der Seite „Geräte“ speichern.....	62
Abfragen des Gerätestatus.....	62

Sperren der Geräte.....	63
Neustart der Geräte.....	63
Registrierung eines Geräts aufheben.....	63
Anmeldungsvalidierung.....	64
Validieren der Anmeldung eines Geräts.....	64
Gerät auf Werkseinstellungen zurücksetzen.....	64
Ändern einer Gruppenzuweisung auf der Seite „Geräte“.....	65
Senden von Meldungen an ein Gerät.....	65
Wake on LAN-Befehl.....	65
Anzeigen der Gerätedetails.....	65
Anzeigen der Anzeigeparameter.....	66
Anzeigen der Details zu virtuellen NICs.....	66
Überprüfen der BIOS-Details.....	67
Verwalten der Gerätezusammenfassung.....	67
Anzeigen von Systeminformationen.....	67
Anzeigen von Geräteereignissen.....	67
Anzeigen installierter Anwendungen.....	68
Umbenennen des Thin Client.....	68
Aktivieren von Remote Shadowing-Verbindung.....	69
Konfigurieren der Remote Shadowing-Verbindung für Dell Hybrid Client-Geräte.....	69
Herunterfahren von Geräten.....	69
Hinzufügen eines Tags zu einem Gerät.....	70
Compliance-Status des Geräts.....	70
Pull für Windows Embedded Standard oder ThinLinux-Abbild ausführen.....	70
Anfordern einer Protokolldatei.....	71
Fehlerbehebung auf Ihrem Gerät.....	71
Erstellen eines neuen Image Ihres Dell Hybrid Client.....	72
Benutzeroberflächen-Konfigurationspaket für Dell Hybrid Client herunterladen.....	72
Zurücksetzen des Dell Hybrid Clients auf die Werkseinstellungen.....	72

**Kapitel 8: Anwendungen und Daten..... 74**

Anwendungsrichtlinie.....	74
Konfigurieren einer Thin-Client-Anwendungsbestandsaufnahme.....	75
Konfigurieren der Wyse Software Thin-Client-Anwendungsbestandsaufnahme.....	75
Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Thin Clients.....	75
Erstellen und Bereitstellen einer Standardanwendungsrichtlinie auf Wyse Software Thin Clients.....	76
Einmaliges Anmelden für Citrix StoreFront mithilfe der Standard-Anwendungsrichtlinie aktivieren.....	77
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients.....	78
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie für Wyse Software-Thin Clients.....	79
Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Dell Hybrid Clients.....	81
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Dell Hybrid Clients.....	82
Abbildrichtlinie.....	83
Hinzufügen von Windows-eingebetteten Standard-Betriebssystem- und ThinLinux-Abbildern zum Repository.....	83
Hinzufügen von ThinOS-Firmware zum Repository.....	84
Hinzufügen von ThinOS-BIOS-Datei zum Repository.....	84
Hinzufügen von ThinOS-Paketdatei zu Repository.....	84
Erstellen von Windows-eingebetteten Standard- und ThinLinux-Abbildrichtlinien.....	85
Hinzufügen von ThinOS-Firmware zum Repository.....	85
Hinzufügen von ThinOS-Anwendungspaketen zum Repository.....	85

Erstellen von Dell Hybrid Client-Abbildrichtlinien.....	86
Verwalten eines Datei-Repositorys.....	86
<b>Kapitel 9: Verwalten von Regeln.....</b>	<b>88</b>
Bearbeiten einer Registrierungsregel.....	88
Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte.....	89
Bearbeitung der Regel für die automatische Zuweisung nicht verwalteter Geräte.....	89
Deaktivieren und Löschen von Regeln für die automatische Zuweisung nicht verwalteter Geräte.....	89
Speichern der Regelreihenfolge.....	90
Hinzufügen einer Regel für Warnmeldungen.....	90
Bearbeiten einer Warnmeldungsregel.....	90
<b>Kapitel 10: Aufträge verwalten.....</b>	<b>91</b>
BIOS-Administratorkennwort synchronisieren.....	92
Suchen eines geplanten Jobs mithilfe von Filtern.....	92
Planen des Gerätebefehljobs.....	93
Planen der Abbildrichtlinie.....	93
Planen einer Anwendungsrichtlinie.....	94
<b>Kapitel 11: Verwalten von Ereignissen.....</b>	<b>95</b>
Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern.....	95
Anzeigen einer Zusammenfassung der Ereignisse.....	96
Anzeigen des Überwachungsprotokolls.....	96
Reporting für Endnutzer-Sitzungen.....	96
<b>Kapitel 12: Verwalten von Benutzern.....</b>	<b>97</b>
Hinzufügen eines neuen Administratorprofils.....	98
Erstellen einer benutzerdefinierten WMS-Rolle in Wyse Management Suite.....	99
Massenimport nicht zugewiesener Administratoren oder Cloud Connect-Nutzer.....	99
Bearbeiten eines Administratorprofils.....	100
Aktivieren eines Administratorprofils.....	100
Deaktivieren eines Administratorprofils.....	100
Löschen eines Administratorprofils.....	101
Entsperren eines Administratorprofils.....	101
Deaktivieren eines Administratorprofils.....	101
Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte.....	101
Hinzufügen eines Endnutzers.....	102
Bearbeiten eines Endnutzers.....	102
Konfigurieren der Benutzerrichtlinie.....	102
Massenimport von Endnutzern.....	102
Endnutzer löschen.....	103
Bearbeiten eines Nutzerprofils.....	103
<b>Kapitel 13: Portalverwaltung.....</b>	<b>104</b>
Importieren von nicht zugewiesenen Nutzern oder Nutzergruppen in die Public Cloud über Active Directory...	105
Hinzufügen der Active Directory-Serverinformationen.....	105
Funktion "Active Directory-Verbunddienste" in einer Public Cloud konfigurieren.....	106
Warnungsklassifizierungen.....	107
Erstellen eines API-Kontos (Application Programming Interface).....	107

Zugreifen auf Wyse Management Suite Datei-Repository.....	108
Subnetz-Zuordnung.....	108
Andere Einstellungen konfigurieren.....	109
Verwalten von Teradici-Konfigurationen.....	110
Aktivieren der Zwei-Faktor-Authentifizierung.....	110
Aktivieren von Multi-Tenant Konten.....	110
Generieren von Berichten.....	111
Aktivieren von benutzerdefiniertem Branding.....	111
Verwalten des System-Setups.....	111
<b>Kapitel 14: Konvertieren von Dell Wyse 5070-Geräten und Dell OptiPlex 7070 Ultra in Dell Hybrid-Client.....</b>	<b>113</b>
Dell Wyse 5070-Konvertierung.....	113
Hinzufügen von Dell Hybrid Client-Images zum Repository.....	114
Erstellen von Hybrid Client-Abbildrichtlinien.....	114
Planen der Abbildrichtlinie.....	115
Dell OptiPlex 7070 Ultra-Konvertierung.....	116
<b>Kapitel 15: Sicherheitskonfigurationen.....</b>	<b>117</b>
Unterstützung für die Konfiguration von TLS-Versionen im Wyse Management Suite-Installationsprogramm....	117
Konfigurieren der Funktion Active Directory-Verbunddienste in einer Public Cloud.....	117
Konfigurieren der Secure LDAP- oder LDAPS-Setups.....	118
Veraltetes Protokoll.....	119
<b>Kapitel 16: Teradici-Geräteverwaltung.....</b>	<b>120</b>
Ermittlung von Teradici-Geräten.....	120
CIFS-Anwendungsszenarien.....	123
<b>Kapitel 17: Verwalten des Lizenzabonnements.....</b>	<b>124</b>
Importieren von Lizenzen von der öffentlichen Cloud-Konsole der Wyse Management Suite.....	124
Exportieren von Lizenzen in die private Cloud-Konsole der Wyse Management Suite.....	124
Thin Client-Lizenzzuweisung.....	125
Lizenzbestellungen.....	125
<b>Kapitel 18: Firmware-Upgrade.....</b>	<b>126</b>
Aktualisieren von ThinLinux 1.x auf 2.1 und neuere Versionen.....	126
Vorbereiten des ThinLinux 2.x-Abbilds.....	126
ThinLinux 1.x auf 2.x aktualisieren.....	127
Aktualisieren von ThinOS 8.x auf 9.0.....	128
Hinzufügen von ThinOS-Firmware zum Repository.....	128
Upgrade von ThinOS 8.6 auf ThinOS 9.x.....	128
Aktualisieren von ThinOS 9.x auf spätere Versionen mit der Wyse Management Suite.....	129
<b>Kapitel 19: Remote-Repository.....</b>	<b>130</b>
Verwalten des Wyse Management Suite Repository-Dienstes.....	135
Proxy-Unterstützung für Wyse Management Suite-Remote-Repositories.....	135
<b>Kapitel 20: Fehlerbehebung auf Ihrem Gerät.....</b>	<b>137</b>
Anfordern einer Protokolldatei mithilfe von Wyse Management Suite.....	137

Anzeigen von Prüfprotokollen mithilfe von Wyse Management Suite.....	138
Gerät kann nicht bei Wyse Management Suite registriert werden, wenn der WinHTTP-Proxy konfiguriert ist...	138
RemoteFX USB-Umleitungsrichtlinie wird für USB-Massenspeichergeräte nicht angewendet.....	138
In der Wyse Management Suite konfigurierte WLAN-Einstellungen sind nicht über mehrere Wyse 5070 Thin Clients persistent.....	139

**Kapitel 21: Häufig gestellte Fragen..... 140**

Was hat Vorrang zwischen Wyse Management Suite und der ThinOS-Benutzeroberfläche, wenn in Konflikt stehende Einstellungen durchgesetzt werden?.....	140
Wie verwende ich das Wyse Management Suite Datei-Repository?.....	140
Wie kann ich Benutzer aus einer .csv-Datei importieren?.....	141
Wie prüfe ich die Version von Wyse Management Suite.....	141
Wie Sie DHCP-Options-Tags erstellen und konfigurieren.....	141
Wie Sie DNS-SRV-Einträge erstellen und konfigurieren.....	142
Schritte zum Ändern des Hostnamens zur IP-Adresse.....	143
Wie kann ich das Gerät mit einem selbstsignierten Remote-Repository abbilden?.....	143

# Einführung in die Wyse Management Suite

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

## Themen:

- [Was ist neu in Wyse Management Suite-Version 3.1](#)
- [Editionen von Wyse Management Suite](#)
- [Wyse Management Suite-Funktionsmatrix](#)

## Was ist neu in Wyse Management Suite-Version 3.1

- Bereitstellen von Geräteausnahme-Konfigurationen für mehrere Thin-9.x-Geräte.
- Es werden EULA-Details zu den von Thin-9.x signierten Paketen angezeigt.
- Rollenbasierter Zugriff mit granularen Berechtigungen.
- Suche nach statischen Parametern auf der Konfigurations-Benutzeroberfläche.
- BIOS-Aufzählung für ThinOS 9.x
- Konfigurieren der automatischen Bereitstellung der Anwendung für Windows Embedded-, ThinLinux- und Dell Hybrid Client-Geräte.
- Scripting-Unterstützung für ThinLinux mithilfe von erweiterten oder standardmäßigen Anwendungsrichtlinien.
- EULA-Änderungen für Wyse Management Suite-Server, Repository-Server und Import-Tool-Installationsprogramm.
- Berichterstellungs-Anzeigeparameter und Hervorhebung des primären Anzeigeparameterfelds.
- Berichterstellung der Parameter von virtuellen NICs und Hervorhebung des primären Parameterfelds.
- Konfigurieren des VNC für Dell Hybrid Client-Geräte.
- Konfigurieren der SSH für Dell Hybrid Client-Geräte.
- SOCKS 5-Proxy-Protokoll für Repository-Server.
- Konvertierung von Dell Wyse 5070-Geräten in Dell Hybrid Client.
- Konvertierung von Dell OptiPlex 7070 Ultra in Dell Hybrid Client mithilfe von DCA-Enabler 1.1.

## Editionen von Wyse Management Suite

Wyse Management Suite ist in den folgenden Editionen erhältlich:

- **Standard (kostenlos)** – Die Standard-Edition der Wyse Management Suite verfügt über die grundlegenden Funktionen und ist nur für die Bereitstellung in einer privaten Cloud verfügbar. Sie benötigen keinen Lizenzschlüssel, um die Standard Edition zu verwenden. Diese Version kann nur Dell Thin Clients verwalten. Die Standard Edition eignet sich für kleine und mittelständische Unternehmen.
- **Pro (kostenpflichtig)** – die Pro-Edition der Wyse Management Suite ist eine robustere Lösung. Sie ist für die Bereitstellung in öffentlichen und privaten Clouds verfügbar. Zur Verwendung der Pro Edition (abonnementsbasierte Lizenzierung) ist ein Lizenzschlüssel erforderlich. Mit der Pro-Lösung können Unternehmen ein Hybridmodell und bewegliche Lizenzen zum Wechsel zwischen der Bereitstellung in der öffentlichen und privaten Cloud nutzen. Diese Version ist für die Verwaltung von Teradici-basierten Geräten, Wyse Converter for PC-basierte Thin Clients, Dell Hybrid Client-Geräte, integrierte PCs und Edge Gateway-Geräte erforderlich. Sie bietet außerdem erweiterte Funktionen für die Verwaltung von Dell Thin Clients. Für eine Bereitstellung in der Public Cloud kann die Pro Edition in Nicht-Firmennetzwerken verwaltet werden (Home Office, Drittanbieter, Partner, mobile Thin Clients usw.).

 **ANMERKUNG:** Lizenzen können ganz einfach zwischen Cloud- und vor-Ort-Installation gewechselt werden.

Die Pro Edition der Wyse Management Suite bietet außerdem:

- Eine mobile App, zum Anzeigen von kritischen Warnungen sowie Benachrichtigungen und dem Senden von Befehlen in Echtzeit.

- Verbesserte Sicherheit durch Zwei-Faktoren-Identifizierung und Active Directory-Authentifizierung für rollenbasierte Verwaltung.
- Erweiterte App-Richtlinie und -Berichterstellung

**i ANMERKUNG:** Cloud-Services werden gehostet in den USA und Deutschland. Kunden in Ländern mit Beschränkungen bezüglich zulässiger Datenspeicherorte können u. U. den Cloud-basierten Dienst nicht nutzen.

Die Wyse Management Suite-Webkonsole unterstützt Internationalisierung. In der unteren rechten Ecke der Seite können Sie aus dem Dropdownmenü eine der folgenden Sprachen wählen:

- Englisch
- Französisch
- Italienisch
- Deutsch
- Spanisch
- Chinesisch
- Japanisch

## Wyse Management Suite-Funktionsmatrix

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

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

Funktionen	Wyse Management Suite Standard	Wyse Management Suite Pro – private Cloud	Wyse Management Suite Pro – Cloud Edition
Hochgradig skalierbare Lösung zur Verwaltung von Thin Clients	Bis zu 10.000 Geräte freigeben	Bis zu 120.000 Geräte	Bis zu 1 Million Geräte
Lizenzbedingungen	Kostenloser Download	Abonnement pro Arbeitsplatz	Abonnement pro Arbeitsplatz
Lizenzschlüssel	Nicht erforderlich	Erforderlich	Erforderlich
Architektur	Private Cloud	Private Cloud	Öffentliche Cloud
Flexible Bereitstellung oder Hybrid Cloud	X	✓	✓
Erweitertes Installationsprogramm	X	✓	✓
Mehrmandantenfähigkeit	X	✓	✓
Delegierte Administration für die Granularität der Berechtigungen	X	✓	✓
Mehrere Repositories zur Unterstützung ihrer verteilten Architektur	X	✓	✓
Option zum Konfigurieren des Wyse Management Suite Server-Alias	X	✓	✓
Architektur für Hochverfügbarkeit	X	✓	X
Proxy-Unterstützung – SOCKS5	✓	✓	✓
Dell ProSupport for Software enthalten	X	✓	✓
<b>Reporting und Überwachung</b>			
Lokalisierte Managementkonsole	X	✓	✓
Warnungen, Ereignisse und Auditprotokolle mithilfe von E-Mail- und mobilen Anwendungen	X	✓	✓
Berichterstellung der Unternehmensklasse	X	✓	✓

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

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

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

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

Funktionen des Dell Hybrid Client-Management	Wyse Management Suite Standard	Wyse Management Suite Pro – private Cloud	Wyse Management Suite Pro – Cloud Edition
Multimonitor-Support	X	√	√
Follow-Me Profil	X	√	√
Dateizugehörigkeit zum Priorisieren des Anwendungsbereitstellungsmodus	X	√	√
BIOS-Einstellungen und Konfigurationsunterstützung	X	√	√
Konfiguration der Export- und Importrichtlinien	X	√	√
Standardmäßige Nutzergruppenrichtlinie	X	√	√
Browserkonfiguration	X	√	√
Konfigurieren des Cloud-Anbieters	X	√	√
Konfigurieren von VNC	X	√	√
Konfigurieren von SSH	X	√	√

**ANMERKUNG:** \* Das Sternchen gibt an, dass für Dell Hybrid Client ein vor-Ort-Repository erforderlich ist, wenn Sie die Wyse Management Suite Public Cloud-Umgebung verwenden.


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

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

Managementfunktionen für Wyse Thin Clients und Zero Clients	Wyse Management Suite Standard	Wyse Management Suite Pro – private Cloud	Wyse Management Suite Pro – Cloud Edition
<b>Vollständige Sichtbarkeit des Bestands</b>			
Automatische Geräteermittlung	√	√	√
Anlagen-, Bestands- und Systemverwaltung	√	√	√
Effektive Konfiguration auf Geräteebene nach Vererbung anzeigen	√	√	√
<b>Reporting und Überwachung</b>			
Remote-Shadow mithilfe von VNC	√	√	
Konfigurierbarer Heartbeat- und Check-in-Intervall	√	√	√
<b>Sicherheit</b>			
Sichere Kommunikation (HTTPS)	√	√	√
802.1x-Zertifikatbereitstellung	√	√	√

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

<b>Managementfunktionen für Wyse Thin Clients und Zero Clients</b>	<b>Wyse Management Suite Standard</b>	<b>Wyse Management Suite Pro – private Cloud</b>	<b>Wyse Management Suite Pro – Cloud Edition</b>
Zweifaktor-Authentifizierung	X	√	√
Active Directory-Authentifizierung für rollenbasierte Verwaltung	X	√	√
Domain-Beitrittsfunktion (Windows Embedded Standard)	X	√	√
Lockdown-Einstellungen (Aktivieren oder Deaktivieren von Ports unterstützter Endpunkte)	X	√	√
<b>Umfassendes Management</b>			
Betriebssystempatch und Abbildverwaltung	√	√	√ **
Smarte Planung	√	√	√
Automatische Bereitstellung	√	√	√
Bundle-Anwendungen zur Vereinfachung der Bereitstellung und zum Minimieren von Neustarts	X	√	√
Dynamische Gruppenerstellung und -Zuweisung basierend auf Geräte-Attributen	X	√	√
Repository-Zuweisung zu Anwendungsrichtlinie und Subnetz-Zuordnung	X	√	√
Erweiterte Anwendungsrichtlinie	X	√	√
<b>Konfiguration</b>			
Konfiguration des Assistenten für Wyse ThinOS 8. x	√	√	√
Multimonitor-Support	√	√	√
Wyse Easy Setup und Wyse Overlay Optimizer	√	√	√
Scripting-Support für benutzerspezifische Anwendungsinstallation	X	√	√
BIOS-Einstellungen und Konfigurationsunterstützung	X	√	√
Konfiguration der Export- und Importrichtlinien	X	√	√
RSP-Paketunterstützung	X	√	√
WDM-Import-Tool	X	√	X
Massenspeichergeräte-Ausnahme	X	√	√

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

# Erste Schritte mit der Wyse Management Suite

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

## Themen:

- Anmelden bei der Wyse Management Suite in einer Public Cloud
- Voraussetzungen für Wyse Management Suite in einer Private Cloud
- Funktionsbereiche der Managementkonsole
- Konfigurieren und Verwalten von Thin Clients
- Wyse-Geräte-Agent
- Dell Client Agent

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

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

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

Wenn Sie sich zum ersten Mal bei der Wyse Management Suite Konsole anmelden, wenn ein neuer Nutzer hinzugefügt wird oder wenn eine Nutzerlizenz erneuert wird, wird die Seite **Geschäftsbedingungen** angezeigt. Lesen Sie die 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](https://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](https://www.wysemanagementsuite.com).

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

## Ändern Ihres Kennworts

So ändern Sie Ihr Anmeldekennwort:

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

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

## Abmelden

So melden Sie sich bei der Managementkonsole ab:

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

## Voraussetzungen für Wyse Management Suite in einer Private Cloud

Tabelle 4. Voraussetzungen

Beschreibung	10 000 Geräte oder weniger	50 000 Geräte oder weniger	120 000 Geräte oder weniger	Wyse Management Suite – Software-Repository
Betriebssystem	Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019 Standard Der Wyse Management Suite Webserver verfügt über einen integrierten Apache Tomcat Webserver. Stellen Sie sicher, dass Sie Microsoft IIS Apache Tomcat Webserver nicht separat installieren. Unterstützte Sprachpakete: Englisch, Französisch, Italienisch, Deutsch, Spanisch, Japanisch und traditionelles Chinesisch			
Mindest-Festplattenspeicherplatz	40 GB	120 GB	200 GB	120 GB
Mindest-Arbeitsspeicher (RAM)	8 GB	16 GB	32 GB	16 GB
Minimale CPU-Anforderungen	4	4	16	4
Netzwerkkommunikationsports	Das Wyse Management Suite-Installationsprogramm fügt die TCP-Ports (Transmission Control Protocol) 443, 8080 und 1883 zur Firewall-Ausnahmeliste hinzu. Die Ports werden für den Zugriff auf die Wyse Management Suite-Konsole und zum Senden der Push-Benachrichtigungen an die Thin Clients hinzugefügt. <ul style="list-style-type: none"> <li>• TCP 443 – HTTPS-Kommunikation</li> <li>• TCP 1883 – MQTT-Kommunikation</li> <li>• TCP 3306 – MariaDB (optional, wenn Remote)</li> <li>• TCP 27017 – MongoDB (optional, wenn Remote)</li> <li>• TCP 11211 – Memcache</li> <li>• TCP 5172, 49159 – End-User Management Software Development Kit (EMSDK) – optional und nur für Teradici Geräte erforderlich</li> </ul> Die Standardschnittstellen, die vom Installationsprogramm verwendet werden, können im Rahmen der Installation zu einem alternativen Port geändert werden.			Das Wyse Management Suite Repository Installationsprogramm fügt die TCP-Ports 443 und 8080 zur Firewall-Ausnahmeliste hinzu. Die Ports werden für den Zugriff auf die Betriebssystem-Abbilder und Anwendungs-Abbilder hinzugefügt, die von der Wyse Management Suite verwaltet werden.
Unterstützte Browser	Internet Explorer Version 11 Google Chrome, Version 58.0 und höher Mozilla Firefox, Version 52.0 und höher Edge-Browser unter Windows – nur in englischer Sprache			

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

**ANMERKUNG:** `WMS.exe` Und `WMS_Repo.exe` müssen auf zwei verschiedenen Servern installiert werden. Sie müssen das Wyse Management Suite Remote-Repository für die 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.

## Funktionsbereiche der Managementkonsole

Die Wyse Management Suite-Konsole ist in die folgenden Funktionsbereiche unterteilt:

- Die **Dashboard**-Seite enthält Informationen zum aktuellen Status jedes Funktionsbereichs des Systems.
- Die Seite **Gruppen und Konfigurationen** nutzt eine hierarchische Gruppenrichtlinienverwaltung zur Device-Konfiguration. Optional können Untergruppen der globalen Gruppenrichtlinien erstellt werden, um Geräte entsprechend den Unternehmensstandards zu kategorisieren. Beispielsweise können Geräte nach Stellenfunktion, Gerätetyp und so weiter untergliedert werden.
- Die Seite **Benutzer** ermöglicht es, lokalen und aus dem Active Directory importierten Benutzern, die Rollen als globaler Administrator, Gruppenadministrator und Viewer zuzuweisen und sich bei der Wyse Management Suite anzumelden. Benutzer erhalten Berechtigungen zum Ausführen von Vorgängen auf Basis der ihnen zugewiesenen Rollen. Außerdem wird die Registerkarte **Endnutzer** für die Nutzerverwaltung hinzugefügt.
- Die Seite **Geräte** ermöglicht das Anzeigen und Verwalten von Geräten, Gerätetypen, und gerätespezifischen Konfigurationen.
- Die Seite **Apps & Data** ermöglicht die Verwaltung von Geräteanwendungen, Anwendungsinventar und Datei-Repository.
- Die Seite **Regeln** ermöglicht Ihnen das Hinzufügen, Bearbeiten und Aktivieren oder Deaktivieren von Regeln wie z. B. automatische Gruppierung und Warnmeldung.
- Die Seite **Jobs** ermöglicht Ihnen die Erstellung von Jobs für Aufgaben wie z. B. Neustart, LAN und Anwendungs- oder Abbildrichtlinien, die auf registrierten Geräten bereitgestellt werden müssen.
- Die Seite **Ereignisse** ermöglicht das Anzeigen und Überprüfen von Systemereignissen und Warnungen.
- Die Seite **Portalverwaltung** ermöglicht Ihnen die Konfiguration verschiedener Systemeinstellungen, wie die Konfiguration des lokalen Repositories, die Dell Hybrid Client Lizenzabonnements, Active Directory-Konfiguration und Zwei-Faktor-Authentifizierung.

## Konfigurieren und Verwalten von Thin Clients

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

**ANMERKUNG:** In der Pro Edition können Sie Regeln für das Erstellen von Gruppen hinzufügen. Sie können auch Geräte zu einer vorhandenen Gruppe zuordnen, je nach Geräteattributen wie z. B. Subnetz, Zeitzone und Standort.

Sie können auch Folgendes konfigurieren:

- Einstellungen, die für alle Geräte im Mandantenkonto gelten. Das ist die Standardrichtliniengruppe. Diese Einstellungen sind der globale Parametersatz, den alle Gruppen und Untergruppen erben. Die für Gruppen auf einer niedrigeren Ebene konfigurierten Einstellungen haben Vorrang vor den Einstellungen, die für übergeordnete Gruppen konfiguriert wurden.

Beispiel:

- Konfigurieren Sie die Richtlinien für die Standardrichtliniengruppe (übergeordnete Gruppe). Nach der Konfiguration der Richtlinien überprüfen Sie die Richtlinien der benutzerdefinierten Gruppe (untergeordnete Gruppe). Derselbe Satz von Richtlinien wird auf die untergeordnete Gruppe angewendet. Eine Konfiguration der Einstellungen der Standardrichtliniengruppe ist der globale Parametersatz, den alle Gruppen und Untergruppen von der übergeordneten Gruppe übernehmen.

- Konfigurieren Sie die verschiedenen Einstellungen für die benutzerdefinierte Gruppe. Die benutzerdefinierte Gruppe empfängt beide Payloads, aber Geräte in der Standardrichtliniengruppe empfangen nicht die Payload, die für die benutzerdefinierte Richtliniengruppe konfiguriert ist.
  - Konfigurieren Sie die verschiedenen Einstellungen für die benutzerdefinierte Gruppe. Die für Gruppen auf einer niedrigeren Ebene konfigurierten Einstellungen haben Vorrang vor den Einstellungen, die für übergeordnete Gruppen konfiguriert wurden.
- Einstellungen, die spezifisch für ein bestimmtes Gerät gelten, können auf der Seite **Gerätedetails** konfiguriert werden. Diese Einstellungen, wie untergeordnete Gruppen, haben Vorrang vor den in übergeordneten Gruppen konfigurierten Einstellungen.

Wenn Sie die Richtlinie erstellen und veröffentlichen, werden die Konfigurationsparameter auf allen Geräten in dieser Gruppe einschließlich der Untergruppen bereitgestellt.

Nachdem eine Richtlinie veröffentlicht und an die Geräte verteilt wurde, werden die Einstellungen nicht erneut an die Geräte gesendet, bis Sie eine Änderung vornehmen. Neue Geräte, die registriert wurden, erhalten die Konfigurationsrichtlinie, die für die Gruppe gilt, in der sie registriert wurden. Dies umfasst die Parameter, die von der globalen Gruppe und Zwischengruppen geerbt wurden.

Richtlinien zur Laufwerkskonfiguration werden sofort veröffentlicht und können nicht für einen späteren Zeitpunkt geplant werden. Einige Richtlinienänderungen, z. B. an den Anzeigeeinstellungen, erzwingen möglicherweise einen Neustart.

- **Bereitstellung der Anwendung und des Betriebssystemabbilds** – Aktualisierungen an Anwendungen und dem Betriebssystemabbild 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 aktuelle und alle Untergruppen basierend auf Ihren Anforderungen. Betriebssystemabbilder können nur in der aktuellen Gruppe bereitgestellt werden.

Die Wyse Management Suite unterstützt die Anwendungsrichtlinien "Standard" und "Erweitert". Eine Standardanwendungsrichtlinie ermöglicht die Installation eines einzigen Anwendungspakets. Das Gerät wird während der Installation einer Anwendung neu gestartet. Starten Sie das Gerät vor und nach jeder Anwendungsinstallation neu. 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 Skripten vor und nach der Installation, die für die Installation einer bestimmten Anwendung erforderlich sein können.

Sie können Standard- und erweiterte Anwendungsrichtlinien konfigurieren, um automatisch angewandt zu werden, wenn ein Gerät in der Wyse Management Suite registriert wurde oder wenn ein Gerät in eine neue Gruppe verschoben wurde.

Die Bereitstellung von Anwendungsrichtlinien und Betriebssystemabbildern auf Thin Clients kann für sofort oder später geplant werden, basierend auf der Zeitzone des Geräts oder festgelegten anderen Zeitzonen.

- **Gerätebestand** – Diese Option finden Sie durch Klicken auf die Registerkarte **Geräte**. Standardmäßig zeigt diese Option eine paginierte Liste aller Geräte im System an. Sie können eine Teilmenge von Geräten mithilfe von verschiedenen Filterkriterien wählen, wie z. B. Gruppen und Untergruppen, Gerätetyp, Art des Betriebssystems, Status, Subnetz und die Plattform oder Zeitzone.

Um zur Seite **Gerätedetails** für dieses Gerät zu navigieren, klicken Sie auf den auf dieser Seite aufgelisteten Geräteeintrag. Alle Einzelheiten für das Gerät werden angezeigt.

Die Seite **Gerätedetails** enthält außerdem alle Konfigurationsparameter, die für dieses Gerät gelten, und auch die Gruppenklasse, auf die die einzelnen Parameter angewendet werden.

Diese Seite ermöglicht außerdem das Einstellen der Konfigurationsparameter, die speziell für das Gerät gelten, indem sie die Schaltfläche **Geräteausnahmen** aktiviert. Parameter in diesem Abschnitt überschreiben alle Parameter, die in Gruppen und/oder auf globaler Ebene konfiguriert wurden.

- **Berichte** – Sie können vordefinierte Berichte auf der Grundlage der voreingestellten Filter generieren und anzeigen. Klicken Sie zum Erzeugen von vordefinierten Berichten auf der Seite **Portalverwaltung** auf die Registerkarte **Berichte**.
- **Mobile-Anwendung** – Sie können mithilfe der mobilen App **Dell Mobile Agent** Warnbenachrichtigungen erhalten und Geräte verwalten. Sie ist für Android-Geräte verfügbar. Zum Herunterladen der mobilen App und des **Dell Mobile Agent Handbuchs zum Einstieg** klicken Sie auf die Registerkarte **Warnungen und Klassifizierung** auf der Seite **Portaladministrator**.

## 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.

## Dell Client Agent

Der Dell Client Agent (DCA) ist ein einheitlicher Agent für alle Lösungen zur Dell Hybrid Client-Management. Durch die Installation des DCA können Sie Dell Hybrid Clients mit der Wyse Management Suite verwalten.

DCA Enabler ist ein Client-Agent zur Verwaltung von Ubuntu Version 18.04 LTS 64-Bit auf OptiPlex 7070 Ultra-Geräten. Die Dell Hybrid Client-Software wird mit Dell Client Agent-Enabler (DCAE) vorinstalliert geliefert. Mit DCA-Enabler können Sie die folgenden Aktionen durchführen, die von der Wyse Management Suite verwaltet werden:

- Registrierung
- Bereitstellen von Echtzeitbefehlen (RTC)
- Registrierung beim Server aufheben
- Bereitstellen einer Standard-Anwendungsrichtlinie
- Zertifikatrichtlinie bereitstellen

So installieren Sie Dell Hybrid Client auf dem OptiPlex 7070 Ultra-Gerät:

1. Registrieren Sie das Gerät bei der Wyse Management Suite mithilfe der Erkennungsmethode (DNS oder DHCP) oder der manuellen Methode über eine **reg.json**-Datei – siehe [Methoden zum Registrieren von Geräten bei der Wyse Management Suite](#).
2. Erstellen Sie ein neues Image Ihres OptiPlex 7070 Ultra-Geräts – siehe [Erstellen eines neuen Image Ihres Dell Hybrid Client](#).

# Installieren oder Aktualisieren von Wyse Geräte-Agent

Dieser Abschnitt enthält Informationen über die Installation oder Aktualisierung des Wyse Gerät-Agents auf Ihren Thin Clients, wie z. B. Windows-eingebettete Standard-, Linux- und ThinLinux-Geräte, unter Verwendung der Wyse Management Suite.

- **Windows-eingebettete Standard-Geräte** – Wyse Geräte-Agent Version 1.4.x kann von [support.dell.com](http://support.dell.com) heruntergeladen werden. Sie können den Wyse Geräte-Agent auf Windows-eingebetteten Standard-Geräten mithilfe einer der folgenden Methoden installieren oder aktualisieren:
  - [Manuelles Installieren von Wyse Geräte-Agent](#)
  - [Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie](#)
- **ANMERKUNG:** Sie können auch den Wyse Geräte-Agent manuell aktualisieren, indem Sie auf die neueste Version der Wyse Geräte-Agent-.exe-Datei doppelklicken.
- **ANMERKUNG:** Der Wyse Geräte-Agent kann nur auf dem Betriebssystem Windows Embedded Standard 7 installiert werden, wenn KB3033929 verfügbar ist.
- **Linux- und ThinLinux-Geräte** – Der Wyse Gerät-Agent kann auf Linux- und ThinLinux-Geräten mithilfe der Wyse Management Suite installiert oder aktualisiert werden. Weitere Informationen finden Sie unter [Installieren oder Aktualisieren von Wyse Geräte-Agenten auf ThinLinux- und Linux-Clients](#).

## Themen:

- [Manuelles Installieren von Wyse Geräte-Agenten auf einem Windows-eingebetteten Gerät](#)
- [Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie](#)
- [Installieren oder Aktualisieren von Wyse Geräte-Agenten auf ThinLinux- und Linux-Clients](#)

## Manuelles Installieren von Wyse Geräte-Agenten auf einem Windows-eingebetteten Gerät

### Schritte

1. Kopieren Sie die Datei `WDA.exe` in den Thin Client.
2. Doppelklicken Sie auf die Datei `WDA.exe`.
3. Klicken Sie auf **Ja**.
  - **ANMERKUNG:** Es wird eine Warnmeldung angezeigt, wenn eine ältere Version von Wyse Geräte-Agent oder HAgent auf dem Gerät installiert ist.
4. Geben Sie in das Feld **Gruppentoken** ein Gruppentoken ein. Dieses Feld ist optional. Wenn Sie diesen Schritt überspringen, klicken Sie auf **Weiter**. Sie können die Einzelheiten des Gruppentokens im weiteren Verlauf über die Wyse Geräte-Agent-Benutzeroberfläche eingeben.
5. Wählen Sie aus der Dropdownliste **Region** die Region des Public-Cloud-Servers der Wyse Management Suite. Nach der erfolgreichen Installation der Wyse Management Suite registriert der öffentliche Cloud-Server automatisch das Gerät in der Wyse Management Suite-Konsole.

# Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie

## Voraussetzungen

Dell empfiehlt die Verwendung der Wyse Management Suite-Anwendung für Upgrades des Wyse Geräte-Agents. In der Wyse Management Suite als private Cloud-Lösung sind die neuesten Wyse Geräte-Agent-Pakete für Windows Embedded Standard im lokalen Repository verfügbar. Wenn Sie mit einer öffentlichen Cloud oder einem Remote-Repository in einer privaten Cloud arbeiten, kopieren Sie die Datei `WDA.exe` in den Ordner `thinClientApps` im Repository.

## Schritte

1. Nachdem die Datei `WDA.exe` in das Repository kopiert wurde, gehen Sie zu **Apps & Daten** und erstellen Sie eine Standard-Anwendungsrichtlinie mit diesem Paket – siehe [Erstellen und Bereitstellen einer Standard-Anwendungsrichtlinie für Thin Clients](#).

**ANMERKUNG:** Eine erweiterte Anwendungsrichtlinie wird nur von Wyse Geräte-Agent ab Version 14.x unterstützt. Dell empfiehlt die Verwendung der normalen Anwendungsrichtlinie beim Upgrade des Wyse Geräte-Agents ab Version 14.x. Sie können auch die erweiterte Anwendungsrichtlinie für das Upgrade des Wyse Geräte-Agents von Version 14.x auf die neuesten Versionen verwenden.

2. Gehen Sie auf die Seite **Jobs** und planen Sie einen Job für das Upgrade des Wyse Geräte-Agents.

**ANMERKUNG:** Für das Upgrade eines Windows-eingebetteten Standard-Wyse Geräte-Agents von Version 13.x auf 14.x empfiehlt Dell, dass Sie HTTP als Repository-Protokoll verwenden.

Nach einer erfolgreichen Installation wird der Status an den Server gesendet.

# Installieren oder Aktualisieren von Wyse Geräte-Agenten auf ThinLinux- und Linux-Clients

## Voraussetzungen

- Um Wyse Geräte-Agenten auf Dell Wyse 3040 Thin Clients mit ThinLinux Version 2.0, Abbildversion 2.0.14 und Wyse Geräte-Agent-Version 3.0.7 zu installieren, müssen Sie die Datei `wda3040_3.0.10-01_amd64.deb` und anschließend die Datei `wda_3.2.12-01_amd64.tar` installieren.
- Sie müssen das Plattform-Dienstprogramm-Add-on und das Wyse Geräte-Agent-Add-on für Linux Thin Clients installieren. Sie können die Datei `wda_x.x.x.tar` für ThinLinux Thin Clients installieren.

## Info über diese Aufgabe

Sie können Add-ons über eine beliebige der folgenden Optionen installieren oder aktualisieren:

- Mit INI-Parametern
- Add-ons-Manager
- RPM-Befehle

## Schritte


1. Wenn Sie mit einer öffentlichen Cloud oder einem Remote-Repository in einer privaten Cloud arbeiten, kopieren Sie die RPM-Datei in den Ordner `thinClientApps` im Repository. Standardmäßig sind die aktuellsten Wyse Geräte-Agenten und die Plattform-Dienstprogramm-RPMs für Linux und ThinLinux Clients im lokalen Repository verfügbar.

2. Gehen Sie auf die Seite **Jobs** und planen Sie einen Job für das Upgrade des Plattform-Dienstprogramm-Add-Ons.

Sie müssen warten, bis das Plattform-Dienstprogramm-Add-On erfolgreich auf dem Thin Client installiert wurde.

**ANMERKUNG:** Installieren Sie zuerst das Plattform-Dienstprogramm-Add-On und installieren Sie dann ein Wyse Geräte-Agent-Add-On. Eine Installation des neuesten Wyse Geräte-Agents vor der Installation des aktuellen Plattform-Dienstprogramm-Add-Ons ist nicht möglich.

3. Planen Sie auf der Seite **Jobs** einen Job für das Upgrade des Wyse Geräte-Agents auf dem Client.

 **ANMERKUNG:** Der Linux-Client startet nach der Installation des Wyse Geräte-Agent-Add-ons Version 2.0.11 neu.

# Registrieren und Konfigurieren eines neuen Geräts mithilfe von Wyse Management Suite

## Themen:

- Registrieren und konfigurieren Sie ein neues Windows-eingebettetes Standard-Gerät mithilfe von Wyse Management Suite
- Registrieren und Konfigurieren eines neuen ThinOS-8.x-Geräts mithilfe von Wyse Management Suite
- Registrieren und Konfigurieren eines neuen ThinOS-9.x-Geräts mithilfe von Wyse Management Suite
- Registrieren und Konfigurieren eines neuen Linux- oder ThinLinux-Geräts mithilfe von Wyse Management Suite
- Registrieren und Konfigurieren eines neuen Wyse Software-Thin Clients mithilfe der Wyse Management Suite
- Registrieren und konfigurieren Sie den Dell Hybrid-Client mithilfe der Wyse Management Suite

## Registrieren und konfigurieren Sie ein neues Windows-eingebettetes Standard-Gerät mithilfe von Wyse Management Suite

### Schritte

1. Installieren Sie den Wyse Geräte-Agent auf Ihrem Thin Client – siehe [Installieren oder Aktualisieren des Wyse Geräte-Agent](#).
2. Registrieren Sie Ihren Thin Client für die Wyse Management Suite – siehe [Registrieren von Windows-eingebetteten Standard-Thin Clients bei Wyse Management Suite](#), indem Sie den Wyse Geräte-Agent verwenden.
  - i ANMERKUNG:** Sie können die Geräte auch mit einer der folgenden Methoden registrieren:
    - Verwenden von DHCP-Option-Tags – siehe [Registrieren von Geräten mithilfe von DHCP-Option-Tags](#).
    - Verwenden von DNS-SRV-Eintrag – siehe [Registrieren von Geräten mit DNS-SRV-Eintrag](#).
  - i ANMERKUNG:** Wenn die Option zur **Registrierungsvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Registrierungsvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Registrierung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben. Weitere Informationen zum Validieren der Geräte finden Sie unter [Registrierungsvalidierung](#).
3. Fügen Sie das Gerät zu Ihrer gewünschten Gruppe hinzu (optional) – siehe [Verwalten von Gruppen und Konfigurationen](#).
4. Konfigurieren Sie den Thin Client mit einer der folgenden Optionen:
  - Mithilfe der Seite **Gruppen und Konfigurationen** – siehe [Bearbeiten der Windows-eingebetteten Standard-Richtlinieneinstellungen](#).
  - Auf der **Seite „Geräte“** – siehe [Verwalten von Geräten](#).

## Registrieren und Konfigurieren eines neuen ThinOS-8.x-Geräts mithilfe von Wyse Management Suite

### Schritte

1. Klicken Sie im Desktopmenü des Thin Client 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 **Registrierungvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Registrierungvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Registrierung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben. Weitere Informationen zum Validieren der Geräte finden Sie unter [Registrierungvalidierung](#).

Das Gerät wird in der Wyse Management Suite registriert.

8. Melden Sie sich bei der Wyse Management Suite an.
9. Fügen Sie das Gerät zu Ihrer gewünschten Gruppe hinzu (optional) – siehe [Verwalten von Gruppen und Konfigurationen](#).
10. Konfigurieren Sie den Thin Client mit einer der folgenden Optionen:
  - Mithilfe der Seite **Gruppen und Konfigurationen** – siehe [Bearbeiten der ThinOS-Richtlinieneinstellungen](#).
  - Auf der **Seite „Geräte“** – siehe [Verwalten von Geräten](#).

## Registrieren und Konfigurieren eines neuen ThinOS-9.x-Geräts mithilfe von Wyse Management Suite

### Schritte

1. Klicken Sie im Desktopmenü des Thin Client 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. Öffentliche 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.

**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.

Es wird ein Fenster mit einer Warnung angezeigt.

7. Klicken Sie auf **OK**.
8. Klicken Sie im Fenster **Zentrale Konfiguration** auf **OK**.

- i ANMERKUNG:** Sie können die Geräte auch mit einer der folgenden Methoden registrieren:
- Verwenden von DHCP-Option-Tags – siehe [Registrieren von Geräten mithilfe von DHCP-Option-Tags](#).
  - Verwenden von DNS-SRV-Eintrag – siehe [Registrieren von Geräten mit DNS-SRV-Eintrag](#).
- i ANMERKUNG:** Wenn die Option zur **Registrierungsvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Registrierungsvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Registrierung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben. Weitere Informationen zum Validieren der Geräte finden Sie unter [Registrierungsvalidierung](#).

Das Gerät wird in der Wyse Management Suite registriert.

9. Melden Sie sich bei der Wyse Management Suite an.
10. Fügen Sie das Gerät zu Ihrer gewünschten Gruppe hinzu (optional) – siehe [Verwalten von Gruppen und Konfigurationen](#).
11. Konfigurieren Sie den Thin Client mit einer der folgenden Optionen:
  - Auf der Seite **Gruppen und Konfigurationen** – siehe [Bearbeiten der Richtlinien für die ThinOS-9.x-Einstellungen](#).
  - Auf der **Seite „Geräte“** – siehe [Verwalten von Geräten](#).

## Registrieren und Konfigurieren eines neuen Linux- oder ThinLinux-Geräts mithilfe von Wyse Management Suite

### Schritte

1. Installieren Sie den Wyse Geräte-Agent auf Ihrem Thin Client – siehe [Installieren oder Aktualisieren des Wyse Geräte-Agent](#).
2. Registrieren Sie Ihren Thin Client für die Wyse Management Suite – siehe [Registrieren von Linux/ThinLinux-Thin Clients für Wyse Management Suite unter Verwendung von Wyse Geräte-Agent](#).

**i ANMERKUNG:** Sie können die Geräte auch mit einer der folgenden Methoden registrieren:

  - Verwenden von DHCP-Option-Tags – siehe [Registrieren von Geräten mithilfe von DHCP-Option-Tags](#).
  - Verwenden von DNS-SRV-Eintrag – siehe [Registrieren von Geräten mit DNS-SRV-Eintrag](#).

**i ANMERKUNG:** Wenn die Option zur **Registrierungsvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Registrierungsvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Registrierung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben. Weitere Informationen zum Validieren der Geräte finden Sie unter [Registrierungsvalidierung](#).
3. Fügen Sie das Gerät zu Ihrer gewünschten Gruppe hinzu (optional) – siehe [Verwalten von Gruppen und Konfigurationen](#).
4. Konfigurieren Sie den Thin Client mit einer der folgenden Optionen:
  - Mithilfe der Seite **Gruppen und Konfigurationen** – siehe [Bearbeiten der ThinLinux-Richtlinieneinstellungen](#) oder [Bearbeiten der Einstellungen für die Linux-Richtlinie](#).
  - Auf der **Seite „Geräte“** – siehe [Verwalten von Geräten](#).

## Registrieren und Konfigurieren eines neuen Wyse Software-Thin Clients mithilfe der Wyse Management Suite

### Schritte

1. Installieren Sie den Wyse Geräte-Agent auf Ihrem Thin Client – siehe [Installieren oder Aktualisieren des Wyse Geräte-Agent](#).

2. Registrieren Sie Ihren Thin Client bei der Wyse Management Suite – siehe [Registrieren von Wyse Software-Thin Client bei der Wyse Management Suite mit Wyse Geräte-Agent](#).

**ANMERKUNG:** Sie können die Geräte auch mit einer der folgenden Methoden registrieren:

- Verwenden von DHCP-Option-Tags – siehe [Registrieren von Geräten mithilfe von DHCP-Option-Tags](#).
- Verwenden von DNS-SRV-Eintrag – siehe [Registrieren von Geräten mit DNS-SRV-Eintrag](#).

**ANMERKUNG:** Wenn die Option zur **Registrierungsvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Registrierungsvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Registrierung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben. Weitere Informationen zum Validieren der Geräte finden Sie unter [Registrierungsvalidierung](#).

3. Fügen Sie das Gerät zu Ihrer gewünschten Gruppe hinzu (optional) – siehe [Verwalten von Gruppen und Konfigurationen](#).

4. Konfigurieren Sie den Thin Client mit einer der folgenden Optionen:

- Auf der Seite **Gruppen und Konfigurationen** – siehe [Bearbeiten der Einstellungen für die Wyse Software Thin Client-Richtlinie](#).
- Auf der **Seite „Geräte“** – siehe [Verwalten von Geräten](#).


## Registrieren und konfigurieren Sie den Dell Hybrid-Client mithilfe der Wyse Management Suite

### Voraussetzungen

Stellen Sie vor der Registrierung des Geräts sicher, dass Ihr Gerät über eine Netzwerkverbindung verfügt, um den Wyse Management Suite Server zu kontaktieren.

**ANMERKUNG:** Sie können das Gerät nur über das Gast-Konto registrieren. Das gilt auch für das Aufheben der Registrierung.

### Schritte

1. Melden Sie sich beim Dell Hybrid-Client als Gastbenutzer an.
2. Klicken Sie in der oberen Leiste auf .

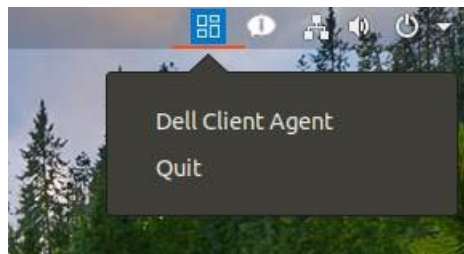


Abbildung 1. DCA-Symbol

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

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

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

Die Option CA-Validierung wird automatisch aktiviert und kann nicht deaktiviert werden, wenn die URL einer öffentlichen Cloud eingegeben wurde.

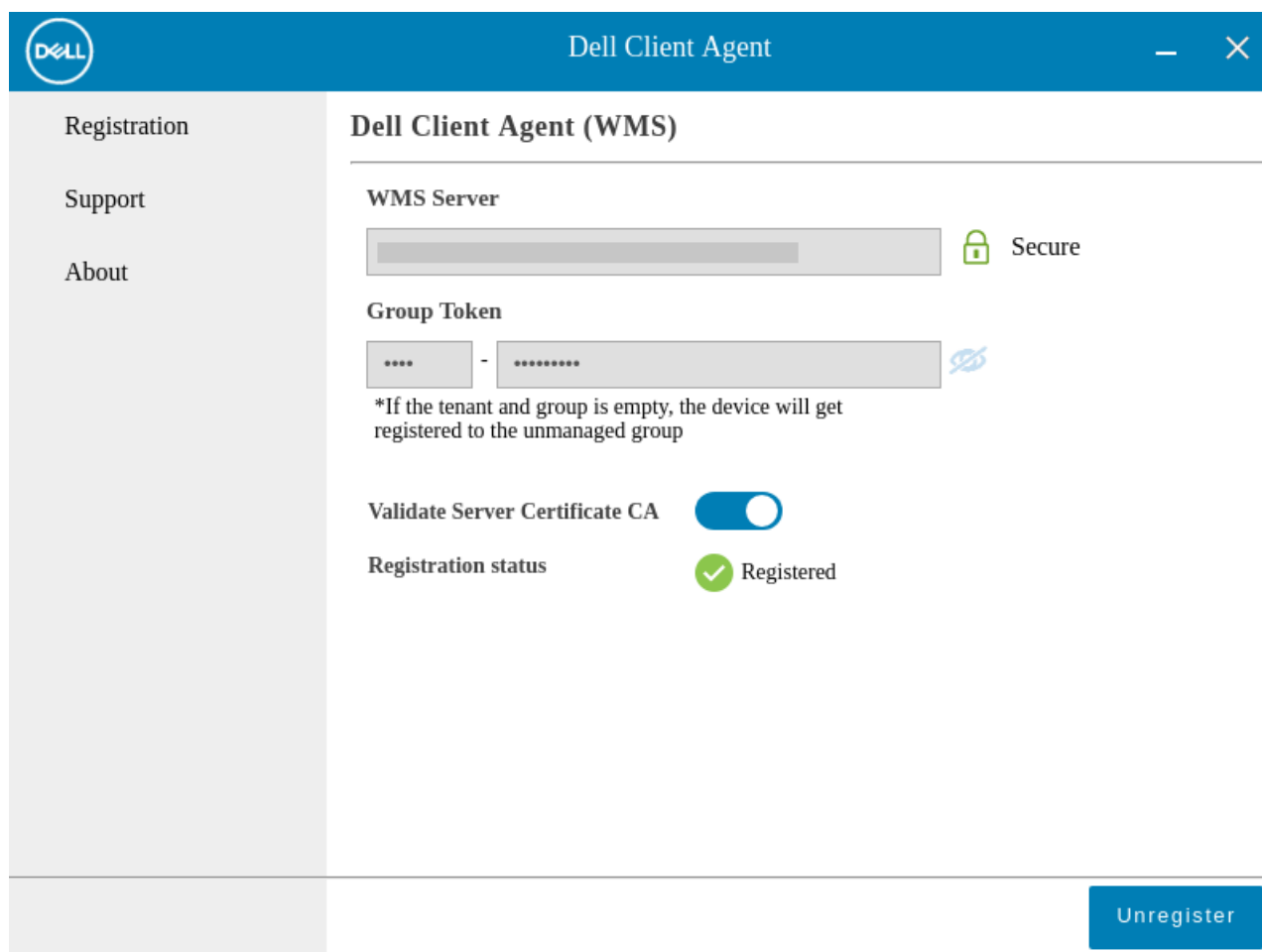
9. Klicken Sie auf **Registrieren**, um Ihren Hybrid Client auf dem Wyse Management Suite-Server zu registrieren.

Sie können die Geräte auch mit einer der folgenden Methoden registrieren:

- Verwenden von DHCP-Option-Tags – siehe [Registrieren von Geräten mithilfe von DHCP-Option-Tags](#).
- Verwenden von DNS-SRV-Eintrag – siehe [Registrieren von Geräten mit DNS-SRV-Eintrag](#).

**ANMERKUNG:** Wenn die Option zur **Registrierungsvalidierung** aktiviert ist, befinden sich die manuellen oder automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Registrierungsvalidierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Registrierung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben. Weitere Informationen zum Validieren der Geräte finden Sie unter [Registrierungsvalidierung](#).

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



**Abbildung 2. Dell Client Agent**

10. Melden Sie sich bei der Wyse Management Suite an.
11. Fügen Sie das Gerät zu Ihrer gewünschten Gruppe hinzu (optional) – siehe [Verwalten von Gruppen und Konfigurationen](#).
12. Konfigurieren Sie den Thin Client mit einer der folgenden Optionen:
  - Auf der Seite **Gruppen und Konfigurationen** – siehe [Bearbeiten der Einstellungen für die Dell Hybrid Client-Richtlinie](#).
  - Auf der **Seite „Geräte“** – siehe [Verwalten von Geräten](#).

# Wyse Management Suite-Dashboard

Die Seite **Dashboard** ermöglicht das Anzeigen des Status eines Systems und der letzten ausgeführten Aufgaben innerhalb des Systems. Zum Anzeigen einer bestimmten Warnung klicken Sie auf den Link im Abschnitt **Warnungen**. Die Seite **Dashboard** ermöglicht es Ihnen auch, eine Zusammenfassung des Geräts anzuzeigen.

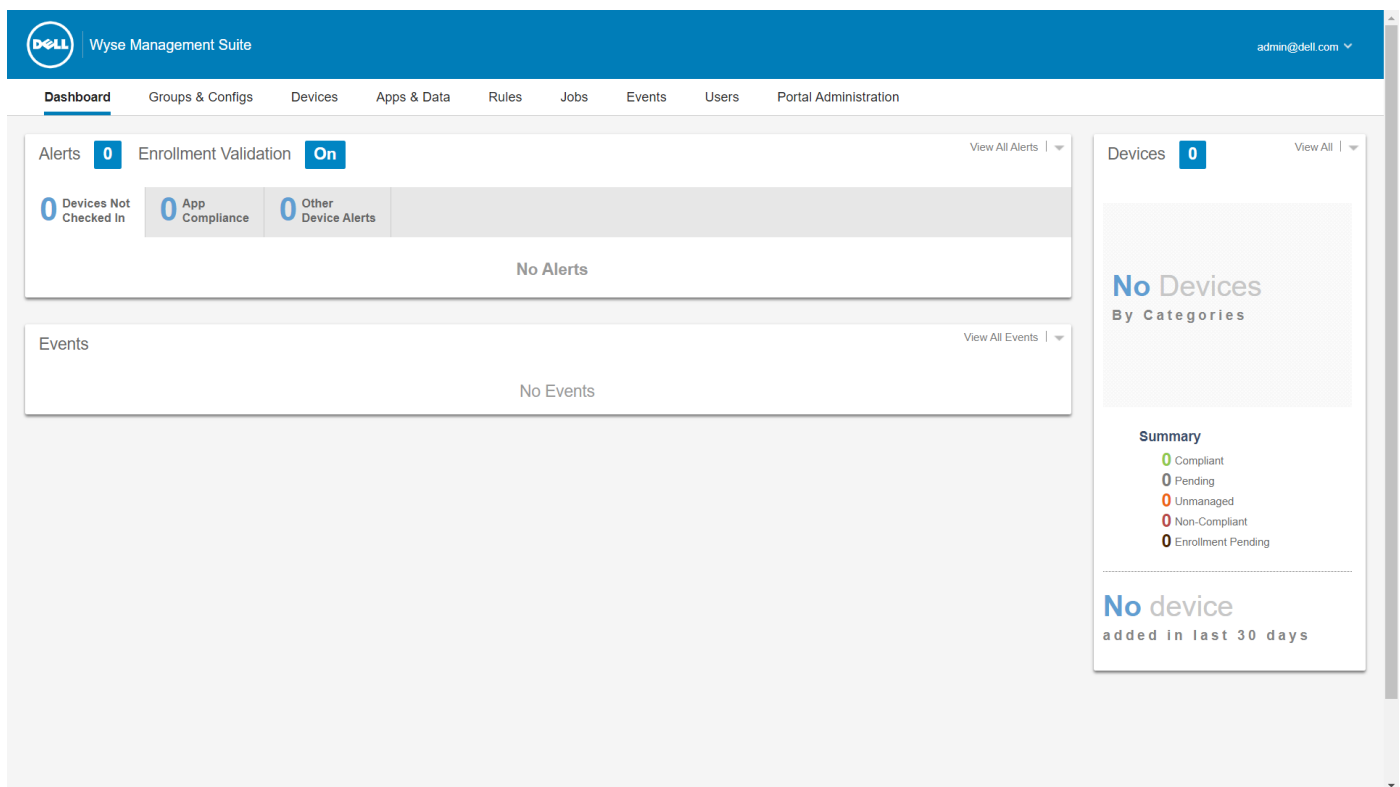


Abbildung 3. Dashboard

## Themen:

- Anzeigen von Warnungen
- Anzeigen der Ereignisliste
- Anzeigen des Gerätestatus
- Aktivieren der Anmeldevalidierung
- Ändern von Benutzereinstellungen
- Zugriff auf die Onlinehilfe
- Ändern Ihres Kennworts
- Abmelden von der Verwaltungskonsole

## Anzeigen von Warnungen

Im Bereich **Warnungen** wird die Zusammenfassung aller Warnungen angezeigt.

### Schritte

1. Klicken Sie auf **Dashboard**.  
Die Warnungsübersicht wird angezeigt.

2. Klicken Sie auf **Alle Warnungen anzeigen**.  
Die folgenden Optionen werden auf der Seite **Ereignisse** angezeigt:
  - **Gerät nicht eingecheckt**
  - **App-Konformität**
  - **Andere Gerätewarnungen**

## Anzeigen der Ereignisliste

Im Abschnitt **Ereignisse** wird die Zusammenfassung der Ereignisse der letzten Tage angezeigt.

### Schritte

1. Klicken Sie auf **Dashboard**.  
Die Ereignisübersicht wird angezeigt.
2. Klicken Sie auf **Alle Ereignisse anzeigen**.  
Die Seite **Ereignisse** wird angezeigt. Sie enthält eine Liste mit allen Ereignissen.

## Anzeigen des Gerätestatus

Der Abschnitt **Anzeige** enthält die Zusammenfassung der Gerätestatus.

### Schritte

1. Klicken Sie auf **Dashboard**.  
Es wird eine Geräteübersicht angezeigt.
2. Klicken Sie auf **Alle anzeigen**.  
Die Seite **Geräte** wird angezeigt. Sie enthält eine Liste mit allen registrierten Geräten. Der Abschnitt **Zusammenfassung** zeigt die Geräteanzahl auf Basis der folgenden Gerätestatuskategorie an:
  - **Konform**
  - **Ausstehend**
  - **Nicht verwaltet**
  - **Nicht konform**
  - **Anmeldung ausstehend**

## Aktivieren der Anmeldevalidierung

Sie können die **Anmeldung validieren**, damit Administratoren die manuelle und automatische Registrierung von Thin Clients in einer Gruppe steuern können.

### Schritte

1. Klicken Sie auf **Dashboard**.
2. Klicken Sie auf die Schaltfläche **EIN/AUS** neben der Option **Anmeldevalidierung**.  
Sie werden auf der Seite **Portalverwaltung** auf die Option **Andere Einstellungen** umgeleitet.
3. Aktivieren oder Deaktivieren der Option **Anmeldevalidierung**.

## Ändern von Benutzereinstellungen

So ändern Sie die Benutzereinstellungen wie z. B. Warnmeldung, Richtlinieneinstellungen und Seitengröße.

### Schritte

1. In der rechten oberen Ecke der Seite **Dashboard** klicken Sie auf die Anmeldungs-Dropdownliste.
2. Klicken Sie auf **Benutzereinstellungen**.  
Das Fenster **Benutzereinstellungen** wird angezeigt.

3. Klicken Sie auf **Warnungen** und wählen Sie die entsprechenden Kontrollkästchen für die Zuweisung eines Warnungstyps (Kritisch, Warnung oder Info) für Benachrichtigungen aus Ihre E-Mails und mobilen Anwendungen aus.
4. Klicken Sie auf **Richtlinien** und wählen Sie das Kontrollkästchen **Fragen, ob der ThinOS-Assistentenmodus verwendet werden soll**, um das Fenster **ThinOS-Konfigurationsmodus auswählen** jedes Mal anzuzeigen, wenn Sie die ThinOS-Richtlinieneinstellungen konfigurieren.
5. Klicken Sie auf **Seitengröße** und geben Sie eine Zahl zwischen 10 und 100 im Textfeld **Anzahl der Elemente pro Seite** ein. Mithilfe dieser Option können Sie die Anzahl der auf jeder Seite angezeigten Elemente festlegen.

## Zugriff auf die Onlinehilfe

### Schritte

1. In der rechten oberen Ecke der Seite **Dashboard** klicken Sie auf die Anmeldungs-Dropdownliste.
2. Klicken Sie auf **WMS Hilfe**.  
Die Seite **Support für Wyse Management Suite** wird angezeigt.

## Ändern Ihres Kennworts

### Schritte

1. In der rechten oberen Ecke der Seite **Dashboard** klicken Sie auf die Anmeldungs-Dropdownliste.
2. Klicken Sie auf **Kennwort ändern**.  
Daraufhin wird das Fenster **Kennwort ändern** angezeigt.
3. Geben Sie das aktuelle Kennwort ein.
4. Neues Kennwort eingeben.
5. Geben Sie das neue Kennwort zur Bestätigung erneut ein.
6. Klicken Sie auf **Kennwort ändern**.

## Abmelden von der Verwaltungskonsole

### Schritte

1. In der rechten oberen Ecke der Seite **Dashboard** klicken Sie auf die Anmeldungs-Dropdownliste.
2. Klicken Sie auf **Abmelden**.

# Verwalten von Gruppen und Konfigurationen

Die Seite **Gruppen und Konfigurationen** ermöglicht es Ihnen, Richtlinien festzulegen, die erforderlich sind, um Ihre Geräte zu konfigurieren. Sie können Untergruppen der globalen Gruppenrichtlinien erstellen und Geräte basierend auf Ihren Anforderungen kategorisieren. Beispielsweise können Geräte nach Stellenfunktion, Gerätetyp und so weiter untergliedert werden.

Für jede Gruppe können Sie Richtlinien für die folgenden Betriebssysteme festlegen:

- **ThinOS**
  - **ThinOS**
  - **ThinOS 9.x**
- **WES**
- **Linux**
- **ThinLinux**
- **Teradici**
- **Wyse Software Thin Client**
- **Hybrid Client**

Geräte erben Richtlinien in der Reihenfolge, in der sie erstellt werden. Die in der Standardrichtliniengruppe konfigurierten Einstellungen werden als Standardeinstellungen in allen Richtlinien angewendet, die in der Standardrichtliniengruppe aufgeführt sind. In einer Gruppe haben alle Geräte, die in dieser Gruppe vorhanden sind, die Standardrichtliniengruppe als den Standardwert eingestellt.

Auf der Seite **Gerätedetails** können Sie eine Ausnahme für ein Gerät in der Gruppe erstellen, sodass es eine Teilmenge von Richtlinien nutzt, die sich von den Standardeinstellungen der Gruppe unterscheiden.

Die Konfiguration für eine bestimmte Ressource mit Einzelheiten dazu, wo Konfigurationen festgelegt werden (global, auf Gruppen- oder Geräteebene), werden auf der Seite angezeigt. Die Option zum Erstellen von Ausnahmen ist auf der Seite verfügbar. Die **Ausnahme**-Einstellungen gelten nur für die ausgewählten Geräte.

**i ANMERKUNG:** Beim Ändern der Richtlinien auf niedrigeren Ebenen, wird ein Punkt-Symbol neben der Richtlinie angezeigt. Dieses Symbol weist darauf hin, dass diese Richtlinie eine Richtlinie auf einer höheren Ebene überschreibt. Beispiel: Systempersonalisierung, Netzwerke, Sicherheit usw. Wenn Sie Richtlinien ändern, wird ein Sternchen (\*) neben der Richtlinie angezeigt. Dieses Symbol weist darauf hin, dass ungespeicherte oder unveröffentlichte Änderungen vorhanden sind. Zum Überprüfen dieser Änderungen vor der Veröffentlichung klicken Sie auf den Link **Ausstehende Änderungen anzeigen**.

Falls eine Richtlinienkonfiguration zwischen den verschiedenen Ebenen priorisiert werden muss, hat immer die Richtlinie auf unterster Ebene Vorrang.

Nach dem Konfigurieren der Richtlinieneinstellungen werden die Thin Clients über die Änderungen benachrichtigt. Die Änderungen werden sofort nach der Konfiguration der Thin Clients übernommen.

**i ANMERKUNG:** Gewisse Einstellungen, wie z. B. die BIOS-Konfiguration für Windows-eingebetteten Standard machen einen Neustart erforderlich, damit die Änderungen wirksam werden. Jedoch müssen Sie das Gerät neu starten, damit die meisten Einstellungen auf ThinOS wirksam werden.

Die Richtlinien werden in der folgenden Reihenfolge angewendet:

- Richtlinie der globalen Ebene
- Richtlinien der Gerätegruppenebene
- Geräteausnahmen
- Richtlinien der Nutzergruppenebene
- Benutzerausnahmen
- Benutzerpersonalisierung

## Themen:

- [Bearbeiten einer nicht verwalteten Gruppe](#)
- [Erstellen einer Standard-Geräterichtliniengruppe](#)
- [Erstellen einer Nutzerrichtliniengruppe](#)
- [Konfigurieren von Richtlinien der Globalen Klasse](#)

- Importieren einer Nutzerrichtliniengruppe
- Entfernen einer Gruppe
- Konfigurieren von Richtlinien der Geräteklasse
- Gruppenrichtlinien exportieren
- Importieren von Gruppenrichtlinien
- Bearbeiten der Einstellungen für ThinOS-Richtlinien
- Bearbeiten der Einstellungen für ThinOS-9.x-Richtlinien
- Bearbeiten von Windows Embedded Standard-Richtlinieneinstellungen
- Bearbeiten der Einstellungen für die Linux-Richtlinie
- Bearbeiten der Einstellungen für die ThinLinux-Richtlinie
- Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen
- Bearbeiten der Einstellungen für die Cloud Connect-Richtlinieneinstellungen
- Bearbeiten der Einstellungen der Dell Hybrid Client-Richtlinien
- Erstellen und Importieren einer Ausnahmedatei für ein Massenspeichergerät

## Bearbeiten einer nicht verwalteten Gruppe

Geräte, die der nicht verwalteten Gruppe angehören, verwenden keine Lizenzen oder empfangen Konfigurationen oder anwendungs-basierte Richtlinien. Zum Hinzufügen von Geräten zu einer nicht verwalteten Gruppe verwenden Sie den Geräte-registrierungsschlüssel für die nicht verwaltete Gruppe im Rahmen der automatischen Registrierung oder der manuellen Registrierung.

### Schritte

1. Wählen Sie auf der Seite **Gruppen und Konfigurationen nicht verwaltete Gruppe** aus.

2. Klicken Sie auf .

Die Seite **Nicht verwaltete Gruppe bearbeiten** wird angezeigt. Der **Gruppenname** zeigt den Namen der Gruppe an.

3. Bearbeiten Sie die folgenden Details:

- **Beschreibung** – Zeigt eine kurze Beschreibung der Gruppe an.
- **Gruppentoken** – Wählen Sie diese Option aus, um das Gruppentoken zu aktivieren.

4. Klicken Sie auf **Speichern**.



**ANMERKUNG:** Bei einer öffentlichen Cloud muss der Gruppentoken für eine nicht verwaltete Gruppe aktiviert sein, um Geräte zu registrieren. Bei einer privaten Cloud wird der Gruppentoken für eine nicht verwaltete Gruppe automatisch aktiviert.

## Erstellen einer Standard-Geräterichtliniengruppe

Sie können Untergruppen der globalen Gruppenrichtlinie erstellen und Geräte basierend auf Ihren Anforderungen kategorisieren.

### Schritte

1. Klicken Sie auf der Seite **Gruppen und Konfigurationen** auf das Symbol **Standard-Geräterichtliniengruppe**.

2. Klicken Sie auf .

3. Im Dialogfeld **Hinzufügen neuer Gruppe** geben Sie den **Gruppennamen** und eine **Beschreibung** ein.

4. Wählen Sie die Option **Dies ist eine übergeordnete ThinOS-Auswahlgruppe** aus, um eine übergeordnete Auswahlgruppe für ThinOS-Geräte zu erstellen. Dieser Schritt ist optional.

Weitere Informationen finden Sie unter [Erstellen einer ThinOS-Auswahlgruppe](#).


5. Aktivieren Sie auf der Registerkarte **Registrierung** das Kontrollkästchen **Aktiviert** unter Gruppentoken.

6. Geben Sie das Gruppentoken ein.

7. Auf der Registerkarte **Verwaltung** können Sie den Namen der Gruppenadministratoren auswählen, die diese Gruppe verwalten sollten. Wählen Sie im Feld **Verfügbare Gruppenadministratoren** die betreffende Gruppe aus und klicken Sie dann auf den Rechtspfeil, um sie in das Feld **Zugewiesene Gruppenadministratoren** zu verschieben. Zum Verschieben einer Gruppe von **Zugewiesene Gruppenadministratoren** nach **Verfügbare Gruppenadministratoren** gehen Sie umgekehrt vor. Dieser Schritt ist optional.


8. Klicken Sie auf **Speichern**.

Die Gruppe wird der Liste verfügbarer Gruppen auf der Seite **Gruppen und Konfigurationen** hinzugefügt.

 **ANMERKUNG:** Die Geräte können in einer Gruppe registriert werden, indem Sie das Gruppentoken eingeben, das auf der Seite **Gruppen und Konfigurationen** für die entsprechende Gruppe verfügbar ist.


## Erstellen einer ThinOS-Auswahlgruppe


### Schritte

1. Klicken Sie auf der Seite **Gruppen und Konfigurationen** auf das Symbol **Standard-Geräterichtliniengruppe**.
2. Klicken Sie auf .
3. Im Dialogfeld **Hinzufügen neuer Gruppe** geben Sie den **Gruppennamen** und eine **Beschreibung** ein.
4. Wählen Sie die Option **Dies ist eine übergeordnete ThinOS-Auswahlgruppe**.
5. Wählen Sie den Namen der Gruppenadministratoren aus, die für die Verwaltung dieser Gruppe zuständig sind. Wählen Sie im Feld **Verfügbare Gruppenadministratoren** die betreffende Gruppe aus und klicken Sie dann auf den Rechtspfeil, um sie in das Feld **Zugewiesene Gruppenadministratoren** zu verschieben. Zum Verschieben einer Gruppe von **Zugewiesene Gruppenadministratoren** nach **Verfügbare Gruppenadministratoren** gehen Sie umgekehrt vor. Dieser Schritt ist optional.
6. Klicken Sie auf **Speichern**.

Die Gruppe wird der Liste verfügbarer Gruppen auf der Seite **Gruppen und Konfigurationen** hinzugefügt.

Um Untergruppen zur erstellten übergeordneten Gruppe hinzuzufügen, klicken Sie auf der Seite **Gruppen & Konfigurationen** auf die übergeordnete Gruppe und befolgen Sie die Schritte, die in [Erstellen der Gerärichtliniengruppe](#) beschrieben sind.

 **ANMERKUNG:** Die übergeordnete Auswahlgruppe kann 10 untergeordnete Auswahlgruppen haben und Sie können die Geräte für untergeordnete Auswahlgruppe registrieren.

 **ANMERKUNG:** Profile können für andere Betriebssysteme konfiguriert werden. Die erstellten Profile sind identisch mit anderen benutzerdefinierten Gruppen.


## Bearbeiten einer Standard-Geräterichtliniengruppe

### Schritte

1. Navigieren Sie zur Seite **Gruppen und Konfigurationen** und wählen Sie die **Standard-Geräterichtliniengruppe** aus.
2. Bearbeiten Sie im Dialogfeld **Standard-Geräterichtliniengruppe bearbeiten** die erforderlichen Gruppeninformationen.
3. Klicken Sie auf **Speichern**.

## Bearbeiten einer ThinOS-Auswahlgruppe




### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und klicken Sie auf die ThinOS-Auswahlgruppe, die Sie bearbeiten möchten.
2. Klicken Sie auf .
3. Bearbeiten Sie im Dialogfeld **Standardrichtliniengruppe bearbeiten** die Gruppeninformationen wie z. B. **Gruppenname** und **Beschreibung**.
4. Wählen Sie auf der Registerkarte **Verwaltung** den Namen der Gruppenadministratoren aus, die diese Gruppe verwalten sollten. Wählen Sie im Feld **Verfügbare Gruppenadministratoren** die betreffende Gruppe aus und klicken Sie dann auf den Rechtspfeil, um sie in das Feld **Zugewiesene Gruppenadministratoren** zu verschieben. Zum Verschieben einer Gruppe von **Zugewiesene Gruppenadministratoren** nach **Verfügbare Gruppenadministratoren** klicken Sie den Pfeil nach links. Dieser Schritt ist optional.
5. Klicken Sie auf **Speichern**.

## Entfernen einer ThinOS-Auswahlgruppe

Als Administrator können Sie eine Gruppe aus der Gruppenhierarchie entfernen.


### Schritte

1. Auf der Registerkarte **Gruppen & Konfigurationen** wählen Sie die ThinOS-Auswahlgruppe, die Sie löschen möchten.
2. Klicken Sie auf .  
Eine Warnmeldung, die darauf hinweist, dass diese Maßnahme eine oder mehrere Gruppen aus der Gruppenstruktur-Hierarchie entfernt, wird angezeigt.
3. Wählen Sie in der Dropdownliste „Gruppen“ eine neue Gruppe für Benutzer und Geräte in der aktuellen Gruppe aus.
4. Klicken Sie auf **Gruppe entfernen**.
  -  **ANMERKUNG:** Wenn Sie eine Gruppe aus der Gruppenhierarchie entfernen, werden alle Benutzer und Geräte, die zu der gelöschten Gruppe gehören, in die benutzerdefinierte, Standard- oder nicht verwaltete Gruppe verschoben.
  -  **ANMERKUNG:** Wenn Sie die Auswahlgruppe löschen, können die Geräte der entfernten Gruppe nicht in eine andere Auswahlgruppe verschoben werden.

## Erstellen einer Nutzerrichtliniengruppe

Sie können Untergruppen der globalen Nutzergruppenrichtlinien erstellen und Nutzer basierend auf ihren Nutzergruppen kategorisieren.

### Schritte

1. Klicken Sie auf der Seite **Gruppen und Konfigurationen** auf die Option **Standard-Nutzerrichtliniengruppe**.
2. Klicken Sie auf .
3. Geben Sie im Dialogfeld **Neue Gruppe hinzufügen** den **Gruppennamen**, die **Beschreibung**, die **Domain**, das **AD-Attribut** (AD-Gruppe oder die OU-Gruppe) und den **AD-Attributnamen** ein, der in der AD-Domain vorhanden ist. Sie müssen den **Gruppennamen** als **AD-Attributnamen** verwenden.

## Add New Group X

**Group Name**  \*

**Description**  \*

**Parent Group** **Default User Policy Group**

**Domain**  \*

**AD Attribute** AD group ?

**AD Attribute Name**  \*

---

**Administration**
Device Group Mapping

---

**Select which group admin(s) will be managing this group (Optional).**

**Available Group Admins**

>  
<

**Assigned Group Admins**

Cancel
Save

**Abbildung 4. Hinzufügen einer neuen Gruppe**


**ANMERKUNG:** Wenn die AD-Gruppe sich innerhalb einer OU-Gruppe in der Domain befindet, müssen Sie die OU-Gruppe als AD-Attribut auswählen.

4. Wählen Sie den Namen der Gruppenadministratoren aus, die für die Verwaltung dieser Gruppe zuständig sind.
5. Wählen Sie im Feld **Verfügbare Gruppenadministratoren** die betreffende Gruppe aus und klicken Sie dann auf den Rechtspfeil, um sie in das Feld **Zugewiesene Gruppenadministratoren** zu verschieben.  
Zum Verschieben einer Gruppe von **Zugewiesene Gruppenadministratoren** nach **Verfügbare Gruppenadministratoren** gehen Sie umgekehrt vor.
6. Klicken Sie auf **Speichern**.  
Die Gruppe wird der Liste verfügbarer Gruppen auf der Seite **Gruppen und Konfigurationen** hinzugefügt.

 **ANMERKUNG:** Eine Nutzerrichtliniengruppe muss einer AD-Gruppe oder einer Organisationseinheit zugeordnet sein, jedoch nicht beiden.


7. Wählen Sie die Option **Gerätegruppenzuordnung** aus, um Nutzergruppen mit Gerätezuordnung zu importieren, um die Konfigurationen zu steuern, die standardmäßig auf alle Gerätegruppen angewendet werden.

AD-Nutzergruppen, die in die Wyse Management Suite importiert wurden, können der jeweiligen Gerätegruppe zugeordnet werden. Durch Zuordnung der Geräte erhalten Sie keine unerwünschten Nutzergruppen-Richtlinien.

 **ANMERKUNG:** Standardmäßig sind Nutzergruppen nicht einer Gerätegruppe zugeordnet. Wenn Sie die **Standard-Gerätegruppen**-Richtlinie auswählen, werden alle Untergerätegruppen ausgewählt. Diese Funktion ist nur für die Pro-Lizenz der Wyse Management Suite verfügbar. Sie können 100 Nutzergruppen in die Wyse Management Suite importieren.

## Bearbeiten der Nutzerrichtliniengruppe

### Schritte

1. Navigieren Sie zur Seite **Gruppen und Konfigurationen** und wählen Sie die standardmäßige Nutzerrichtliniengruppe aus.
2. Klicken Sie auf .
3. Bearbeiten Sie im Dialogfeld **Standard-Nutzerrichtliniengruppe bearbeiten** die erforderlichen Gruppeninformationen.
4. Klicken Sie auf **Speichern**.


## Konfigurieren von Richtlinien der Globalen Klasse

### Schritte

1. Wählen Sie auf der Seite **Gruppen und Konfigurationen** aus der Dropdownliste **Richtlinien bearbeiten** den Gerätetyp aus. Die Richtlinieneinstellungen des entsprechenden Gerätetyps werden angezeigt.
2. Wählen Sie die Richtlinieneinstellung aus, die Sie konfigurieren möchten, und klicken Sie dann auf **Dieses Element konfigurieren**.
3. Klicken Sie nach der Konfiguration der Optionen auf **Speichern und veröffentlichen**.


## Importieren einer Nutzerrichtliniengruppe

### Schritte

1. Klicken Sie auf der Seite **Gruppen und Konfigurationen** auf die Option **Standard-Nutzerrichtliniengruppe**.
2. Klicken Sie auf .
3. Klicken Sie im Dialogfeld **Massenimport** auf **Durchsuchen** und wählen Sie die .csv-Datei.

Die .csv-Datei muss die Details in der folgenden Reihenfolge enthalten:

- Gruppenname – Anzeigename
- Beschreibung
- Domain – Domänenname
- AD-Attribut – AD-Gruppe oder OU-Gruppe
- AD-Attributname – Gruppenname in AD-Domain vorhanden


 **ANMERKUNG:** Sie müssen den Gruppennamen als AD-Attributnamen verwenden. Außerdem müssen Sie, wenn sich die AD-Gruppe innerhalb einer OU-Gruppe in der Domain befindet, die **OU-Gruppe** als **AD-Attribut** auswählen.


4. Aktivieren Sie das Kontrollkästchen **CSV Datei hat eine Kopfzeile**, wenn die CSV-Datei eine Kopfzeile enthält.
5. Klicken Sie auf **Importieren**.

# Entfernen einer Gruppe

Als Administrator können Sie eine Gruppe aus der Gruppenhierarchie entfernen.

## Schritte

1. Auf der Seite **Gruppen & Konfigurationen** wählen Sie die Gruppe, die Sie löschen möchten.
2. Klicken Sie auf .  
Eine Warnmeldung, die darauf hinweist, dass diese Maßnahme eine oder mehrere Gruppen aus der Gruppenstruktur-Hierarchie entfernt, wird angezeigt.
3. Wählen Sie in der Dropdownliste eine neue Gruppe, um die Benutzer und Geräte in die aktuelle Gruppe zu verschieben.
4. Klicken Sie auf **Gruppe entfernen**.

 **ANMERKUNG:** Wenn eine Gerätegruppe gelöscht wird, werden alle Geräte der Gruppe in eine ausgewählte Gerätegruppe verschoben. Wenn eine Nutzergruppe gelöscht wird, gibt es keine Geräte oder Benutzer, die mit ihr verknüpft sind.

# Konfigurieren von Richtlinien der Geräteklasse

## Schritte


1. Wählen Sie das Gerät, das Sie konfigurieren möchten, auf der Seite **Geräte** aus.  
Die Seite **Gerätedetails** wird angezeigt.
2. Klicken Sie im Abschnitt **Gerätekonfiguration** auf **Ausnahmen erstellen/bearbeiten**.


# Gruppenrichtlinien exportieren

Mit der Option **Richtlinien exportieren** können Sie die Richtlinien aus der aktuellen Gruppe exportieren. Diese Option ist für Benutzer mit Wyse Management Suite Pro-Lizenz verfügbar.

## Schritte

1. Wählen Sie auf der Seite **Gruppen und Konfigurationen** die Gruppe aus, aus der Sie Richtlinien exportieren möchten. Für die Gruppe müssen Richtlinien konfiguriert sein.
2. Klicken Sie auf **Richtlinien exportieren**.  
Der Bildschirm **Richtlinien exportieren** wird angezeigt.
3. Wählen Sie die zu exportierenden Gerätetypen aus.  
Die folgenden Optionen stehen zur Verfügung:
  - Alle Gerätetypen: Alle Gerätetyp-Richtlinien werden exportiert.
  - Spezifische Gerätetypen: Wählen Sie einen oder mehrere Gerätetypen aus der Dropdown-Liste aus. Nur die ausgewählten Gerätetypen werden exportiert.
4. Klicken Sie auf die Schaltfläche **Ja**, um die ausgewählten Gerätetypen zu exportieren.  
Übergeordnete Gruppenrichtlinien werden nicht exportiert. Es werden nur Richtlinien exportiert, die auf der ausgewählten oder Zielgruppen-Ebene konfiguriert sind.
5. Klicken Sie auf den Download-Link oder mit der rechten Maustaste auf die Datei und anschließend auf **Speichern unter**, um die JSON-Datei zu speichern.

 **ANMERKUNG:** Die Kennwörter werden in der exportierten Datei verschlüsselt. Der Dateiname ist im Format [Group Name]-[ALL]-[Exported Date & Time]UTC.json.

 **ANMERKUNG:** Um zu vermeiden dass ein Richtlinienimport fehlschlägt, stellen Sie sicher, dass Sie Kennwörter und alle Verweise auf Dateien wie Zertifikat, Hintergrundbild, Firmware, Logo usw. entfernen, bevor Sie in eine Datei exportieren.

# Importieren von Gruppenrichtlinien

Die Option **Richtlinien importieren** ermöglicht das Importieren der Richtlinien. Diese Option ist für Benutzer mit Wyse Management Suite PRO-Lizenz verfügbar. Sie können die Gruppenrichtlinien von der Seite **Gruppen und Konfigurationen** oder von der Seite **Richtlinien bearbeiten** importieren.

## Importieren von Gruppenrichtlinien aus Gruppen- und Konfigurationen-Seite

### Schritte

1. Wählen Sie auf der Seite **Gruppen und Konfigurationen** die gewünschte Gruppe aus.  
Wenn die Zielgruppe Richtlinien des gleichen Gerätetyps wie die importierten enthält, werden sie entfernt und neue hinzugefügt.
2. Klicken Sie auf **Richtlinien importieren**.  
Daraufhin wird der Bildschirm **Assistent zum Import von Richtlinien** angezeigt.
3. Wählen Sie den Modus zum Importieren der Gruppenrichtlinien aus der ausgewählten Gruppe.  
Die folgenden Optionen stehen zur Verfügung:
  - Aus einer vorhandenen Gruppe: Wählen Sie eine Gruppe aus der Dropdown-Liste aus. Richtlinien aus dieser Gruppe werden in die aktuelle Gruppe kopiert.
  - Aus einer exportierten Datei – suchen Sie die Datei `.json`. Richtlinien aus dieser Datei werden in die aktuelle Gruppe kopiert.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie die zu importierenden Gerätetypkonfigurationen aus.  
Die folgenden Optionen stehen zur Verfügung:
  - Alle Gerätetyprichtlinien: Alle konfigurierten Gerätetyprichtlinien werden in die aktuelle Gruppe importiert.
  - Spezifische Gerätetyprichtlinien: Wählen Sie einen oder mehrere Gerätetypen aus der Dropdown-Liste aus. Nur die ausgewählten Gerätetyprichtlinien werden in die aktuelle Gruppe importiert.
6. Klicken Sie auf **Weiter**.  
Eine Vorschau der Richtlinien in der ausgewählten Gruppe wird angezeigt.
7. Klicken Sie auf **Weiter**.  
Die Zusammenfassung des Importvorgangs wird angezeigt. Die folgenden Arten von Warnungen können angezeigt werden:
  - **Importierte <Betriebssystemtyp>-Richtlinien werden auf die Gruppe <Gruppenname> angewendet:** Diese Warnung wird angezeigt, wenn Sie die Betriebssystemkonfigurationen in eine Gruppe importieren, die keine der Konfigurationen enthält.
  - **<Betriebssystemtyp>-Richtlinie existiert bereits für die Gruppe <Gruppenname>. Vorhandene <Betriebssystemtyp>-Richtlinien werden entfernt, Richtlinien werden angewendet:** Diese Warnung wird angezeigt, wenn Sie neue Betriebssystemtypkonfigurationen in eine Gruppe importieren, die die Betriebssystemtypkonfigurationen enthält.
  - **Das Importieren von Richtlinien aus einer Datei, die Abhängigkeiten enthält, in Bestandsaufnahme-dateien schlägt fehl. Um diesen Import zu ermöglichen, verwenden Sie die Importoption aus dem Fenster "Richtlinien bearbeiten":** Diese Warnung wird angezeigt, wenn Sie die Gerätetypkonfigurationen aus einer Datei importieren, die Verweise auf Bestandsaufnahme-dateien enthält.
8. Klicken Sie auf **Importieren**.
  - ANMERKUNG:** Nur die ausgewählten Gerätetypkonfigurationen können importiert werden. Die Richtlinien, die in der Zielgruppe für den ausgewählten Gerätetyp definiert sind, werden entfernt, bevor die neuen Richtlinien des gleichen Gerätetyps angewendet werden.
  - ANMERKUNG:** Beim Importieren der Gruppenrichtlinien werden die Kennwörter und Referenzdateien nicht importiert. Der Administrator muss sie vor dem Veröffentlichen der Richtlinie auswählen.

## Importieren von Gruppenrichtlinien von der Seite „Richtlinien bearbeiten“

### Schritte

1. Wählen Sie auf der Seite **Gruppen und Konfigurationen** die gewünschte Gruppe aus.

2. Klicken Sie auf **Richtlinien bearbeiten** und wählen Sie die gewünschte Option.
3. Klicken Sie auf **Importieren**.  
Daraufhin wird der Bildschirm **Assistent zum Import von Richtlinien** angezeigt.
4. Wählen Sie den Modus zum Importieren der Gruppenrichtlinien aus der ausgewählten Gruppe. Die folgenden Optionen stehen zur Verfügung:
  - Aus einer vorhandenen Gruppe: Wählen Sie eine Gruppe aus der Dropdown-Liste aus. Richtlinien aus dieser Gruppe werden in die aktuelle Gruppe kopiert.
  - Aus einer exportierten Datei – klicken Sie auf **Durchsuchen** und wählen Sie die .JSON-Datei aus. Richtlinien aus dieser Datei werden in die aktuelle Gruppe kopiert.
5. Klicken Sie auf **Weiter**.  
Eine Vorschau der Richtlinien in der ausgewählten Gruppe wird angezeigt.
6. Klicken Sie auf **Weiter**. Die Zusammenfassung des Importvorgangs wird angezeigt. Die folgenden Arten von Warnungen können angezeigt werden:
  - **Importierte <Gerätetyp>-Richtlinien werden auf die Gruppe <Gruppenname> angewendet** – Diese Warnung wird angezeigt, wenn Sie die Gerätetypkonfigurationen in eine Gruppe importieren, die keine dieser Gerätetypkonfigurationen enthält.
  - **<Gerätetyp>-Richtlinie existiert bereits für die Gruppe <Gruppenname>. Vorhandene <Gerätetyp>-Richtlinien werden entfernt und importierte Richtlinien werden angewendet** – Diese Warnung wird angezeigt, wenn Sie die Gerätetypkonfigurationen in eine Gruppe importieren, die die Gerätetypkonfigurationen enthält.
  - **Das Importieren von Richtlinien aus einer Datei, die Abhängigkeiten enthält, in Bestandsaufnahme Dateien schlägt fehl. Um diesen Import zu ermöglichen, verwenden Sie die Importoption aus dem Fenster „Richtlinien bearbeiten“** – Diese Warnung wird angezeigt, wenn Sie die Gerätetypkonfigurationen aus einer Datei importieren, die Verweise auf Bestandsaufnahme Dateien enthält.
7. Klicken Sie auf **Importieren**.
  - i ANMERKUNG:** Wenn Sie eine Richtlinie aus einer Datei importieren und Verweise oder ungültige Abhängigkeiten existieren, schlägt der Import fehl und es wird eine Fehlermeldung angezeigt. Wenn die zu importierende Datei über eine Referenz oder eine Abhängigkeitsdatei verfügt, gehen Sie zu der Seite **Richtlinie bearbeiten** des jeweiligen Gerätetyps und importieren Sie dann die Gruppenrichtlinien.
  - i ANMERKUNG:** Sie können Gruppenrichtlinien mithilfe einer Datei von einem Gerät zu einer Nutzergruppe und umgekehrt importieren oder exportieren oder von einer Gruppe zu einer anderen. Die nicht unterstützten Konfigurationen, z. B. BIOS, Domänenbeitritt usw., werden ignoriert, wenn Sie Konfigurationen in eine Nutzergruppe importieren.

## Ergebnisse

Wenn die Zielgruppe Richtlinien des gleichen Gerätetyps wie die importierten enthält, werden sie entfernt und neue hinzugefügt.

- i ANMERKUNG:** Beim Importieren der Gruppenrichtlinien werden die Kennwörter nicht importiert. Der Administrator muss das Kennwort in allen Kennwortfeldern erneut eingeben.

# Bearbeiten der Einstellungen für ThinOS-Richtlinien

## Schritte

1. Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
2. Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
3. Klicken Sie auf **ThinOS**.  
Es wird das Fenster **ThinOS-Konfigurationsmodus auswählen** angezeigt.
4. Wählen Sie Ihren bevorzugten Modus zum Konfigurieren der Richtlinieneinstellungen. Die verfügbaren Modi sind:
  - Assistentenmodus
  - Erweiterter Konfigurationsmodus
  - i ANMERKUNG:** Zum Einstellen der Erweiterten ThinOS-Konfiguration als Standardmodus, wählen Sie das Kontrollkästchen aus.
5. Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.
  - i ANMERKUNG:** Der Thin Client wird neu gestartet, wenn Sie Änderungen an den folgenden Einstellungen vornehmen:
    - BIOS-Einstellung


- DP-Audio
- Buchsen-Popup
- Terminalname
- Ethernet-Geschwindigkeit
- Änderung der Anzeige – Auflösung, Drehen, Bildwiederholfrequenz, Dual- und Mehrfachanzeigen
- Systemmodus – DVD, Storefront und klassisch
- LPT-Port-Bindung

## ThinOS – Assistentenmodus

Verwenden Sie diese Seite zum Konfigurieren der am häufigsten verwendeten Parameter für ThinOS-Geräte.

### Schritte

1. Wählen Sie **Assistent** als Modus der Konfiguration.
2. Die Optionen müssen konfiguriert werden.
3. Klicken Sie auf **Weiter** und gehen Sie zur nächsten Richtlinieneinstellung.
4. Klicken Sie nach der Konfiguration der Optionen auf **Speichern & veröffentlichen**.

 **ANMERKUNG:** Klicken Sie auf **Weiter**, um den erweiterten Konfigurationsmodus von ThinOS zu öffnen.

## ThinOS – Erweiterter Modus

Verwenden Sie diese Seite zum Konfigurieren erweiterter Einstellungen für ThinOS-Geräte.

### Schritte

1. Wählen Sie **Erweiterte Konfiguration** als Modus der Konfiguration.
2. Konfigurieren Sie die Optionen nach Bedarf.
3. Klicken Sie auf **Speichern und veröffentlichen**, um die Konfiguration zu speichern und zu veröffentlichen.

 **ANMERKUNG:** Um zur Seite **ThinOS** zurückzukehren, klicken Sie auf **Richtlinie entfernen**.

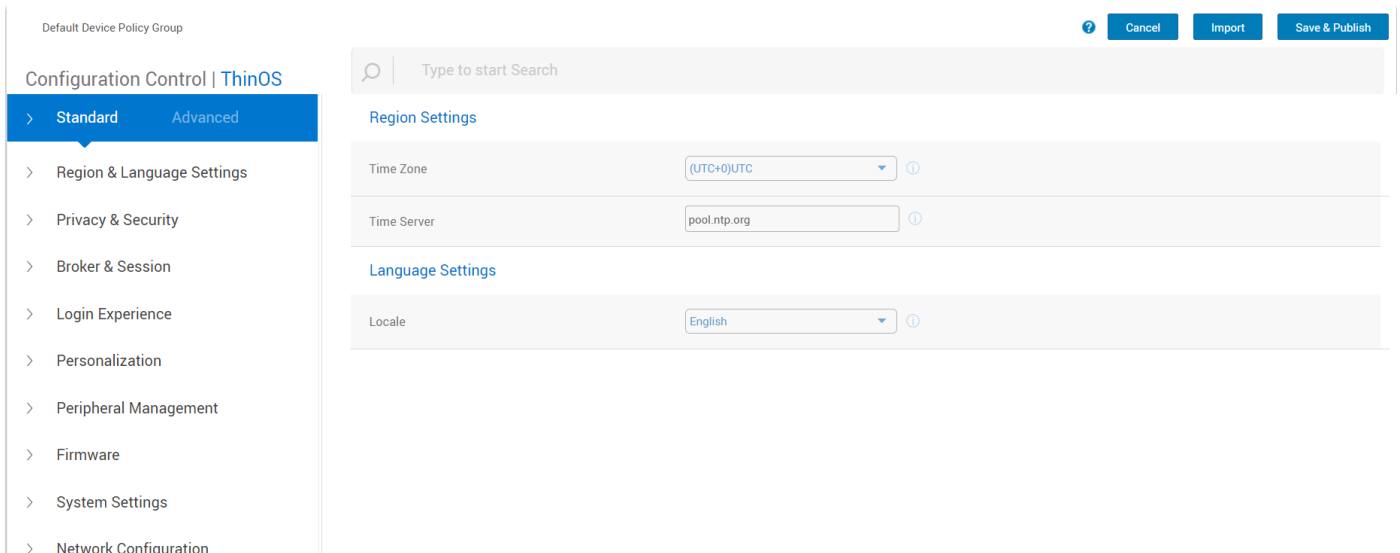
# Bearbeiten der Einstellungen für ThinOS-9.x-Richtlinien

### Voraussetzungen

- Erstellen Sie eine Gruppe mit einem Gruppentoken für die Geräte, für die Sie das Anwendungspaket übertragen möchten.
- Registrieren des Thin Clients bei der Wyse Management Suite

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **ThinOS 9.x**.  
Das Fenster **Konfigurationssteuerelement | ThinOS** wird angezeigt.



**Abbildung 5. Konfigurationssteuerung | ThinOS**

3. Klicken Sie auf die Option **Erweitert** oder **Standard**.
4. Wählen Sie die Optionen aus, die Sie konfigurieren wollen.
5. Klicken Sie in den entsprechenden Feldern auf die Option, die Sie konfigurieren möchten.

Mithilfe der Option „Globale Suche“ können Sie die relevanten Einstellungen oder Parameter suchen, die in den Richtlinieneinstellungen verfügbar sind. In den Suchergebnissen werden die Einstellungen in der folgenden Reihenfolge angezeigt:

- Stellung
- Parameter Gruppe
- Parameter Untergruppe
- Parameter

6. Konfigurieren Sie die Optionen nach Bedarf.
7. Klicken Sie auf **Speichern und Veröffentlichen**.

**ANMERKUNG:** Nachdem Sie auf **Speichern und Veröffentlichen** klicken, werden die konfigurierten Einstellungen auch auf der Registerkarte **Standard** angezeigt.

## BIOS-Konfigurationen für ThinOS 9.x

### Info über diese Aufgabe

BIOS-Konfigurationseinstellungen können mit Wyse Management Suite 2.1 für ThinOS 9.x-Geräte konfiguriert werden. Sie können die BIOS-Pakete über die Seite **Gruppen und Konfigurationen** oder über die Option zur Subnetz-Zuordnung bereitstellen.

**ANMERKUNG:** Diese Funktion ist nur mit der Pro-Lizenz der Wyse Management Suite verfügbar.

### Schritte


1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.  
Das Fenster Konfigurationssteuerelement | ThinOS wird angezeigt.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **ThinOS 9.x**.
3. Klicken Sie auf **Erweitert**.
4. Klicken Sie im Feld **BIOS** auf **Plattform auswählen**, um die Plattform auszuwählen, auf der Sie die BIOS-Einstellungen konfigurieren möchten.

# Aktualisieren von ThinOS 9.x auf spätere Versionen mit der Wyse Management Suite

## Voraussetzungen

- Stellen Sie sicher, dass Sie eine Gruppe mit einem Gruppentoken erstellt haben. Verwenden Sie dieses Gruppentoken, um die ThinOS-9.x-Geräte zu registrieren.
- Stellen Sie sicher, dass der Thin Client bei Wyse Management Suite registriert ist.

## Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
  2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **ThinOS 9.x**.  
Das Fenster **Konfigurationssteuerelement | ThinOS** wird angezeigt.
  3. Klicken Sie auf **Erweitert**.
  4. Wählen Sie im Feld **Firmware** die Option **OS-Firmware-Updates** aus.
  5. Klicken Sie auf **Durchsuchen**, um die Firmware zu durchsuchen und hochzuladen.  
Es werden die EULA Details des Pakets und der Name der Anbieter angezeigt.
  6. Um eine Datei auszuwählen, klicken Sie auf **Durchsuchen** und wechseln Sie zum Speicherort, an dem sich die Firmware befindet.
    - Wenn die EULA im Paket integriert ist, werden die EULA-Details des Pakets und der Name der Anbieter angezeigt. Sie können auf die Namen der einzelnen Anbieter klicken, um ihre jeweilige Lizenzvereinbarung zu lesen. Klicken Sie auf **Akzeptieren**, um das Paket hochzuladen. Wenn Sie mehrere Pakete hochladen, werden die EULA-Details jedes Pakets angezeigt. Sie müssen die Lizenzvereinbarung der Pakete einzeln akzeptieren.
    - Wenn Sie die EULA nicht akzeptieren, wird die Firmware nicht installiert.
-  **ANMERKUNG:** Sie können mehrere Firmware-Pakete aus dem Remote-Repository, dem Mandanten-Cloud-Repository oder dem Operator-Cloud-Repository hochladen und bereitstellen.
7. Wählen Sie aus dem Dropdownmenü **Bereitstellung von ThinOS-Firmware auswählen** die hochgeladene Firmware aus.

 **ANMERKUNG:** Sie können mehrere Firmware-Pakete aus dem Remote-Repository, dem Mandanten-Cloud-Repository oder dem Operator-Cloud-Repository hochladen und bereitstellen.
  8. Klicken Sie auf **Speichern und Veröffentlichen**.  
Der Thin Client lädt die Firmware herunter und startet sie neu. Die Firmware-Version wird aktualisiert.

# Hochladen und Pushen von BIOS-Paketen

## Voraussetzungen

- Erstellen Sie eine Gruppe in der Wyse Management Suite mit einem Gruppentoken. Verwenden Sie dieses Gruppentoken, um die ThinOS-9.x-Geräte zu registrieren.
- Registrieren des Thin Clients bei der Wyse Management Suite

## Schritte

1. Navigieren Sie zur Seite **Gruppen und Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **ThinOS 9.x**.  
Das Fenster Konfigurationssteuerelement | ThinOS wird angezeigt.
3. Klicken Sie auf **Erweitert**.
4. Wählen Sie im Feld **Firmware** die Option **BIOS-Firmware-Updates** aus.
5. Wählen Sie das Paket aus dem Dropdownmenü zur **Bereitstellung von ThinOS-BIOS auswählen** aus.

 **ANMERKUNG:** Sie können mehrere Firmware-Pakete aus dem Remote-Repository, dem Mandanten-Cloud-Repository oder dem Operator-Cloud-Repository hochladen und bereitstellen. Sie können 10 Pakete aus dem Mandanten-Cloud-Repository hochladen.
6. Klicken Sie auf **Speichern und Veröffentlichen**.  
Der Thin Client wird neu gestartet und das Anwendungspaket ist installiert.

Sie können die BIOS-Firmware auch über **Apps und Daten** in der Wyse Management Suite 2.1 hochladen, wie in den folgenden Schritten beschrieben:

- a. Navigieren Sie zur Seite **Apps & Daten**.
- b. Klicken Sie auf das **Betriebssystem-Image-Repository** und wählen Sie **Thin 9.x**.
- c. Klicken Sie auf **BIOS-Datei hinzufügen**, um die Datei zu suchen und hinzuzufügen, die Sie dem Repository hinzufügen möchten.


 **ANMERKUNG:** Diese Funktion ist nur für die Pro-Lizenz der Wyse Management Suite verfügbar.

## Hochladen und Pushen von ThinOS 9.x-Anwendungspaketen mit Gruppen und Konfigurationen

### Voraussetzungen

- Stellen Sie sicher, dass Sie eine Gruppe mit einem Gruppentoken erstellt haben. Verwenden Sie dieses Gruppentoken, um die ThinOS-9.x-Geräte zu registrieren.
- Registrieren des Thin Clients bei der Wyse Management Suite

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **ThinOS 9.x**.  
Das Fenster **Konfigurationssteuerelement | ThinOS** wird angezeigt.
3. Klicken Sie auf **Erweitert**.
4. Klicken Sie im Feld **Firmware** auf **Anwendungspaket-Updates**.
5. Um eine Datei auszuwählen, klicken Sie auf **Durchsuchen** und wechseln Sie zum Speicherort, an dem sich die Datei befindet.
  - Wenn die EULA im Paket integriert ist, werden die EULA-Details des Pakets und der Name der Anbieter angezeigt. Sie können auf die Namen der einzelnen Anbieter klicken, um ihre jeweilige Lizenzvereinbarung zu lesen. Klicken Sie auf **Akzeptieren**, um das Paket hochzuladen. Wenn Sie mehrere Pakete hochladen, werden die EULA-Details jedes Pakets angezeigt. Sie müssen die Lizenzvereinbarung der Pakete einzeln akzeptieren.
  - Wenn die EULA nicht im Paket integriert ist, fahren Sie mit Schritt 6 fort.
-  **ANMERKUNG:** Sie können mehrere Firmware-Pakete aus dem Remote-Repository, dem Mandanten-Cloud-Repository oder dem Operator-Cloud-Repository hochladen und bereitstellen.
6. Wählen Sie das Paket aus dem Dropdownmenü zur **Bereitstellung von ThinOS-Paket (s) auswählen** aus.
7. Klicken Sie auf **Speichern und Veröffentlichen**.  
Der Thin Client wird neu gestartet und das Anwendungspaket ist installiert.

## Bearbeiten von Windows Embedded Standard-Richtlinieneinstellungen

### Schritte

1. Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
2. Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
3. Klicken Sie auf **WES**.  
Die Seite **WES** wird angezeigt.
4. Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Konfigurieren der Bereitstellungseinstellungen für Windows Embedded-Geräten

Ab Wyse Management Suite 3.1 können Sie die Bereitstellungseinstellungen für Windows Embedded-Geräte konfigurieren. Sie können die Einstellungen für die automatische Bereitstellung von Konfigurationen für Geräte konfigurieren.

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdown-Menü **Richtlinien bearbeiten** auf **WES** oder **ThinLinux**.
3. Klicken Sie auf **Bereitstellungseinstellungen**.
4. Klicken Sie auf **Dieses Element konfigurieren**.
5. Legen Sie die folgenden Optionen fest:
  - **Alle Benachrichtigungen aktivieren/deaktivieren:** Wenn Sie diese Option deaktivieren, werden alle Optionen und Benachrichtigungen deaktiviert.
  - **Benachrichtigung zur Konfigurationsaktualisierung:** Wenn Sie diese Option deaktivieren, wird das Dialogfeld "Konfigurationsaktualisierung" auf dem Gerät nicht angezeigt.
  - **Benachrichtigung zur Anwendungsaktualisierung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn Sie eine Anwendungsrichtlinie bereitstellen.
  - **Benachrichtigung zur Image-Aktualisierung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung bei der Bereitstellung einer Abbildrichtlinie nicht angezeigt.
  - **Abmeldebenachrichtigung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn sich ein Benutzer vom Gerät abmeldet.
  - **Neustartbenachrichtigung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn die Gerätereustart-Konfiguration bereitgestellt wird.
  - **Bildschirm Sperre:** Wenn Sie diese Option deaktivieren, wird der Sperrbildschirm während der Aktualisierung von Anwendungen und Images nicht angezeigt.

 **ANMERKUNG:** Alle Optionen sind standardmäßig aktiviert.

6. Klicken Sie auf **Speichern und Veröffentlichen**.

## Bearbeiten der Einstellungen für die Linux-Richtlinie

### Schritte

1. Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
2. Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
3. Klicken Sie auf **Linux**.
4. Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Bearbeiten der Einstellungen für die ThinLinux-Richtlinie

### Schritte

1. Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
2. Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
3. Klicken Sie auf **ThinLinux**.
4. Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Konfigurieren von Bereitstellungseinstellungen für ThinLinux-Geräte

Ab Wyse Management Suite 3.1 können Sie die Bereitstellungseinstellungen für ThinLinux-Geräte konfigurieren. Sie können die Einstellungen für die automatische Bereitstellung von Konfigurationen für Geräte konfigurieren.

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.

2. Klicken Sie im Dropdown-Menü **Richtlinien bearbeiten** auf **ThinOS**.
3. Klicken Sie auf **Bereitstellungseinstellungen**.
4. Klicken Sie auf **Dieses Element konfigurieren**.
5. Konfigurieren Sie eine der folgenden Optionen:
  - **Alle Benachrichtigungen aktivieren/deaktivieren:** Wenn Sie diese Option deaktivieren, werden alle Optionen und Benachrichtigungen deaktiviert.
  - **Benachrichtigung zur Konfigurationsaktualisierung:** Wenn Sie diese Option deaktivieren, wird das Dialogfeld "Konfigurationsaktualisierung" auf dem Gerät nicht angezeigt.
  - **Benachrichtigung zur Anwendungsaktualisierung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn Sie eine Anwendungsrichtlinie bereitstellen.
  - **Benachrichtigung zur Image-Aktualisierung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung bei der Bereitstellung einer Abbildrichtlinie nicht angezeigt.
  - **Abmeldebenachrichtigung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn sich ein Benutzer vom Gerät abmeldet.
  - **Neustartbenachrichtigung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn die Gerätereuestart-Konfiguration bereitgestellt wird.
  - **Bildschirmsperre:** Wenn Sie diese Option deaktivieren, wird der Sperrbildschirm während der Aktualisierung von Anwendungen und Images nicht angezeigt.

 **ANMERKUNG:** Alle Optionen sind standardmäßig aktiviert.

6. Klicken Sie auf **Speichern und Veröffentlichen**.

## Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen

### Schritte

1. Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
2. Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
3. Klicken Sie auf **Wyse Software Thin Client**.  
Die Seite **Wyse Software Thin Client** wird angezeigt.
4. Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Bearbeiten der Einstellungen für die Cloud Connect-Richtlinieneinstellungen

### Schritte

1. Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
2. Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
3. Klicken Sie auf **Cloud Connect**.
4. Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Bearbeiten der Einstellungen der Dell Hybrid Client-Richtlinien

### Voraussetzungen

- Erstellen Sie eine Gruppe mit einem Gruppentoken für die Geräte, für die Sie das Anwendungspaket übertragen möchten.

- Registrieren von Dell Hybrid Clients bei der Wyse Management Suite

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **Hybrid Client**.  
Das Fenster **Konfigurationssteuerelement | Hybrid Client** wird angezeigt.
3. Klicken Sie auf die Option **Erweitert**.
4. Wählen Sie die Optionen aus, die Sie konfigurieren wollen.
5. Klicken Sie in den entsprechenden Feldern auf die Einstellung und konfigurieren Sie die Optionen nach Bedarf.
6. Klicken Sie auf **Speichern und Veröffentlichen**.

**ANMERKUNG:** Nachdem Sie auf **Speichern und Veröffentlichen** klicken, werden die konfigurierten Einstellungen auch auf der Registerkarte **Standard** angezeigt.

In der folgenden Tabelle sind die Funktionen aufgeführt, die Sie im Fenster **Konfigurationssteuerelement | Hybrid Client** konfigurieren können.

**Tabelle 5. Einstellungen für Hybrid Client-Richtlinien**

Funktion	Unterfunktion – Richtliniengruppe für Benutzer	Unterfunktion – Richtliniengruppe für Geräte
<b>Peripherieverwaltung</b>	Anzeigeeinstellungen	Anzeigeeinstellungen
	Drucker	Drucker
	Audio	Audio
	Maus	Maus
	Tastatur	Tastatur
<b>Netzwerkkonfiguration</b>	Wireless	Wireless
		Proxy
		Bluetooth
<b>Browsereinstellungen</b>	Einstellungen für Google Chrome	Browser-Verknüpfungen
	Einstellungen für Firefox	
	Browser-Verknüpfungen	
	Standardbrowser	
<b>Sprach- &amp; Regionseinstellungen</b>	Region	Region
		Zeitserver
		Sprache
<b>Personalisierung</b>	Desktop	Desktop
		Geräteinfo
<b>Anmeldung</b>	Nicht zutreffend	Domäne beitreten
		Zuvor angemeldete Benutzerliste
<b>Datenschutz &amp; Sicherheit</b>	Nicht zutreffend	Zertifikat
		Eigenschaften des Gast-Kontos
		USB-Sperre
		GRUB-Kennwort
		Bremen-Kennwort
		VNC-Server
SSH-Server		

**Tabelle 5. Einstellungen für Hybrid Client-Richtlinien (fortgesetzt)**

Funktion	Unterfunktion – Richtliniengruppe für Benutzer	Unterfunktion – Richtliniengruppe für Geräte
<b>Energieeinstellungen</b>	Energiesparmodus	Energiesparmodus
	Standby-und Betriebsschalter	Standby-und Betriebsschalter
<b>Citrix Workspace</b>	Citrix Broker Sitzung	Citrix Broker Sitzung
	Globale Citrix-Einstellungen	Globale Citrix-Einstellungen
<b>VMware ViewClient</b>	VMware ViewClient Broker-Sitzung	VMware ViewClient Broker-Sitzung
	VMware globale Einstellungen	VMware globale Einstellungen
<b>RDP</b>	RDP Broker-Sitzung	RDP Broker-Sitzung
<b>Dell Hybrid Client-Modus</b>	Dell Hybrid Client-Modus	Dell Hybrid Client-Modus
<b>WMS-Einstellungen</b>	Nicht zutreffend	WMS-Clienteinstellungen
		Bereitstellungseinstellungen
<b>Anwendungssicherheit</b>	VLC Media Player	VLC Media Player
	Bildbetrachter	Bildbetrachter
	Libre Office	Libre Office
<b>Netzlaufwerke</b>	Liste der Netzwerklaufwerke	Liste der Netzwerklaufwerke
<b>BIOS</b>	Nicht zutreffend	Wählen Sie Ihre Plattform aus: <ul style="list-style-type: none"> <li>● DHC 5070</li> <li>● DHC 7070</li> </ul>

**ANMERKUNG:** Verwenden Sie keine Sonderzeichen und fügen Sie keine Leerzeichen in den Namen der Ressourcendatei ein, wie z. B. Hintergrundbild, Zertifikat, AD-Logo-Dateien.

Weitere Informationen zur Konfiguration Ihres Dell Hybrid Clients finden Sie im *Dell Hybrid Client Administratorhandbuch* unter [www.Dell.com/Support](http://www.Dell.com/Support).

## Konfigurieren der Wyse Management Suite Clienteinstellungen für Dell Hybrid Client

Administratoren können das Verhalten des Wyse Management Suite-Agenten in Bezug auf Dell Hybrid Client-Konfigurationen konfigurieren. Administratoren können Geräte auch für die Anwendung von Konfigurationen außerhalb der Geschäftszeiten konfigurieren.

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **Hybrid Client**.  
Das Fenster **Konfigurationssteuerelement | Hybrid Client** wird angezeigt.
3. Klicken Sie auf die Option **Standard**.
4. Gehen Sie zu **WMS Einstellungen > WMS Clienteinstellungen**.
5. Um die Geschäftszeiten und Arbeitstage für die Gerätegruppe zu konfigurieren, klicken Sie **Zeile hinzufügen** im Feld **Geschäftszeit** und wählen Sie die Tage aus dem Dropdown-Menü **Geschäftstage**.
6. Aktivieren Sie die Option **Sitzungs-Reporting aktivieren** und wählen Sie im Drop-Down-Menü **Bericht über Sitzung erstellen** die Zeitplanung aus, um den Agent für das Melden von Benutzersitzungen zu aktivieren. Die verfügbaren Optionen sind:
  - **Benutzersitzung während der Laufzeit senden** – der Dell Client-Agent sendet den Benutzersitzungsbericht jedes Mal, wenn sich ein Benutzer vom Gerät abmeldet.
  - **Benutzersitzung beim Check-in-Zeitpunkt senden** – der Dell Client-Agent sendet den Bericht der Benutzersitzung alle 8 Stunden.
  - **Benutzersitzung außerhalb der Geschäftszeiten senden** – der Dell Client-Agent sendet den Benutzersitzungsbericht außerhalb der Geschäftszeiten, wie sie in Schritt 5 konfiguriert sind.

7. Aktivieren Sie zum Bereitstellen der Konfigurationen auf einem Gerät basierend auf den Konfigurationen auf Benutzerebene die Option **Benutzerpersonalisierungs-Roaming aktivieren**. Wenn diese Option aktiviert ist, werden die Einstellungen, die von einem Benutzer auf einem Gerät konfiguriert werden, auf dem Wyse Management Suite-Server gespeichert und die Konfigurationen werden automatisch angewendet, wenn sich ein Benutzer bei einem anderen Gerät anmeldet. Die konfigurierten Einstellungen haben Vorrang vor allen anderen Konfigurationen.
8. Aktivieren Sie die Option **Push-Benachrichtigung aktivieren**, um Benachrichtigungen auf dem Gerät zu aktivieren. Wenn diese Option aktiviert ist, werden die konfigurierten Einstellungen unmittelbar nach dem Klicken auf **Speichern und Veröffentlichen** angewendet. Wenn Sie diese Option deaktivieren, werden die Taktsignale gesendet.
 

**i ANMERKUNG:** Wenn Sie die Option deaktivieren, kann die Anwendungsbereitstellung einen Fehlerzustand eingeben, da Wyse Management Suite die Push-Benachrichtigung nicht an Dell Hybrid-Clients sendet.
9. Wenn Sie die Konfiguration außerhalb der angegebenen Geschäftszeiten anwenden möchten, wählen Sie die Option aus dem Drop-Down-Menü aus. Die verfügbaren Optionen sind:
  - **Sofort** – Wenn Sie diese Option auswählen, werden die Konfigurationen unmittelbar nach dem Klicken auf **Speichern und veröffentlichen** angewendet.
  - **Außerhalb der angegebenen Geschäftszeit** – Wenn Sie diese Option auswählen, werden die Konfigurationen außerhalb der Geschäftszeiten angewendet, die in Schritt 5 konfiguriert wurden.
  - **Wenn sich kein Benutzer für eine bestimmte Zeit am Gerät angemeldet hat** – Wenn Sie diese Option auswählen, wird die Konfiguration angewendet, wenn sich kein Benutzer für eine festgelegte Zeit am Gerät angemeldet hat. Sie können die Leerlaufzeit festlegen, nach der die Konfigurationen auf das Gerät angewendet werden.

**i ANMERKUNG:** Sie können diese Einstellungen für ein bestimmtes Gerät auch über die Seite **Geräte** konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren von Richtlinien der Geräteklasse](#).

## Konfigurieren von Bereitstellungseinstellungen für Dell Hybrid Client-Geräte

Ab Wyse Management Suite 3.1 können Sie die Bereitstellungseinstellungen für Dell Hybrid Client-Geräte konfigurieren. Sie können die Einstellungen für die automatische Bereitstellung von Konfigurationen für Geräte konfigurieren.

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **Hybrid Client**.
3. Gehen Sie zu **WMS-Einstellungen > WMS-Bereitstellungseinstellungen**.
4. Legen Sie die folgenden Optionen fest:
  - **Benachrichtigung zur Konfigurationsaktualisierung:** Wenn Sie diese Option deaktivieren, wird das Dialogfeld "Konfigurationsaktualisierung" auf dem Gerät nicht angezeigt.
  - **Benachrichtigung zur Anwendungsaktualisierung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn Sie eine Anwendungsrichtlinie bereitstellen.
  - **Benachrichtigung zur Image-Aktualisierung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung bei der Bereitstellung einer Abbildrichtlinie nicht angezeigt.
  - **Abmeldebenachrichtigung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn sich ein Benutzer vom Gerät abmeldet.
  - **Neustartbenachrichtigung:** Wenn Sie diese Option deaktivieren, wird die Benutzerbenachrichtigung nicht angezeigt, wenn die Gerätereinstellung-Konfiguration bereitgestellt wird.
  - **Bildschirm Sperre:** Wenn Sie diese Option deaktivieren, wird der Sperrbildschirm während der Aktualisierung von Anwendungen und Images nicht angezeigt.

**i ANMERKUNG:** Sie können die Option **Alle Benachrichtigungen aktivieren/deaktivieren** aktivieren, wenn Sie alle Optionen und Benachrichtigungen aktivieren möchten.

**i ANMERKUNG:** **Benachrichtigung zur Konfigurationsaktualisierung** und **Bildschirm Sperre** sind standardmäßig deaktiviert.
5. Klicken Sie auf **Speichern und Veröffentlichen**.

# Erstellen und Importieren einer Ausnahmedatei für ein Massenspeichergerät

Ab Wyse Management Suite 3.1 können Sie Geräteausnahmekonfigurationen für mehrere ThinOS 9.x-Geräte bereitstellen.

## Schritte

1. Erstellen Sie eine Ausnahmedatei für ein Massenspeichergerät. Führen Sie einen der folgenden Schritte aus, um eine Datei zu erstellen:
  - Erstellen Sie eine Gruppenrichtlinie für eine Testgruppe und exportieren Sie dann diese Richtlinie in eine Datei. Wenn die Konfiguration Kennwörter enthält, werden Sie in der exportierten Datei durch \* ersetzt. Beispiel:

```
{
  "WMSVersion": "4.6.8",
  "exportedDate": "1581466633677",
  "deviceTypes": [
    {
      "type": 6,
      "configurations": {
        "version": "0.0.1",
        "sequence": 1581466506281,
        "parameters": {
          "AdminModeUsername": {
            "value": "admin",
            "updatedAt": "1581466506234"
          },
          "AdminModePassword": {
            "value": "*****",
            "updatedAt": "1581466506234"
          },
          "TerminalName": {
            "value": "outpatient",
            "updatedAt": "1581466506234"
          },
          "TimeServer": {
            "value": "10.10.10.10",
            "updatedAt": "1581466506234"
          },
          "timeZone": {
            "value": "America/Phoenix",
            "updatedAt": "1581466506234"
          },
          "TerminalNameCapital": {
            "value": "yes",
            "updatedAt": "1581466506234"
          },
          "DeviceNICDefault": {
            "value": "Wlan",
            "updatedAt": "1581466506234"
          },
          "AdminMode": {
            "value": "yes",
            "updatedAt": "1581466506234"
          }
        }
      }
    }
  ]
}
```

- Erstellen Sie eine .json-Datei mit folgendem Format:

```
{
  "devices": {
    <serialnumber>: {
      "parameters": {
```

```

"<parametername>": {
    "value": <value>
},
"<parametername>": {
    "value": <value>
}
},
configurations: [<configuration name>]
}
}
"configurations": {
<configurationName>: {
"<parametername>": {
    "value": <value>
},
"<parametername>": {
    "value": <value>
}
}
}
}
}

```

Beispiel:

```

{
  "devices": {
    "9EPDL900051": {
      "parameters": {
        "TerminalName": {
          "value" : "Cubical 5 - Floor 3"
        },
        "TerminalNameCapital": {
          "value": "no"
        }
      },
      configurations: ["westWingExceptions"]
    },
    "5LGDO600108": {
      "parameters": {
        "TerminalName": {
          "value" : "Cubical 15 - Floor 2"
        },
        "TerminalNameCapital": {
          "value": "no"
        }
      },
      configurations: ["westWingExceptions"]
    }
  },
  "configurations": {
    "westWingExceptions": {
      "DeviceNICDefault": {
        "value": "Wlan"
      }
    }
  }
}

```

```

    },
    "timeZone": {
      "value": "America/Phoenix"
    },
    "TimeServer": {
      "value": "10.10.10.10"
    },
    "TerminalNameCapital": {
      "value": "yes"
    },
    "AdminMode": {
      "value": "yes"
    },
    "AdminModeUsername": {
      "value": "admin"
    },
    "AdminModePassword": {
      "value": "password"
    }
  }
}

```

2. Komprimieren und verschlüsseln Sie die Datei.

**i ANMERKUNG:** Sie können die Datei mithilfe der 7-Zip-Software komprimieren und verschlüsseln.

**i ANMERKUNG:** Die Dateigröße darf nicht mehr als 1 MB betragen.

3. Navigieren Sie zu **Gruppen & Konfigurationen** und klicken Sie auf **Richtlinien importieren**.

Daraufhin wird der Bildschirm **Assistent zum Import von Richtlinien** angezeigt.

4. Wählen Sie **Massenspeichergeräte-Ausnahmen**.

5. Klicken Sie auf **Durchsuchen** und wählen Sie die Kennwortverschlüsselte .zip-Datei aus.

6. Klicken Sie auf **Weiter**.

Die Seite **Wählen Sie die zu importierenden Gerätetypkonfigurationen aus** wird angezeigt.

7. Klicken Sie auf **Weiter**.

**i ANMERKUNG:** Da Sie einen Massenimport für eine Geräte-Ausnahmedatei für ThinOS 9.x-Geräte durchführen können, können Sie die Optionen auf der Seite nicht konfigurieren.

8. Geben Sie das Kennwort für die .zip-Datei ein, das zum Komprimieren der .json-Datei verwendet wurde.

9. Klicken Sie auf **Weiter**.

Eine Zusammenfassung des Imports von Massenspeichergeräte-Ausnahmen wird angezeigt.

10. Klicken Sie auf **Importieren**.

Nachdem die Konfigurationen importiert wurden, wird ein Link zum Erstellen und Herunterladen eines Berichts auf der Seite **Gruppen und Konfigurationen** erzeugt. Eine Erfolgsmeldung wird auf der Seite **Gruppen und Konfigurationen** angezeigt.

**i ANMERKUNG:** Wenn ein Gerät nicht registriert ist und die Konfigurationen importiert wurden, werden Ausnahmen nur dann auf dieses Gerät angewendet, wenn sich das Gerät in den nächsten 30 Tagen bei einem der Geräte mit vorinstallierten Seriennummern registriert.

**i ANMERKUNG:** Wenn ein Gerät bereits registriert ist und die Konfigurationen mit der Geräteseriennummer importiert wurden, werden die Geräteausnahmen auf das Gerät angewendet.

**i ANMERKUNG:** Die importierte Datei ist passwortgeschützt. AES-256- und ZipCrypto-Verschlüsselung werden unterstützt.

**i ANMERKUNG:** Konfigurationen, wie z. B. Zertifikate, Hintergrundbild, Logo usw. mit ihnen zugeordneten Ressourcen werden nicht importiert.

# Verwalten von Geräten

In diesem Abschnitt wird die Durchführung routinemäßiger Gerätemanagementaufgaben in der Managementkonsole beschrieben. Zum Aufrufen des Gerätebestands klicken Sie auf die Registerkarte **Geräte**. Sie können eine Teilmenge von Geräten mithilfe von verschiedenen Filterkriterien wählen, wie z. B. Gruppen und Untergruppen, Gerätetyp, Art des Betriebssystems, Status, Subnetz, Plattform oder Zeitzone.

Sie können die Geräteliste nach folgenden Kriterien sortieren:

- Typ
- Plattform
- Version des Betriebssystems
- Seriennummer
- IP-Adresse
- Details über den letzten Benutzer
- Gruppendetails
- Letzter Check-in-Zeitpunkt
- Registrierungsstatus
- Schreibfilterstatus

Zum Anzeigen der Seite **Gerätedetails** für ein bestimmtes Gerät klicken Sie auf den auf der Seite aufgelisteten Geräteeintrag. Alle Konfigurationsparameter des Geräts und der Gruppenklasse, in der die einzelnen Parameter angewendet werden, finden Sie auf der Seite **Gerätedetails**.

Sie können die Konfigurationsparameter festlegen, die speziell für das Gerät gelten. Parameter in diesem Abschnitt überschreiben alle Parameter, die in Gruppen und/oder auf globaler Ebene konfiguriert wurden.

Abbildung 6. Seite „Geräte“

## Themen:

- [Methoden zum Registrieren Geräten bei Wyse Management Suite](#)
- [Suchen nach einem Gerät mithilfe von Filtern](#)
- [Filter auf der Seite „Geräte“ speichern](#)
- [Abfragen des Gerätstatus](#)
- [Sperren der Geräte](#)
- [Neustart der Geräte](#)
- [Registrierung eines Geräts aufheben](#)
- [Anmeldungsvalidierung](#)
- [Gerät auf Werkseinstellungen zurücksetzen](#)

- Ändern einer Gruppenzuweisung auf der Seite „Geräte“
- Senden von Meldungen an ein Gerät
- Wake on LAN-Befehl
- Anzeigen der Gerätedetails
- Anzeigen der Anzeigeparameter
- Anzeigen der Details zu virtuellen NICs
- Überprüfen der BIOS-Details
- Verwalten der Gerätezusammenfassung
- Anzeigen von Systeminformationen
- Anzeigen von Geräteereignissen
- Anzeigen installierter Anwendungen
- Umbenennen des Thin Client
- Aktivieren von Remote Shadowing-Verbindung
- Konfigurieren der Remote Shadowing-Verbindung für Dell Hybrid Client-Geräte
- Herunterfahren von Geräten
- Hinzufügen eines Tags zu einem Gerät
- Compliance-Status des Geräts
- Pull für Windows Embedded Standard oder ThinLinux-Abbild ausführen
- Anfordern einer Protokolldatei
- Fehlerbehebung auf Ihrem Gerät
- Erstellen eines neuen Image Ihres Dell Hybrid Client
- Benutzeroberflächen-Konfigurationspaket für Dell Hybrid Client herunterladen
- Zurücksetzen des Dell Hybrid Clients auf die Werkseinstellungen

## Methoden zum Registrieren Geräten bei Wyse Management Suite

Sie können einen Thin-Client bei der Wyse Management Suite auf eine der folgenden Arten registrieren:

- Manuelles Registrieren über die Benutzeroberfläche, die von dem Wyse Geräte-Agent (WDA) auf dem Gerät bereitgestellt wird.
- Automatisches Registrieren über die Konfiguration der angemessenen Optionskategorien auf dem DHCP-Server.
- Automatisches Registrieren durch Konfigurieren der entsprechenden DNS-SRV-Einträge auf dem DNS-Server.

### ANMERKUNG:

- Registrieren Sie für eine öffentliche Cloud einen Thin Client durch die Angabe der Wyse Management Suite-URL und den Gruppentoken für die Gruppe, in der Sie das Gerät registrieren möchten.
- Registrieren Sie für eine private Cloud einen Thin Client durch die Angabe der Wyse Management Suite-URL und den Gruppentoken – optional für die Gruppe, in der Sie dieses Gerät registrieren möchten. Geräte werden in der nicht verwalteten Gruppe registriert, wenn kein Gruppentoken angegeben wurde.


## Manuelles Registrieren von Dell Hybrid Clients

### Voraussetzungen

Stellen Sie vor der Registrierung des Geräts sicher, dass Ihr Gerät über eine Netzwerkverbindung verfügt, um den Wyse Management Suite Server zu kontaktieren.

 **ANMERKUNG:** Sie können das Gerät nur über das Gast-Konto registrieren. Das gilt auch für das Aufheben der Registrierung.

### Schritte

1. Melden Sie sich bei Dell Hybrid Client als Gast-Nutzer an. Standardmäßig lautet der Nutzernamen **Gast**.
2. Klicken Sie in der oberen Leiste auf .

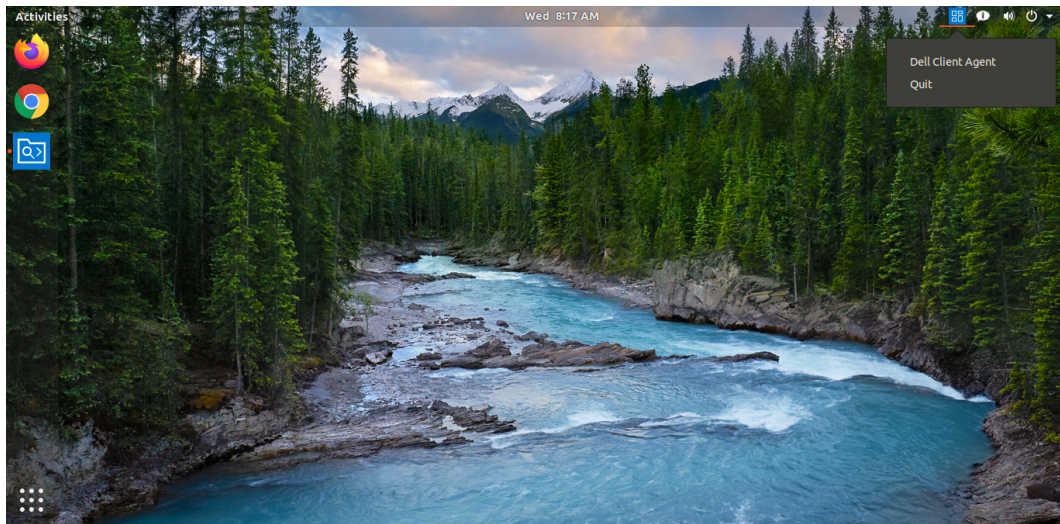


Abbildung 7. Dell Client Agent-Symbol

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

**ANMERKUNG:** Wenn die Felder Mandant und Gruppe leer sind, wird das Gerät in der nicht verwalteten Gruppe registriert. Das Gruppentoken ist jedoch zwingend erforderlich, um das Gerät in einer öffentlichen Cloud zu registrieren.
8. Klicken Sie auf die Schaltfläche **EIN/AUS**, um die Option **Server-Zertifikat CA validieren** zu aktivieren oder zu deaktivieren. Aktivieren Sie diese Option, um die Validierung des Serverzertifikats für die gesamte Kommunikation zwischen Geräten und Servern durchzuführen.  
Die Option CA-Validierung wird automatisch aktiviert und kann nicht deaktiviert werden, wenn die URL einer öffentlichen Cloud eingegeben wurde.
9. Klicken Sie auf **Registrieren**, um Ihr Gerät auf dem Wyse Management Suite-Server zu registrieren.  
Wenn Ihr Gerät erfolgreich registriert wurde, wird der Status **Registriert** angezeigt, wobei neben der Bezeichnung **Registrierungsstatus** die Option „grün“ markiert ist. Die Beschriftung der Schaltfläche **Registrieren** ändert sich in **Registrierung aufheben**.

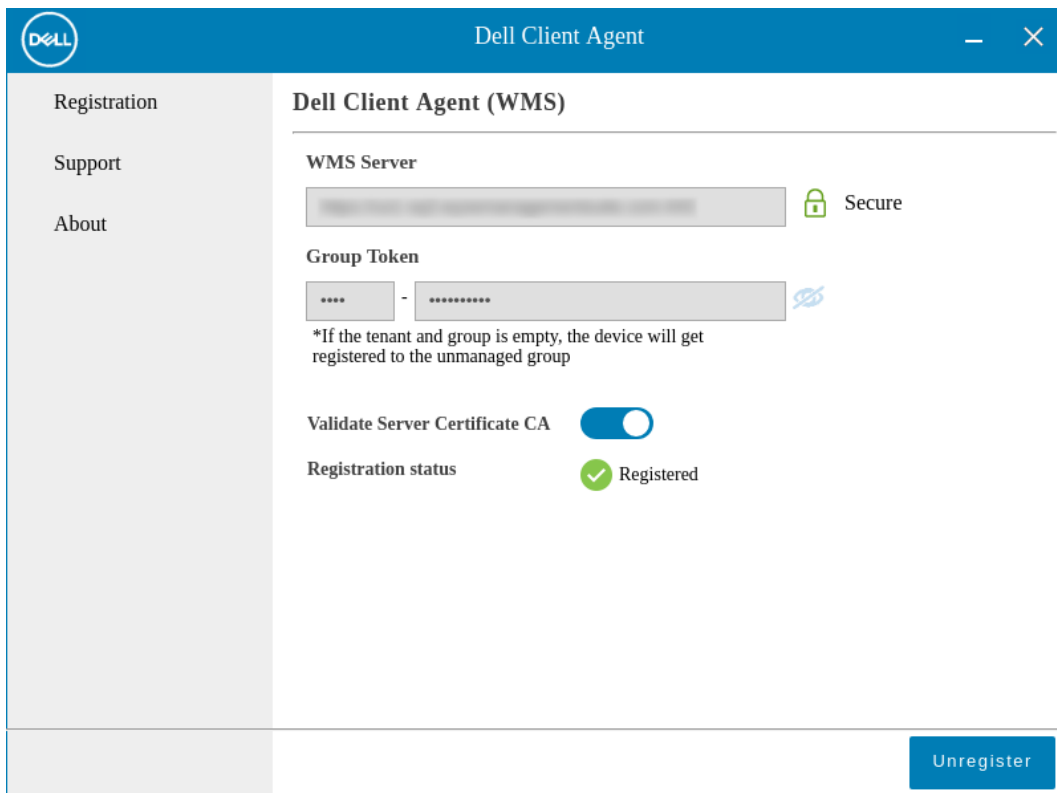


Abbildung 8. Dell Client Agent

## Registrieren von Dell Hybrid Clients mithilfe der manuellen Ermittlungsmethode

Sie können die manuelle Ermittlungsmethode verwenden, um OptiPlex 7070 Ultra-Geräte, auf denen Ubuntu Version 18.04 LTS 64-Bit ausgeführt wird, mithilfe des Dell Client Agent Enabler Agents in der Wyse Management Suite zu registrieren.

### Schritte

1. Erstellen Sie mithilfe des folgenden Skripts eine reg.json-Datei:

```
{ "ccm":
  { "ccmserver": "WMSserverURL.Domain.com", "ccmport": "443", "usessl": "true", "mqttserver": "
  WMSserverURL.Domain.com
  ", "mqttport": "1883", "grouptoken": "GroupToken", "isCaValidationOn": "false" } }
```

2. Kopieren Sie die Datei reg.json nach /etc/dcae/config.
3. Starten Sie das Gerät neu.

## Registrieren von ThinOS-Geräten mit dem Wyse Geräte-Agenten

So registrieren Sie ThinOS Geräte manuell:

### Schritte

1. Klicken Sie auf dem Desktopmenü des Thin Client auf **System-Setup > Zentrale Konfiguration**. Das Fenster **Zentrale-Konfiguration** wird angezeigt.
2. Klicken Sie auf die Registerkarte **WDA**. Der WDA-Dienst wird automatisch ausgeführt, sobald der Client-Startprozess abgeschlossen ist.  
**WMS** ist standardmäßig ausgewählt.

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 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.

**ANMERKUNG:**

- Eine Warnmeldung wird angezeigt, wenn Sie die CA-Validierung deaktivieren. Sie müssen zum Bestätigen auf OK klicken.
- Nehmen Sie an der Public-Cloud-Version von Wyse Management Suite im Rechenzentrum in den USA keine Änderungen an den Standarddetails des WMS-Servers und MQTT-Servers vor. Verwenden Sie für die Public-Cloud-Version von Wyse Management Suite im Rechenzentrum in Europa Folgendes:
  - CCM-Server – [eu1.wysemanagementsuite.com](http://eu1.wysemanagementsuite.com)
  - MQTT-Server – [eu1-pns.wysemanagementsuite.com:1883](http://eu1-pns.wysemanagementsuite.com:1883)
- Eine Warnmeldung wird angezeigt, wenn die Serveradresse „http“ enthält. Sie müssen zum Bestätigen auf OK klicken.

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 den Gruppenschlüssel und die WMS-Server-URL, den bzw. 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 registriert.

## Registrieren von Windows Embedded Standard Thin Clients bei der Wyse Management Suite über Wyse Geräte-Agent

### Voraussetzungen

Erstellen Sie eine Gruppe in der Wyse Management Suite, um ein Gerät zu registrieren.

### Schritte



1. Öffnen Sie die Anwendung Wyse Geräte-Agent.  
Der Bildschirm mit dem Wyse Geräte-Agenten wird angezeigt.
2. Wählen Sie in der Dropdown-Liste **Verwaltungsserver** die Option **Wyse Management Suite** aus.
3. Geben Sie die Serveradresse und die Portnummer in die jeweiligen Felder ein.  
**ANMERKUNG:** Wenn die Serveradresse **http** enthält, wird eine Warnmeldung angezeigt. Klicken Sie zum Bestätigen auf **OK**.
4. Geben Sie das Gruppentoken ein. Für einen einzelnen Mandanten ist die Eingabe eines Gruppentokens ein optionaler Schritt.  
**ANMERKUNG:** Das Gruppentoken, das im Feld **Gruppentoken** eingegeben wird, wird nicht als Klartext angezeigt.
5. Aktivieren oder deaktivieren Sie die CA-Validierung abhängig von Ihrem Lizenztyp.  
**ANMERKUNG:** Wenn Sie die CA-Validierung deaktivieren, wird eine Warnmeldung angezeigt. Klicken Sie zum Bestätigen auf **OK**.
6. Klicken Sie auf **Registrieren**.

# Registrieren des Wyse Software Thin Client bei der Wyse Management Suite über den Wyse Geräte-Agenten

## Voraussetzungen

Erstellen Sie eine Gruppe, um ein Gerät bei der Wyse Management Suite zu registrieren.

## Schritte

1. Öffnen Sie die Anwendung **Wyse Geräte-Agent**.  
Das Fenster **Wyse Geräte-Agent** wird angezeigt.
2. Geben Sie die Geräteregistrierungsinformationen ein.
3. Wählen Sie in der Dropdown-Liste **Verwaltungsserver** die Option **Wyse Management Suite** aus.
4. Geben Sie die Serveradresse und die Portnummer in die jeweiligen Felder ein.  
 **ANMERKUNG:** Wenn die Serveradresse **http** enthält, wird eine Warnmeldung angezeigt. Klicken Sie zum Bestätigen auf **OK**.
5. Geben Sie das Gruppentoken ein. Für einen einzelnen Mandanten ist die Eingabe eines Gruppentokens ein optionaler Schritt.
6. Aktivieren oder deaktivieren Sie die CA-Validierung abhängig von Ihrem Lizenztyp.  
 **ANMERKUNG:** Wenn Sie die CA-Validierung deaktivieren, wird eine Warnmeldung angezeigt. Klicken Sie zum Bestätigen auf **OK**.
7. Klicken Sie auf **Registrieren**.  
Nachdem die Registrierung abgeschlossen ist, wird die Meldung **An Wyse Management Suite registriert** angezeigt.

# Registrieren von ThinLinux Thin Clients über Wyse Geräte-Agent

## Voraussetzungen

Erstellen Sie eine Gruppe in der Wyse Management Suite, um ein Gerät zu registrieren.

## Schritte

1. Öffnen Sie die Anwendung Wyse Geräte-Agent.  
Der Bildschirm mit dem Wyse Geräte-Agenten wird angezeigt.
2. Geben Sie die Geräteregistrierungsinformationen ein.
3. In der Wyse Management Suite geben Sie die Daten des Wyse Management Suite-Servers ein.
4. Geben Sie das Gruppentoken ein.  
Für einen einzelnen Mandanten ist die Eingabe eines Gruppentokens ein optionaler Schritt.
5. Klicken Sie auf **Registrieren**.  
Nachdem die Registrierung abgeschlossen ist, wird eine Bestätigungsmeldung angezeigt.

# Registrieren von ThinOS-Geräten mithilfe der FTP-INI-Methode

## Voraussetzungen

Erstellen Sie eine Gruppe, die bei der Wyse Management Suite registriert werden soll.

## Schritte

1. Erstellen Sie eine `wnos.ini`-Datei. Geben Sie folgenden Parameter ein:

**CCMEnable**=yes/no **CCMServer**=FQDN of WMS Server **GroupPrefix**=The prefix of the Group Token  
**GroupKey**=The Group Key **CAVAlidation**=yes/no **Discover**=yes/no

Geben Sie zum Beispiel zum Registrieren des Geräts mit ThinOS in der Wyse Management Suite (FQDN des Servers ist ServerFQDN.domain.com) mit dem Gruppentoken defa-defadefa und mit aktivierter CA-Validierungsoption die folgenden INI-Parameter ein:

**CCMEnable**=yes **CCMServer**= is ServerFQDN.domain.com **GroupPrefix**=defa **GroupKey**=defadefa  
**CAValidation**=yes **Discover**=yes

2. Legen Sie die `wnos.ini`-Datei im `wnos`-Ordner eines beliebigen FTP-Pfads ab.
3. Gehen Sie zu **Zentrale Konfiguration** auf dem ThinOS-Gerät.
4. Geben Sie in der Registerkarte **Allgemein** den FTP-Pfad bei Dateiservern oder den Pfad zum übergeordneten Ordner an.
5. Geben Sie die FTP-Anmeldeinformationen an, falls erforderlich. Wenn der FTP keine Anmeldeinformationen erfordert, können Benutzername und Kennwort anonym sein.
6. Klicken Sie auf **OK** und starten Sie dann den Thin Client neu.
7. Gehen Sie zu **Zentrale Konfiguration** auf dem ThinOS-Gerät.  
In der Registerkarte **Wyse Geräte-Agent** stehen die Wyse Verwaltungsserverdetails in dem entsprechenden Feld und der Client-Eintrag auf der Seite „Geräte“ des Wyse Verwaltungsservers zur Verfügung.

## Registrieren von Geräten mit ThinLinux Version 2.0 mithilfe der FTP- INI-Methode

### Voraussetzungen

Erstellen Sie eine Gruppe, die bei der Wyse Management Suite registriert werden soll.

### Schritte

1. Erstellen Sie eine `wlx.ini`-Datei. Geben Sie folgenden Parameter ein:

**WMSEnable**=yes\no

**WMSServer**=https://FQDN of the WMS Server:Port <By default 443 is used>

**GroupRegistrationKey**=GroupToken present in WMS Server

**CAValidation**=True/False

Geben Sie zum Beispiel zum Registrieren des Geräts mit ThinLinux Version 2.0 in der Wyse Management Suite (FQDN des Servers ist `ServerFQDN.domain.com`) mit dem Gruppentoken `defa-defadefa` und mit aktivierter CA-Validierungsoption die folgenden INI-Parameter ein:

**WMSEnable**=yes

**WMSServer**=https://ServerFQDN.domain.com:443

**GroupRegistrationKey**=defa-defadefa

**CAValidation**=True

2. Speichern Sie die `wlx.ini`-Datei im Ordner „`wyse\wlx2`“.
3. Gehen Sie zu **Einstellungen** und wechseln Sie auf dem ThinLinux Thin Client zum Administrator.
4. Gehen Sie zu **Verwaltung > INI**.
5. Geben Sie die FTP-Server-URL ein.
6. Klicken Sie auf **Speichern** und starten Sie den Thin Client neu.
7. Gehen Sie zu **Verwaltung > Wyse Geräte-Agent**.  
In der Registerkarte „Wyse Geräte-Agent“ stehen die Wyse Verwaltungsserverdetails in dem entsprechenden Feld und der Client-Eintrag auf der Seite „Geräte“ des Wyse Verwaltungsservers zur Verfügung.

## Registrieren von Geräten mit ThinLinux Version 1.0 mithilfe der FTP- INI-Methode

### Voraussetzungen

Erstellen Sie eine Gruppe, die bei der Wyse Management Suite registriert werden soll.

## Schritte

1. Erstellen Sie eine `wlx.ini`-Datei und geben Sie den folgenden Parameter ein:

**WMSEnable**=yes\no

**WMSServer**=https://FQDN of the WMS Server:Port <By default 443 is used>

**GroupRegistrationKey**=GroupToken present in WMS Server

**CAValidation**=True/False

Geben Sie zum Beispiel zum Registrieren des Geräts mit ThinLinux Version 1.0 in der Wyse Management Suite (FQDN des Servers ist `ServerFQDN.domain.com`) mit dem Gruppentoken `defa-defadefa` und mit aktivierter CA-Validierungsoption die folgenden INI-Parameter ein:

**WMSEnable**=yes

**WMSServer**=https://ServerFQDN.domain.com:443

**GroupRegistrationKey**=defa-defadefa

**CAValidation**=True

2. Speichern Sie die `wlx.ini`-Datei im Ordner `wyse\wlx`.
3. Gehen Sie zu **Einstellungen** und wechseln Sie auf dem ThinLinux Thin Client zum Administrator.
4. Gehen Sie zu **Verwaltung > INI**.
5. Geben Sie die FTP-Server-URL ein.
6. Klicken Sie auf **Speichern** und starten Sie den Thin Client neu.
7. Gehen Sie zu **Verwaltung > Wyse Geräte-Agent**.  
In der Registerkarte „Wyse Geräte-Agent“ stehen die Wyse Verwaltungsserverdetails in dem entsprechenden Feld und der Client-Eintrag auf der Seite „Geräte“ des Wyse Verwaltungsservers zur Verfügung.


## Registrieren von Geräten mithilfe von DHCP-Options-Tags


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

**Tabelle 6. Registrieren von Geräten mithilfe von DHCP-Options-Tags**

Options-Tag	Beschreibung
<p><b>Name</b> – WMS</p> <p><b>Datentyp</b> – Zeichenfolge</p> <p><b>Code</b> – 165</p> <p><b>Beschreibung</b> – WMS-Server-FQDN</p>	<p>Dieses Tag verweist auf die Wyse Management Suite-Server-URL. Beispiel: <code>wmserver.acme.com</code>, wobei <code>wmserver.acme.com</code> der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist.</p> <p> <b>ANMERKUNG:</b> Verwenden Sie nicht "https://FQDN or FQDN:443" in der Server-URL, da der Thin Client sich sonst nicht bei der Wyse Management Suite anmeldet.</p>
<p><b>Name</b> – MQTT</p> <p><b>Datentyp</b> – Zeichenfolge</p> <p><b>Code</b> – 166</p> <p><b>Beschreibung</b> – 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:<a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>EU1:<a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p> <p>Sie müssen die MQTT-Serverdetails eingeben, wenn Sie Wyse Geräte-Agent-Details in der älteren Version von in ThinOS und Windows eingebetteten Geräten konfigurieren. MQTT ist eine Komponente von WMS, die erforderlich ist, um die Thin Clients zu benachrichtigen. Die URLs – mit und ohne MQTT-Details – müssen zur Zulassungsliste in der Wyse Management Suite Umgebung der öffentlichen Cloud hinzugefügt werden.</p>

**Tabelle 6. Registrieren von Geräten mithilfe von DHCP-Options-Tags (fortgesetzt)**

Options-Tag	Beschreibung
	 <b>ANMERKUNG:</b> Sie können die MQTT-URLs nicht verwenden, um sich bei der Wyse Management Suite anzumelden.
<b>Name</b> – CA-Validation <b>Datentyp</b> – Zeichenfolge <b>Code</b> – 167 <b>Beschreibung</b> – Zertifizierungsstellenprüfung	<p>Sie können die Option „CA-Validierung“ aktivieren oder deaktivieren, wenn Sie Ihre Geräte mit der Wyse Management Suite in der privaten Cloud registrieren. Standardmäßig ist die CA-Validierung in der öffentlichen Cloud aktiviert. Sie können die CA-Validierung auch in der öffentlichen Cloud deaktivieren.</p> <p>Geben Sie <b>Wahr</b> 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 <b>Falsch</b> 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>
<b>Name</b> – GroupToken <b>Datentyp</b> – Zeichenfolge <b>Code</b> – 199 <b>Beschreibung</b> – 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>


 **ANMERKUNG:** Ausführliche Informationen zum Hinzufügen von DHCP-Option-Tags auf dem Windows Server finden Sie unter [Wie Sie DHCP-Option-Tags erstellen und konfigurieren](#).

## Geräte mit DNS-SRV-Eintrag registrieren

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 7. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags**

URL/Tag	Beschreibung
<b>Eintragsname</b> – _WMS_MGMT <b>Eintrags-FQDN</b> – _WMS_MGMT._tcp.<Domänenname> <b>Eintragstyp</b> – SRV	<p>Dieser Eintrag verweist auf die Wyse Management Suite Server-URL. Beispiel: <code>wmserver.acme.com</code>, wobei <code>wmserver.acme.com</code> der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist.</p> <p> <b>ANMERKUNG:</b> Verwenden Sie nicht "https://FQDN or FQDN:443" in der Server-URL, da der Thin Client sich sonst nicht bei der Wyse Management Suite anmeldet.</p>
<b>Eintragsname</b> – _WMS_MQTT <b>Eintrags-FQDN</b> – _WMS_MQTT._tcp.<Domänenname> <b>Eintragstyp</b> – 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>

**Tabelle 7. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags (fortgesetzt)**

URL/Tag	Beschreibung
	<p> <b>ANMERKUNG:</b> MQTT ist bei der neuesten Version der Wyse Management Suite optional.</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 –<a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>EU1 –<a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p> <p>Sie müssen die MQTT-Serverdetails eingeben, wenn Sie Wyse Geräte-Agent-Details in der älteren Version von in ThinOS und Windows eingebetteten Geräten konfigurieren. MQTT ist eine Komponente von WMS, die erforderlich ist, um die Thin Clients zu benachrichtigen. Die URLs – mit und ohne MQTT-Details – müssen zur Zulassungsliste in der Wyse Management Suite Umgebung der öffentlichen Cloud hinzugefügt werden.</p> <p> <b>ANMERKUNG:</b> Sie können die MQTT-URLs nicht verwenden, um sich bei der Wyse Management Suite anzumelden.</p>
<p><b>Eintragsname</b> – _WMS_GROUPTOKEN</p> <p><b>Eintrags-FQDN</b> – _WMS_GROUPTOKEN._tcp.&lt;Domainname&gt;</p> <p><b>Eintragstyp</b> – 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> <b>ANMERKUNG:</b> Das Gruppentoken ist optional für die neueste Version von Wyse Management Suite in einer privaten Cloud.</p>
<p><b>Eintragsname</b> – _WMS_CAVALIDATION</p> <p><b>Eintrags-FQDN</b> – _WMS_CAVALIDATION._tcp.&lt;Domänenname&gt;</p> <p><b>Eintragstyp</b> – TEXT</p>	<p>Sie können die Option „CA-Validierung“ aktivieren oder deaktivieren, wenn Sie Ihre Geräte mit der Wyse Management Suite in der privaten Cloud registrieren. Standardmäßig ist die CA-Validierung in der öffentlichen Cloud aktiviert. Sie können die CA-Validierung auch in der öffentlichen Cloud deaktivieren.</p> <p>Geben Sie <b>Wahr</b> 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 <b>Falsch</b> 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> <b>ANMERKUNG:</b> CA Validation ist bei der neuesten Version der Wyse Management Suite optional.</p>

## Suchen nach einem Gerät mithilfe von Filtern

### Schritte

1. Wählen Sie aus der Dropdownliste **Konfigurationsgruppen** entweder die Standardrichtliniengruppe oder die Gruppen aus, die durch einen Administrator hinzugefügt wurden.
2. Wählen Sie in der Dropdownliste **Status** eine der folgenden Optionen aus:
  - **Registrierung**

- Registriert
  - Vorregistriert
  - Nicht registriert
  - Konform
  - Registrierungsvalidierung ausstehend
  - Ausstehend
  - Nicht konform
  - **Onlinestatus**
    - Online
    - Offline
    - Unbekannt
  - **Andere**
    - Zuletzt hinzugefügt
3. Wählen Sie in der Dropdownliste **OS-Typen** eines der folgenden Betriebssysteme aus:
- **Thin Client**
    - Linux
    - ThinLinux
    - ThinOS
    - WES
    - Teradici (private Cloud)
    - Wyse Software Thin Client
  - **Hybrid Client**
    - Hybrid Client
4. Wählen Sie aus der Dropdownliste **OS-Subtyp** einen Subtyp für Ihr Betriebssystem aus.
5. Wählen Sie eine Plattform aus der Dropdownliste **Plattform** aus.
6. Wählen Sie aus der Dropdownliste **OS-Version** eine Version des Betriebssystems aus.
7. Wählen Sie aus der Dropdownliste **Agentversion** eine Agentversion.
8. Wählen Sie aus der Dropdownliste **Subnetz/Präfix** ein Subnetz aus.
9. Wählen Sie aus der Dropdownliste **Zeitzone** eine Zeitzone aus.
10. Wählen Sie in der Dropdownliste **Tag-Nummer des Geräts** die Tag-Nummer des Geräts aus.
11. Wählen Sie in der **IP-Typ**-Dropdown-Liste den IP-Typ aus.
12. Wählen Sie aus der Dropdownliste **BIOS-Version** die BIOS-Version aus.

## Filter auf der Seite „Geräte“ speichern

Sie können den aktuellen Filter als Gruppe speichern, indem Sie die erforderlichen Filteroptionen konfigurieren.

### Schritte

1. Geben Sie den **Namen** des Filters ein.
2. Geben Sie eine Beschreibung des Filters im Kästchen **Beschreibung** ein.
3. Markieren Sie das Kontrollkästchen zum Einstellen der aktuellen Filter als Standardoption.
4. Klicken Sie auf **Filter speichern**.

## Abfragen des Gerätestatus

Zum Senden eines Befehls zum Aktualisieren der Geräte- und Statusinformationen im System führen Sie die folgenden Schritte aus:

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.

3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Klicken Sie auf **Abfragen**.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Klicken Sie auf **Befehl senden** zum Senden des Abfragebefehls.

## Sperrern der Geräte

Sie können einen Befehl senden, um das registrierte Gerät zu sperren. Diese Option wird nur für Thin Clients unterstützt, auf denen ThinOS als Betriebssystem ausgeführt wird.

### Voraussetzungen

Das Gerät sollte mit einer VDI Verbindung verbunden werden und ein Benutzer muss am Gerät angemeldet sein.

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Klicken Sie auf **Sperrern**.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Klicken Sie auf **Befehl senden** zum Senden des Befehls zum Sperrern.

## Neustart der Geräte

Sie können einen Befehl zum Neustart eines registrierten Geräts senden.

### Schritte


1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Klicken Sie auf **Neu starten**.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Klicken Sie auf **Befehl senden** zum Senden des Befehls zum Neustart.

## Registrierung eines Geräts aufheben

Sie können einen Befehl zum Aufheben der Registrierung eines Geräts über Wyse Management Suite senden.

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Klicken Sie auf **Registrierung aufheben**.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Aktivieren Sie das Kontrollkästchen **Aufhebung der Registrierung erzwingen**.
6. Klicken Sie auf **Befehl senden** zum Senden des Befehls zur Aufhebung der Registrierung.

 **ANMERKUNG:** Die Option „Aufhebung der Registrierung erzwingen“ kann verwendet werden, um das Gerät zu entfernen, wenn keine Kommunikation zwischen dem Server und dem Client besteht. Das Gerät wird in den nicht verwalteten Zustand versetzt

und lässt sich aus dem Servereintrag entfernen. Die Aktionen „Registrierung aufheben“ und „Aufhebung der Registrierung erzwingen“ können auch über die WES WDA UI durchgeführt werden kann.

## Anmeldungsvalidierung

Wenn Sie ein Gerät manuell oder mithilfe von DHCP/DNS-Auto-Ermittlungsmethode registrieren, wird das Gerät bei einer bestimmten Gruppe registriert, wenn das Gruppentoken definiert ist. Wenn das Gruppentoken nicht definiert ist, wird das Gerät in der nicht verwalteten Gruppe registriert.

In Wyse Management Suite wird die Option zur **Anmeldungsvalidierung** eingeführt, in der der Mandant manuell genehmigen muss, bevor das Gerät in einer Gruppe registriert wird.

Wenn die Option zur **Anmeldungsvalidierung** aktiviert ist, befinden sich die automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Validierung 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. Weitere Informationen zum Validieren der Geräte finden Sie unter [Anmeldungsvalidierung](#).

**ANMERKUNG:** Die Option zur **Anmeldungsvalidierung** ist für vorhandene Mandanten in der öffentlichen Cloud oder beim Upgrade von Vor-Ort-Mandanten deaktiviert.

Der Validierungsstatus der Geräte wird auch im Abschnitt **Geräte** auf der Seite **Dashboard** angezeigt.

## Validieren der Anmeldung eines Geräts

Sie können die **Anmeldung validieren**, damit Administratoren die manuelle und automatische Registrierung von Thin Clients in einer Gruppe steuern können. Sie können die Geräte im Status **Validierung ausstehend** filtern, indem Sie auf der Seite **Dashboard** auf den **Ausstehend**-Zähler klicken oder indem Sie in der Dropdownliste **Status** auf der Seite **Geräte** die Option **Anmeldungsvalidierung ausstehend** auswählen.

### Voraussetzungen

- Sie müssen die Option zur **Anmeldungsvalidierung** aktivieren, wenn Sie Wyse Management Suite oder auf der Seite **Portalverwaltung** installieren.
- Das Gerät muss sich im Status „Anmeldung ausstehend“ befinden.

### Schritte

1. Aktivieren Sie das Kontrollkästchen des Geräts, das Sie validieren möchten.
2. Klicken Sie auf die Option **Anmeldungsvalidierung**.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
3. Klicken Sie auf **Befehl senden**.  
Das Gerät wechselt zur gewünschten Gruppe und das Gerät wird registriert.

## Gerät auf Werkseinstellungen zurücksetzen

Sie können einen Befehl senden, um Ihr Gerät auf die werksseitigen Standardeinstellungen zurückzusetzen.

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Wählen Sie aus der Dropdownliste **Weitere Maßnahmen** die Option **Zurücksetzen auf Werkseinstellungen** aus.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Geben Sie den Grund für das Zurücksetzen des Clients an.
6. Klicken Sie auf **Befehl senden**.

# Ändern einer Gruppenzuweisung auf der Seite „Geräte“

Sie können die Gruppenzuweisung eines Geräts über die Seite **Geräte** ändern.

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Wählen Sie aus der Dropdownliste **Weitere Maßnahmen** die Option **Gruppe ändern** aus.  
Das Fenster **Gruppenzuweisung ändern** wird angezeigt.
5. Wählen Sie aus der Dropdownliste eine neue Gruppe für das Gerät aus.
6. Klicken Sie auf **Speichern**.

# Senden von Meldungen an ein Gerät

Sie können über die Seite **Geräte** eine Nachricht an ein registriertes Gerät senden.

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Geräte** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Wählen Sie aus der Dropdownliste **Weitere Maßnahmen** die Option **Nachricht senden** aus.  
Der Bildschirm **Nachricht senden** wird angezeigt.
5. Geben Sie die Nachricht ein.
6. Klicken Sie auf **Senden**.

# Wake on LAN-Befehl

Sie können einen Befehl senden, um ein Gerät zu aktivieren, wenn es ausgeschaltet ist oder sich im Energiesparmodus befindet.

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Wählen Sie aus der Dropdownliste **Weitere Maßnahmen** die Option **Wake on LAN** aus.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Klicken Sie auf **Befehl senden**.

# Anzeigen der Gerätedetails

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.

# Anzeigen der Anzeigeparameter

Ab Wyse Management Suite 3.1 können Sie die Anzeigeeinstellungen der Geräte anzeigen, die ein Windows Embedded- und ThinLinux-Betriebssystem ausführen. Sie können den Herstellernamen, die Modellnummer, die Seriennummer, die Auflösung, das Seitenverhältnis, den Modus, die Ausrichtung und die Rotationsdetails der Anzeigeeinstellungen anzeigen.

## Schritte

1. Rufen Sie die Seite **Geräte** auf.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
4. Navigieren Sie zu **Systeminfo > Peripheriegeräte**.  
Sie können auch die Details der Anzeigeeinstellungen anzeigen:

▼ Peripherals

Monitor							
Vendor	Model	Serial Number	Resolution	Aspect Ratio	Rotation	Mode	Alignment
DELL	UP3017	216L	2560x1600	16:10	normal	Span	3840,0
DELL	P2415Q	J0V0B(Primary)	3840x2160	16:9	normal	Span	0,0
DELL	P2415Q	V0D4L	3840x2160	16:9	normal	Span	6400,0
DELL	UP3017	211L	2560x1600	16:10	normal	Span	10240,0
DELL	P2415Q	YRB	0x0	0:0	normal	Span	12800,0
DELL	P2415Q	D5L	0x0	0:0	normal	Span	12800,0

Abbildung 9. Anzeigeparameter

# Anzeigen der Details zu virtuellen NICs

Ab Wyse Management Suite 3.1 können Sie die Details des Netzwerkadapters der Geräte anzeigen, auf denen ein Windows Embedded- und ThinLinux-Betriebssystem ausgeführt wird. Sie können den Adapternamen, die Mac-Adresse, die IP-Adresse, die Gateway-IP-Adresse und die DNS-Server-Details des Netzwerkadapters anzeigen.

## Schritte

1. Rufen Sie die Seite **Geräte** auf.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
4. Navigieren Sie zu **Systeminfo > Netzwerkdetails – Netzwerkadapter**.  
Sie können die Details der virtuellen NICs im Abschnitt **Netzwerkdetails – Netzwerkadapter** anzeigen.

▼ Network Details – Network Adapters

Adapter Name	MAC Address	IP Address	IPv6 Address	Gateway IP Address	DNS Server
eth0	E8:B0	10.150.		10.150.	10.150., 10.150.
eth1	E8:B0	10.150.		10.150.	10.150., 10.150.

Abbildung 10. Netzwerkdetails – Netzwerkadapter

# Überprüfen der BIOS-Details

Ab Wyse Management Suite 3.1 können Sie den BIOS-Parameterwert auf der Seite **Gerätedetails** anzeigen.

## Schritte

1. Rufen Sie die Seite **Geräte** auf.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt. Sie können die BIOS-Details im Abschnitt **BIOS-Einstellungen** auf der Registerkarte **Systeminfo** anzeigen.

# Verwalten der Gerätezusammenfassung

So können Sie Informationen zu Anmerkungen, Gruppenzuordnung, Warnungen und Gerätekonfiguration mit der Seite **Geräte** anzeigen und verwalten.

## Schritte

1. Klicken Sie auf **Geräte**.
2. Klicken Sie auf der Seite **Gerätedetails** auf die Registerkarte **Zusammenfassung**.  
Es wird die Gerätezusammenfassung angezeigt.
3. Klicken Sie im rechten Fensterbereich auf **Anmerkung hinzufügen**.  
Es wird das Fenster **Anmerkung hinzufügen** angezeigt.
4. Geben Sie die Nachricht in das entsprechende Feld ein und klicken Sie auf **Speichern**.
5. Klicken Sie im rechten Fensterbereich auf **Gruppenzuweisung ändern**.  
Das Fenster **Gruppenzuweisung ändern** wird angezeigt.
6. Wählen Sie aus der Dropdownliste eine neue Gruppe für das Gerät aus.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf **Ausnahmen erstellen/bearbeiten** zum Erstellen oder Bearbeiten einer Geräteklassenausnahme und konfigurieren Sie eine bestimmte Gerätegerichtlinie auf der Seite **Geräte**.

# Anzeigen von Systeminformationen

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
4. Klicken Sie auf **Systeminfo**.  
Die folgenden Systeminformationen werden angezeigt:

# Anzeigen von Geräteereignissen

Sie können Informationen über die Systemereignisse im Zusammenhang mit einem Gerät anzeigen und verwalten.

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.

2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
4. Klicken Sie auf der Seite **Gerätedetails** auf die Registerkarte **Ereignisse**.  
Die Ereignisse auf dem Gerät werden angezeigt.

## Anzeigen installierter Anwendungen

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
4. Klicken Sie auf die Registerkarte **installierte Apps**.  
Der Liste der installierten Anwendungen auf dem Gerät wird angezeigt.

Diese Option ist für Windows Embedded Standard-, Linux- und ThinLinux-Geräte verfügbar. Die folgenden Attribute werden auf der Seite angezeigt:

- Name
- Herausgeber
- Version
- Installiert auf

### ANMERKUNG:

Die Anzahl der installierten Anwendungen wird basierend auf der Installation oder Deinstallation von Anwendungen erhöht oder verringert. Die Liste wird beim nächsten Check-in oder Abfragen des Geräts aktualisiert.

## Umbenennen des Thin Client


Verwenden Sie diese Seite zum Ändern des Host-Namens von Thin Clients, die auf Windows-eingebetteten Standard-, ThinLinux- und ThinOS-Betriebssystemen ausgeführt werden.

### Schritte

1. Klicken Sie auf der Seite **Geräte** auf das Gerät.
2. Wählen Sie aus der Dropdownliste **Mehr Optionen** die Option **Host-Namen ändern**.
3. Geben Sie den neuen Host-Namen ein, wenn Sie dazu aufgefordert werden.

 **ANMERKUNG:** Der Host-Name darf nur alphanumerische Zeichen oder Bindestriche enthalten.

4. Für Windows-eingebettete Standard-Geräte befindet sich die Dropdownliste **Neustart** im Fenster **Warnung**. Um das System neu zu starten, wählen Sie die Option **Neu starten**. Wenn die Option **Später neu starten** ausgewählt ist, erfolgt der Neustart des Geräts zum konfigurierten Zeitpunkt und anschließend wird der Host-Name aktualisiert.



 **ANMERKUNG:** Ein ThinLinux-Gerät muss nicht neu gestartet werden, um den Host-Namen zu aktualisieren.

5. Klicken Sie auf **Befehl senden**.  
Es wird eine Bestätigungsmeldung angezeigt.

# Aktivieren von Remote Shadowing-Verbindung

Verwenden Sie diese Seite, um globalen Administratoren und Gruppenadministratoren den Remote-Zugriff auf die Windows-eingebetteten Standard-, ThinLinux- und ThinOS-Thin Client-Sitzungen zu ermöglichen. Diese Funktion ist nur für die private Cloud anwendbar und steht für Standard- und Pro-Lizenzen zur Verfügung.

## Schritte

1. Klicken Sie auf der Seite **Geräte** auf das Gerät.
2. Wählen Sie aus der Dropdownliste **Mehr Optionen** die Option **Remote-Spiegelung (VNC)**.  
Die IP-Adresse und die Port-Nummer des Ziel-Thin Clients wird im Dialogfeld **Remote-Spiegelung (VNC)** angezeigt.  
 **ANMERKUNG:** Die Standardportnummer ist 5900.
3. Ändern Sie die Portnummer des Ziel-Thin Clients – (optional)
4. Klicken Sie auf **Verbinden**, um eine Remote-Sitzung mit dem Ziel-Thin Client zu initiieren.  
 **ANMERKUNG:** Das Wyse Management Suite-Portal unterstützt maximal fünf Remote Shadowing-Sitzungen pro Mandant.

# Konfigurieren der Remote Shadowing-Verbindung für Dell Hybrid Client-Geräte

Auf dieser Seite können Sie den Remote-Zugriff auf die Dell Hybrid Client-Gerätesitzungen für globale und Gruppenadministratoren aktivieren. Diese Funktion ist nur für die private Cloud anwendbar und steht für Standard- und Pro-Lizenzen zur Verfügung.


## Schritte

1. Stellen Sie das VNC-Add-on-Paket von Wyse Management Suite mithilfe der standardmäßigen oder erweiterten Anwendungsrichtlinie bereit – siehe [Anwendungsrichtlinie](#).  
Das Add-on wird installiert und das Gerät neu gestartet.
2. Konfigurieren Sie die VNC-Serveroptionen von Wyse Management Suite und stellen Sie sie bereit. Gehen Sie zur Konfiguration der VNC-Serveroptionen wie folgt vor:
  - a. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
  - b. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **Hybrid Client**.  
Das Fenster **Konfigurationssteuerelement | Hybrid Client** wird angezeigt.
  - c. Klicken Sie auf die Option **Standard** oder **Erweitert**.
  - d. Gehen Sie zu **Datenschutz und Sicherheit > VNC-Server** und konfigurieren Sie die Optionen.
  - e. Klicken Sie auf **Speichern und Veröffentlichen**.

# Herunterfahren von Geräten

Mit der Wyse Management Suite können Sie Geräte wie Windows-eingebettete Standard-, ThinLinux- und ThinOS-Thin-Clients herunterfahren.

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Klicken Sie in der Dropdown-Liste **Weitere Optionen** auf **Jetzt herunterfahren**.  
Der Remote-Befehl zum Abschalten des Geräts wird an das ausgewählte Gerät gesendet. Das Gerät antwortet auf den Server und der Befehl wird erfolgreich ausgeführt.  
 **ANMERKUNG:** Die Option **Jetzt herunterfahren** ist für Thin Clients unter Linux nicht aktiviert.

# Hinzufügen eines Tags zu einem Gerät

Wyse Management Suite ermöglicht Ihnen die Identifizierung eines Geräts oder einer Gruppe von Geräten durch die Verwendung der Option **Gerät mit Tag versehen**.

## Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.  
Die Liste bevorzugter Geräte wird angezeigt.
3. Wählen Sie ein oder mehrere Geräte aus. Klicken Sie in der Dropdownliste **Weitere Optionen** auf **Gerät mit Tag versehen**.  
Das Fenster **Geräte-Tag einrichten** wird angezeigt.
4. Geben Sie den bevorzugten Tag-Namen ein.
5. Klicken Sie auf **Tag einrichten**.

# Compliance-Status des Geräts

Standardmäßig werden die folgenden Farben als Gerätestatus angezeigt:

- Rot: wenn das registrierte Gerät seit mehr als sieben Tagen nicht überprüft wurde.
- Grau: wenn Sie eine beliebige Konfigurationsrichtlinie auf das Gerät anwenden.
- Grün: wenn Sie alle Konfigurationsrichtlinien auf das Gerät anwenden.

Der Standardwert kann von 1 bis 99 Tage geändert werden.

Die Option **Onlinestatus** befindet sich neben dem Gerätenamen. Es werden die folgenden Farben unter Onlinestatus angezeigt:

- Rot: wenn das Gerät seinen Heartbeat öfter als drei Versuche nicht gesendet hat.
- Grau: wenn das Gerät seinen Heartbeat öfter als zwei Versuche, aber nicht öfter als drei Versuche nicht gesendet hat.
- Grün: wenn das Gerät seinen Heartbeat regelmäßig sendet.

# Pull für Windows Embedded Standard oder ThinLinux-Abbild ausführen

## Voraussetzungen

- Wenn Sie das Remote-Repository der Wyse Management Suite 1.3 verwenden, ist die Pull-Vorlage Wiederherstellung/Wiederherstellung + OS nicht im Repository verfügbar. Sie müssen die Wyse Management Suite auf Version 1.4 oder höher aktualisieren, um auf die Vorlagen zugreifen zu können.
- Um den Pull-Vorgang für ein ThinLinux-Abbild durchzuführen, müssen Sie das Fenster **Einstellungen** auf dem ThinLinux-Gerät schließen. Sie müssen diesen Vorgang durchführen, bevor Sie ein OS/OS+Wiederherstellung-Abbild vom ThinLinux-Gerät beziehen.
- Um von ThinLinux 1.x auf 2.x zu aktualisieren, muss der Administrator das Gerät mit dem neuesten WDA und Merlin aktualisieren und dann das Abbild beziehen. Dieses bezogene Abbild muss für ein Upgrade von ThinLinux 1.x auf 2.x verwendet werden.
- Stellen Sie sicher, dass die virtuelle Maschine, auf der der Server ausgeführt wird, über genügend Arbeitsspeicher verfügt, um den Pull-Vorgang durchzuführen und die erforderlichen Dienste für Wyse Management Suite auszuführen, wenn Sie ein lokales Repository verwenden.

## Schritte

1. Wechseln Sie zur Geräteseite **Windows Embedded Standard** oder **ThinLinux**.
2. Wählen Sie die Option **OS-Abbild abrufen** aus der Dropdownliste **Weitere Maßnahmen** aus.
3. Geben Sie folgende Informationen ein bzw. wählen Sie sie aus:
  - **Namen des Images**: Geben Sie einen Namen für das Abbild an. Zum Ersetzen des Abbilds mit einem ähnlichen Namen und Bilddateien, die nicht erfolgreich abgeschlossen wurden, klicken Sie auf **Name überschreiben**.
  - **Datei-Repository**: Wählen Sie aus der Dropdownliste das Datei-Repository aus, in das das Abbild hochgeladen werden soll. Es gibt zwei Arten von Datei-Repositories:
    - Lokales Repository
    - Wyse Management Suite Remote-Repository

- **Pull-Typ:** Wählen Sie entweder **Standard** oder **Erweitert** basierend darauf, welchen Pull-Typ Sie benötigen.
    - Wenn der Pull-Typ **Standard** ausgewählt ist, werden die folgenden Optionen angezeigt:
      - Komprimieren
      - OS
      - BIOS
      - Wiederherstellung – Für ThinLinux 2.x
    - Wenn der Pull-Typ **Erweitert** ausgewählt ist, wird eine Dropdownliste für die Auswahl der Vorlagen angezeigt. Wählen Sie eine Vorlage aus, die standardmäßig verfügbar ist.
- ANMERKUNG:** Sie können durch Bearbeiten der vorhandenen oder Standardvorlagen benutzerdefinierte Vorlagen verwenden, die manuell erstellt wurden.

4. Klicken Sie auf **Auf Image-Pull vorbereiten**.

### Ergebnisse

Wenn der Befehl **OS-Abbild abrufen** gesendet wird, empfängt das Client-Gerät eine Pull-Anforderung für ein Abbild vom Server. Eine Nachricht bezüglich der Pull-Anforderung für ein Abbild wird auf der Client-Seite angezeigt. Klicken Sie auf eine der folgenden Optionen:

- **Pull nach Sysprep** – Das Gerät wird neu gestartet und meldet sich beim Betriebssystem in einem deaktivierten Zustand an. Führen Sie das benutzerdefinierte Sysprep aus. Nachdem das benutzerdefinierte Sysprep abgeschlossen ist, startet das Gerät das Betriebssystem Merlin und der Pull-Vorgang für das Abbild wird durchgeführt.

**ANMERKUNG:** Diese Option gilt nur für Windows Embedded Standard-Geräte.

- **Pull jetzt ausführen** – Das Gerät startet das Betriebssystem Merlin und der Pull-Vorgang für das Abbild wird durchgeführt.

## Anfordern einer Protokolldatei

Um ein Geräteprotokoll von Windows-eingebetteten Standard-, ThinOS- und ThinLinux-Geräten anzufordern, führen Sie die folgenden Schritte aus: Das ThinOS-Gerät lädt die Systemprotokolle hoch. Der Windows Embedded Standard lädt Protokolle des Wyse Geräte-Agenten und der Windows-Ereignisanzeige hoch. Linux oder ThinLinux lädt Protokolle des Wyse Geräte-Agenten und Systemprotokolle hoch.

### Voraussetzungen

Das Gerät muss aktiviert sein, um einen Pull für eine Protokolldatei auszuführen.

### Schritte

1. Gehen Sie auf die Seite **Geräte** und klicken Sie auf ein bestimmtes Gerät.  
Die Gerätedetails werden angezeigt.
2. Klicken Sie auf die Registerkarte **Geräteprotokoll**.
3. Klicken Sie auf **Protokolldatei anfordern**.
4. Nachdem die Protokolldateien auf den Wyse Management Suite-Server hochgeladen wurden, klicken Sie auf den Link **Klicken Sie hier** und laden Sie die Protokolle herunter.

**ANMERKUNG:** Die Geräteprotokolle liegen im `hostname-timestamp`-Format vor. Dell Hybrid Client, Linux oder ThinLinux lädt die Protokolldatei im `.tar`-Format hoch und ein Windows- oder ThinOS 9.x-System im `.zip`-Format.

## Fehlerbehebung auf Ihrem Gerät

Sie können die Fehlerbehebungs-Informationen über die Seite **Geräte** anzeigen und verwalten.

### Schritte

1. Klicken Sie auf der Seite **Gerätedetails** auf die Registerkarte **Fehlerbehebung**.
2. Klicken Sie auf **Screenshot anfordern**.  
Sie können den Screenshot des Thin Client mit oder ohne Zustimmung des Clients erstellen. Wenn das Kontrollkästchen **Zustimmung des Benutzers erforderlich machen** ausgewählt ist, wird auf dem Client eine Meldung angezeigt. Diese Option gilt nur für Windows Embedded Standard-, Linux- und ThinLinux-Geräte.

3. Klicken Sie auf **Prozessliste anfordern**, um die Liste der ausgeführten Verfahren auf dem Thin Client anzufordern.
4. Klicken Sie auf **Dienstliste anfordern**, um die Liste der ausgeführten Dienste auf dem Thin Client anzufordern.
5. Klicken Sie auf **Überwachung starten** für den Zugriff auf die Konsole Leistungsmetrik.  
Auf der Konsole **Leistungsmetrik** werden die folgenden Details angezeigt:
  - Durchschnittliche CPU-Last in der letzten Minute.
  - Durchschnittliche Speichernutzung in der letzten Minute

## Erstellen eines neuen Image Ihres Dell Hybrid Client

Sie können einen Befehl zum Erstellen eines neuen Image Ihres Dell Hybrid Clients senden.

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Wählen Sie aus der Dropdownliste **Weitere Maßnahmen** die Option **Neues Image erstellen** aus.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Klicken Sie auf **Befehl senden**.  
Mit dieser Aktion wird die Funktion, ein Recovery-Image für das Gerät zu erstellen, ausgeführt.

## Benutzeroberflächen-Konfigurationspaket für Dell Hybrid Client herunterladen

Wenn ein Dell Hybrid-Client über eine höhere Version des Konfigurationsschemas verfügt, als auf dem Wyse Management Suite-Server vorhanden ist, können Sie das neueste Benutzeroberflächen-Konfigurationspaket abrufen.

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Klicken Sie auf das Gerät, das Sie konfigurieren möchten.  
Die Seite **Gerätedetails** wird angezeigt.
4. Wählen Sie aus der Dropdownliste **Weitere Maßnahmen** die Option **Benutzeroberflächen-Konfigurationspaket herunterladen** aus.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Klicken Sie auf **Befehl senden**.

## Zurücksetzen des Dell Hybrid Clients auf die Werkseinstellungen

Sie können einen Befehl senden, um Ihren Dell Hybrid Client auf die werksseitigen Standardeinstellungen zurückzusetzen.

### Schritte

1. Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
4. Wählen Sie aus der Dropdownliste **Weitere Maßnahmen** die Option **Zurücksetzen auf Werkseinstellungen** aus.  
Es wird ein Fenster mit einer **Warnung** angezeigt.

5. Geben Sie den Grund für das Zurücksetzen des Dell Hybrid Clients an.
6. Klicken Sie auf **Befehl senden**.

# Anwendungen und Daten

In diesem Abschnitt wird beschrieben, wie Aufgaben zur routinemäßigen Geräteanwendung, Betriebssystem-Abbilderstellung, Bestandsverwaltung und das Festlegen von Richtlinien mithilfe der Wyse-Managementkonsole funktionieren. Die Repository-Namen sind zur Anzeige des Status farblich gekennzeichnet.

Sie können die folgenden Typen von Richtlinien über die Seite **Anwendungen und Daten** konfigurieren:

- Standardanwendungsrichtlinie – Diese Richtlinie ermöglicht die Installation eines einzigen Anwendungspakets.
- Erweiterte Anwendungsrichtlinie – Diese Richtlinie ermöglicht die Installation von mehreren Anwendungspaketen.
- Abbildrichtlinie – Diese Richtlinie ermöglicht die Installation des Betriebssystems.

Die Bereitstellung von Anwendungsrichtlinien und Betriebssystemabbildern auf Thin Clients kann für sofort oder später geplant werden, basierend auf einer bestimmten Zeitzone oder der Zeitzone, die auf dem Gerät konfiguriert ist.

## Themen:

- [Anwendungsrichtlinie](#)
- [Abbildrichtlinie](#)
- [Verwalten eines Datei-Repositorys](#)

## Anwendungsrichtlinie

Die Wyse Management Suite unterstützt die folgenden Arten von Anwendungsbestandsaufnahme- und Anwendungsbereitstellungsrichtlinien:

- Konfigurieren einer Thin-Client-Anwendungsbestandsaufnahme
- Konfigurieren der Wyse Software Thin-Client-Anwendungsbestandsaufnahme
- Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Thin Clients
- Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients
- Erstellen und Bereitstellen einer Standardanwendungsrichtlinie auf Wyse Software Thin Clients
- Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie für Wyse Software-Thin Clients

### Wichtige Hinweise für Windows-basierte Geräte:

- Unterstützt die Installation für Windows-basierte Anwendungen mit der Erweiterung .msi, .exe, .msu, .msp.  
Eine Anwendung mit einer anderen Erweiterung wird heruntergeladen auf %systemdrive%\wyse\WDA" Ex: "C:\wyse\WDA
- Für die Bereitstellung von EXE-Anwendungen unter Verwendung der Wyse Management Suite befolgen Sie die Methode der automatischen Installation. Sie müssen gegebenenfalls die entsprechenden Parameter für die automatische Installation eingeben. Zum Beispiel **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**
- Unterstützt Skriptbereitstellungen mit Dateierweiterungen .bat, .cmd, .ps1, .vbs.  
Ein Skript mit anderer Erweiterung wird heruntergeladen auf %systemdrive%\wyse\WDA" Ex: "C:\wyse\WDA.
- Skripte, die unter Verwendung der Wyse Management Suite bereitgestellt werden, sollten nicht-interaktiv sein, das heißt, dass während der Installation keine Benutzermaßnahme erforderlich ist.
- Wenn in der erweiterten Anwendungsrichtlinie ein Skript/eine EXE-Datei vorhanden ist, die einen anderen Wert als 0 zurückgibt, wird dies als Fehler betrachtet.
- Wenn in der erweiterten Anwendungsrichtlinie die Vorinstallation fehlschlägt, wird die Anwendungsinstallation nicht fortgesetzt.
- Skripte/EXE-Dateien, die unter Verwendung der Standardanwendung bereitgestellt werden, sind erfolgreich, und der Fehlercode wird im Jobstatus aktualisiert.
- Für Anwendungen mit der Erweiterung msi/msu/msp werden Standardfehlercodes berichtet. Wenn eine Anwendung „REBOOT\_REQUIRED“ zurückgibt, wird das Gerät einmal zusätzlich neu gestartet.

### Wichtige Hinweise für Linux-Geräte:

- Unterstützt die Installation für Linux-basierte Anwendungen mit der Erweiterung .bin, .deb für ThinLinux 2.0 und .RPM für Thin Linux 1.0.
- Unterstützt Skriptbereitstellungen für ThinLinux-Geräte mit der Erweiterung .sh.

- Wenn in der Standard- oder erweiterten Anwendungsrichtlinie ein Skript/eine deb./rpm.-Datei vorhanden ist, das bzw. die einen anderen Wert als 0 zurückgibt, wird dies als Fehler betrachtet.
- Wenn in der erweiterten Anwendungsrichtlinie die Vorinstallation fehlschlägt, wird die Anwendungsinstallation nicht fortgesetzt.

## Konfigurieren einer Thin-Client-Anwendungsbestandsaufnahme

### Schritte

1. Klicken Sie auf die Registerkarte **Anwendungen und Daten**.
2. Gehen Sie im linken Fensterbereich auf **App-Bestand Thin Client**. Anwendungsdetails werden im Fenster **Thin Client Bestand** angezeigt.
3. Um eine Anwendung zum Bestand hinzuzufügen, legen Sie die Thin Client-Anwendungsdateien im Ordner `<repo-dir>\repository\thinClientApps` ab. Das Wyse Management Suite Repository sendet Metadaten für alle Dateien in regelmäßigen Abständen an den Wyse Management Suite-Server.
4. Zum Bearbeiten der Anwendung gehen Sie wie folgt vor:
  - a. Wählen Sie die hochgeladene Anwendung aus der Liste aus.
  - b. Klicken Sie auf **App bearbeiten**. Das Fenster **Anwendung bearbeiten** wird angezeigt.
  - c. Geben Sie die Notiz ein.
  - d. Klicken Sie auf **Speichern**.

 **ANMERKUNG:** Den vom Operator hochgeladenen Anwendungen wird ein globales Suffix hinzugefügt.

Die Anwendungen, die in verschiedenen Repositories vorhanden sind, werden einmal aufgelistet. Die Spalte **Repository-Name** zeigt die Anzahl der Repositories an, in denen sich die Anwendung befindet. Sie können den Mauszeiger über die Spalte bewegen, um den Namen der Repositories anzuzeigen. Außerdem ist der Name des Repositories farblich gekennzeichnet, um die Verfügbarkeit anzugeben.

## Konfigurieren der Wyse Software Thin-Client-Anwendungsbestandsaufnahme


### Schritte

1. Klicken Sie auf die Registerkarte **Anwendungen und Daten**.
2. Gehen Sie im linken Fensterbereich auf **App-Bestand > Wyse Software Thin Client**.
3. Zum Hinzufügen einer Anwendung zum Bestand legen Sie die Thin Client-Anwendungsdateien im Ordner `<repo-dir>\repository\softwareTcApps` ab. Das Wyse Management Suite Repository sendet Metadaten für alle Dateien in regelmäßigen Abständen an den Wyse Management Suite-Server.

## Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Thin Clients

### Schritte

1. Gehen Sie im lokalen Repository zu **thinClientApps** und kopieren Sie die Anwendung in den Ordner.
2. Gehen Sie zu **Apps & Daten > App-Bestand > Thin Client** und überprüfen Sie, ob die Anwendung bei der Wyse Management Suite registriert ist.
 

 **ANMERKUNG:** Die App-Bestand-Benutzeroberfläche benötigt etwa zwei Minuten, um alle kürzlich hinzugefügten Programme zu generieren.
3. Gehen Sie zu **Apps & Daten > App-Richtlinien > Thin Client**.
4. Klicken Sie auf **Richtlinie hinzufügen**. Das Fenster **Standard-App-Richtlinie hinzufügen** wird angezeigt.
5. Geben Sie den **Richtliniennamen** ein.

6. Wählen Sie aus dem Dropdownmenü **Gruppe** die Gruppe aus.
7. Wählen Sie die **Aufgabe** aus dem Dropdownmenü aus.
8. Wählen Sie aus dem Dropdownmenü **OS-Typ** das Betriebssystem aus.
9. Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
10. Wählen Sie eine **Anwendung** aus dem Dropdownmenü aus.  
Wenn die Anwendungsdateien in mehreren Repositories verfügbar sind, wird neben dem Dateinamen die Anzahl der Repositories angezeigt.
- ANMERKUNG:** Ab Wyse Management Suite 3.1 können Sie ein Skript hinzufügen, um die Anwendung auf ThinLinux-Geräten zu installieren. Sie müssen überprüfen, ob ein gültiger Hash-Bang im Skript für ThinLinux vorhanden ist.
11. Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
12. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:
  - **Nicht automatisch anwenden** – Richtlinien werden nicht automatisch auf ein Gerät angewendet.
  - **Richtlinie auf neue Geräte anwenden** – Die Richtlinie wird automatisch auf ein registriertes Gerät angewendet, das zu einer ausgewählten Gruppe gehört oder zu dem Gerät, das in eine ausgewählte Gruppe verschoben wird. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle neuen Geräte angewendet, die in der Gruppe registriert werden. Um den Job auf den vorhandenen Geräten in der Gruppe ausführen zu können, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind. Der Jobstatus der neu hinzugefügten Geräteanzahl, die registriert wurde, wird nicht angezeigt.
  - **Richtlinie beim Check-in-Vorgang auf Geräte anwenden** – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle in der Gruppe vorhandenen Geräte angewendet. Um den Job auf vorhandenen Geräten in der Gruppe sofort oder zu einem geplanten Zeitpunkt vor der Geräteanmeldung auszuführen, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind.
- ANMERKUNG:** Der Jobstatus der neu hinzugefügten Geräteanzahl, die bei Wyse Management Suite angemeldet wird, wird nicht angezeigt.
- ANMERKUNG:** Geben Sie für Windows-basierte Geräte die Parameter für die automatische Installation für .exe-Dateien an, um die Anwendung im Hintergrund auszuführen. Zum Beispiel **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**
13. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an. Der Standardwert beträgt 60 Minuten.
- ANMERKUNG:** Die Option für die **Zeitüberschreitung der Anwendungsinstallation** gilt nur für Windows Embedded Standard-, Wyse Software Thin Client-, Linux- und ThinLinux-Geräte.
14. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.  
Eine Meldung wird angezeigt, um dem Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu erlauben.
15. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.
16. Wählen Sie aus den folgenden Optionen aus:
  - **Sofort** – Der Server führt den Job sofort aus.
  - **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
  - **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.
17. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
18. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

## Erstellen und Bereitstellen einer Standardanwendungsrichtlinie auf Wyse Software Thin Clients

### Schritte

1. Gehen Sie im lokalen Repository zu **softwareTcApps** und kopieren Sie die Anwendung in den Ordner.
2. Gehen Sie zu **Apps & Daten > App-Bestand > Wyse Software Thin Client** und überprüfen Sie, ob die Anwendung bei Wyse Management Suite registriert ist.

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

3. Klicken Sie auf **Richtlinie hinzufügen**.  
Das Fenster **Standard-App-Richtlinie hinzufügen** wird angezeigt.
  4. Geben Sie den **Richtliniennamen** ein.
  5. Wählen Sie aus dem Dropdownmenü **Gruppe** die Gruppe aus.
  6. Wählen Sie die **Aufgabe** aus dem Dropdownmenü aus.
  7. Wählen Sie aus dem Dropdownmenü **OS-Typ** das Betriebssystem aus.
  8. Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
  9. Wählen Sie eine **Anwendung** aus dem Dropdownmenü aus.  
Wenn die Anwendungsdateien in mehreren Repositorys verfügbar sind, wird neben dem Dateinamen die Anzahl der Repositorys angezeigt.
  10. Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
  11. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:
    - **Nicht automatisch anwenden** – Richtlinien werden nicht automatisch auf ein Gerät angewendet.
    - **Richtlinie auf neue Geräte anwenden** – Die Richtlinie wird automatisch auf ein registriertes Gerät angewendet, das zu einer ausgewählten Gruppe gehört oder zu dem Gerät, das in eine ausgewählte Gruppe verschoben wird. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle neuen Geräte angewendet, die in der Gruppe registriert werden. Um den Job auf den vorhandenen Geräten in der Gruppe ausführen zu können, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind. Der Jobstatus der neu hinzugefügten Geräteanzahl, die registriert wurde, wird nicht angezeigt.
    - **Richtlinie beim Check-in-Vorgang auf Geräte anwenden** – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle in der Gruppe vorhandenen Geräte angewendet. Um den Job auf vorhandenen Geräten in der Gruppe sofort oder zu einem geplanten Zeitpunkt vor der Geräteanmeldung auszuführen, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind.
- ANMERKUNG:** Der Jobstatus der neu hinzugefügten Geräteanzahl, die bei Wyse Management Suite angemeldet wird, wird nicht angezeigt.
- ANMERKUNG:** Geben Sie für Windows-basierte Geräte die Parameter für die automatische Installation für .exe-Dateien an, um die Anwendung im Hintergrund auszuführen. Zum Beispiel **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**
12. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an. Der Standardwert beträgt 60 Minuten.  
**ANMERKUNG:** Die Option **Zeitüberschreitung für die Anwendungsinstallation** gilt nur für Windows Embedded Standard-Geräte und Wyse Software Thin Clients.
  13. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.  
Eine Meldung wird angezeigt, um dem Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu erlauben.
  14. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.
  15. Wählen Sie aus den folgenden Optionen aus:
    - **Sofort** – Der Server führt den Job sofort aus.
    - **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
    - **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.
  16. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
  17. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

## Einmaliges Anmelden für Citrix StoreFront mithilfe der Standard-Anwendungsrichtlinie aktivieren


Um die einmalige Anmeldung für Citrix StoreFront zu aktivieren, gehen Sie wie folgt vor:


- **Szenario 1:** Wenn Sie die einmalige Anmeldung für StoreFront auf der aktuellen Version von Citrix Receiver aktivieren möchten, gehen Sie wie folgt vor:
  1. Erstellen und verteilen Sie eine Standard-Anwendungsrichtlinie zur Deinstallation von Citrix Receiver mit dem Parameter **/silent**.
  2. Erstellen und verteilen Sie eine Standard-Anwendungsrichtlinie zur Installation von Citrix Receiver mit dem Parameter **/silent /includeSSON /AutoUpdateCheck = Disabled**.
- **Szenario 2:** Wenn Sie Citrix Receiver aktualisieren und die einmalige Anmeldung für StoreFront aktivieren möchten, gehen Sie wie folgt vor:
  1. Erstellen und verteilen Sie eine Standard-Anwendungsrichtlinie zur Aktualisierung von Citrix Receiver mit dem Parameter **/silent /includeSSON /AutoUpdateCheck = Disabled**.
- **Szenario 3:** Wenn Sie für den Citrix Receiver ein Downgrade durchführen und die einmalige Anmeldung für StoreFront aktivieren möchten, gehen Sie wie folgt vor:
  1. Erstellen und verteilen Sie eine Standard-Anwendungsrichtlinie für ein Downgrade von Citrix Receiver mit dem Parameter **/silent /includeSSON /AutoUpdateCheck = Disabled**.

## Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients

### Schritte

1. Kopieren Sie die Anwendung und die Skripte für vor oder nach der Installation (falls erforderlich) zur Bereitstellung auf den Thin Clients.
2. Speichern Sie die Anwendung und die Skripte vor/nach der Installation im Ordner thinClientApps im lokalen Repository oder dem Wyse Management Suite-Repository.
3. Gehen Sie zu **Apps & Daten > App-Bestand > Thin Client** und überprüfen Sie, ob die Anwendung registriert ist.
4. Gehen Sie zu **Apps & Daten > App-Richtlinien > Thin Client**.
5. Klicken Sie auf **Erweiterte Richtlinie hinzufügen**. Die Seite **Erweiterte App-Richtlinie hinzufügen** wird angezeigt.
6. Geben Sie den **Richtliniennamen** ein.
7. Wählen Sie aus dem Dropdownmenü **Gruppe** die Gruppe aus.
8. Aktivieren Sie das Kontrollkästchen **Untergruppen**, um die Richtlinie auf Untergruppen anzuwenden.
9. Wählen Sie die **Aufgabe** aus dem Dropdownmenü aus.
10. Wählen Sie aus dem Dropdownmenü **OS-Typ** das Betriebssystem aus.
11. Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
12. Klicken Sie auf **App hinzufügen** und wählen Sie einen oder mehrere Anwendungen unter **Apps**. Für jede Anwendung können Sie ein Skript vor und nach der Installation unter **Vorinstallation**, **Nachinstallation** und **Installations-Parameter** wählen.
 

 **ANMERKUNG:** Ab Wyse Management Suite 3.1 können Sie ein Skript hinzufügen, um die Anwendung auf ThinLinux-Geräten zu installieren. Sie müssen überprüfen, ob ein gültiger Hash-Bang im Skript für ThinLinux vorhanden ist.
13. Wenn Sie möchten, dass das System nach der erfolgreichen Installation der Anwendung neu starten soll, wählen Sie **Neustart**.
14. Klicken Sie auf **App hinzufügen** und wiederholen Sie den Schritt zum Hinzufügen mehrerer Anwendungen.
 

 **ANMERKUNG:** Zum Beenden der Anwendungsrichtlinie beim ersten Fehler wählen Sie **App-Abhängigkeit aktivieren**. Wenn diese Option nicht ausgewählt ist, wirkt sich der Fehler einer Anwendung auf die Richtlinienimplementierung aus.

Wenn die Anwendungsdateien in mehreren Repositories verfügbar sind, wird neben dem Dateinamen die Anzahl der Repositories angezeigt.
15. Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
16. Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client angezeigt werden soll. Eine Meldung auf dem Client, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt.
17. Damit eine Verzögerung bei der Implementierung der Richtlinie ermöglicht wird, aktivieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Dropdownmenüs aktiviert:
  - Wählen Sie aus der Dropdownliste **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 der Dropdownliste **Max. Verzögerungen** wie oft Sie die Ausführung der Richtlinie verzögern können (1 bis 3 Mal).
18. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:

- **Nicht automatisch anwenden** – Richtlinien werden nicht automatisch auf ein Gerät angewendet.
- **Richtlinie auf neue Geräte anwenden** – Die Richtlinie wird automatisch auf ein registriertes Gerät angewendet, das zu einer ausgewählten Gruppe gehört oder zu dem Gerät, das in eine ausgewählte Gruppe verschoben wird. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle neuen Geräte angewendet, die in der Gruppe registriert werden. Um den Job auf den vorhandenen Geräten in der Gruppe ausführen zu können, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind. Der Jobstatus der neu hinzugefügten Geräteanzahl, die registriert wurde, wird nicht angezeigt.
- **Richtlinie beim Check-in-Vorgang auf Geräte anwenden** – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle in der Gruppe vorhandenen Geräte angewendet. Um den Job auf vorhandenen Geräten in der Gruppe sofort oder zu einem geplanten Zeitpunkt vor der Geräteanmeldung auszuführen, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind.

**ANMERKUNG:** Der Jobstatus der neu hinzugefügten Geräteanzahl, die bei Wyse Management Suite angemeldet wird, wird nicht angezeigt.

**ANMERKUNG:** Geben Sie für Windows-basierte Geräte die Parameter für die automatische Installation für .exe-Dateien an, um die Anwendung im Hintergrund auszuführen. Zum Beispiel **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**

19. Aktivieren Sie das Kontrollkästchen **Überprüfung des Schreibfilters überspringen**, um die Schreibfiltervorgänge zu überspringen. Diese Option gilt für Geräte mit Windows Embedded Standard-Betriebssystem und Wyse Software Thin Client-Geräte.

20. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an. Der Standardwert beträgt 60 Minuten.

**ANMERKUNG:** Die Option **Zeitüberschreitung für die Anwendungsinstallation** gilt nur für Windows Embedded Standard-Geräte und Wyse Software Thin Clients.

21. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.

Eine Meldung wird angezeigt, um dem Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu erlauben.

22. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.

23. Wählen Sie aus den folgenden Optionen aus:

- **Sofort** – Der Server führt den Job sofort aus.
- **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
- **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.

24. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.

25. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

## Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie für Wyse Software-Thin Clients

### Schritte

1. Kopieren Sie die Anwendung und die Skripte vor/nach der Installation (falls erforderlich) zur Bereitstellung auf den Thin Clients.
2. Speichern Sie die Anwendung und die Skripte vor/nach der Installation im Ordner thinClientApps im lokalen Repository oder dem Wyse Management Suite-Repository.
3. Gehen Sie zu **Apps & Daten > App-Bestand > Wyse Software Thin Client** und überprüfen Sie, ob die Anwendung registriert ist.
4. Gehen Sie zu **Apps & Daten > App-Richtlinien > Wyse Software Thin Client**.
5. Klicken Sie auf **Erweiterte Richtlinie hinzufügen**. Die Seite **Erweiterte App-Richtlinie hinzufügen** wird angezeigt.
6. Geben Sie den **Richtliniennamen** ein.
7. Wählen Sie aus dem Dropdownmenü **Gruppe** die Gruppe aus.
8. Aktivieren Sie das Kontrollkästchen **Untergruppen**, um die Richtlinie auf Untergruppen anzuwenden.
9. Wählen Sie die **Aufgabe** aus dem Dropdownmenü aus.
10. Wählen Sie aus dem Dropdownmenü **OS-Typ** das Betriebssystem aus.
11. Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.

12. Klicken Sie auf **App hinzufügen** und wählen Sie einen oder mehrere Anwendungen unter **Apps**. Für jede Anwendung können Sie ein Skript vor und nach der Installation unter **Vorinstallation**, **Nachinstallation** und **Installations-Parameter** wählen.
13. Wenn Sie möchten, dass das System nach der erfolgreichen Installation der Anwendung neu starten soll, wählen Sie **Neustart**.
14. Klicken Sie auf **App hinzufügen** und wiederholen Sie den Schritt zum Hinzufügen mehrerer Anwendungen.

**ANMERKUNG:** Zum Beenden der Anwendungsrichtlinie beim ersten Fehler wählen Sie **App-Abhängigkeit aktivieren**. Wenn diese Option nicht ausgewählt ist, wirkt sich der Fehler einer Anwendung auf die Richtlinienimplementierung aus.

Wenn die Anwendungsdateien in mehreren Repositorys verfügbar sind, wird neben dem Dateinamen die Anzahl der Repositorys angezeigt.

15. Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
16. Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client angezeigt werden soll. Eine Meldung auf dem Client, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt.
17. Damit eine Verzögerung bei der Implementierung der Richtlinie ermöglicht wird, aktivieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Dropdownmenüs aktiviert:
  - Wählen Sie aus der Dropdownliste **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 der Dropdownliste **Max. Verzögerungen** wie oft Sie die Ausführung der Richtlinie verzögern können (1 bis 3 Mal).
18. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:
  - **Nicht automatisch anwenden** – Richtlinien werden nicht automatisch auf ein Gerät angewendet.
  - **Richtlinie auf neue Geräte anwenden** – Die Richtlinie wird automatisch auf ein registriertes Gerät angewendet, das zu einer ausgewählten Gruppe gehört oder zu dem Gerät, das in eine ausgewählte Gruppe verschoben wird. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle neuen Geräte angewendet, die in der Gruppe registriert werden. Um den Job auf den vorhandenen Geräten in der Gruppe ausführen zu können, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind. Der Jobstatus der neu hinzugefügten Geräteanzahl, die registriert wurde, wird nicht angezeigt.
  - **Richtlinie beim Check-in-Vorgang auf Geräte anwenden** – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle in der Gruppe vorhandenen Geräte angewendet. Um den Job auf vorhandenen Geräten in der Gruppe sofort oder zu einem geplanten Zeitpunkt vor der Geräteanmeldung auszuführen, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind.

**ANMERKUNG:** Der Jobstatus der neu hinzugefügten Geräteanzahl, die bei Wyse Management Suite angemeldet wird, wird nicht angezeigt.

**ANMERKUNG:** Geben Sie für Windows-basierte Geräte die Parameter für die automatische Installation für .exe-Dateien an, um die Anwendung im Hintergrund auszuführen. Zum Beispiel **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**




19. Aktivieren Sie das Kontrollkästchen **Überprüfung des Schreibfilters überspringen**, um die Schreibfiltervorgänge zu überspringen. Diese Option gilt für Geräte mit Windows Embedded Standard-Betriebssystem und Wyse Software Thin Client-Geräte.
20. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an. Der Standardwert beträgt 60 Minuten.

**ANMERKUNG:** Die Option **Zeitüberschreitung für die Anwendungsinstallation** gilt nur für Windows Embedded Standard-Geräte und Wyse Software Thin Clients.

21. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen. Eine Meldung wird angezeigt, um dem Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu erlauben.
22. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.
23. Wählen Sie aus den folgenden Optionen aus:
  - **Sofort** – Der Server führt den Job sofort aus.
  - **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
  - **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.
24. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
25. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

# Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Dell Hybrid Clients

## Schritte

1. Gehen Sie im lokalen Repository zu **hybridClientApps** und kopieren Sie die Anwendung in den Ordner.  
 **ANMERKUNG:** Sie können nur von Dell signierte Anwendungen auf Dell Hybrid Clients bereitstellen und installieren.
2. Gehen Sie zu **Apps & Daten > App-Bestand > Hybrid Client** und überprüfen Sie, ob die Anwendung bei der Wyse Management Suite registriert ist.  
 **ANMERKUNG:** Die App-Bestand-Benutzeroberfläche benötigt etwa zwei Minuten, um die kürzlich hinzugefügten Programme zu generieren.
3. Gehen Sie zu **Apps & Daten > App-Richtlinien > Hybrid Client**.
4. Klicken Sie auf **Richtlinie hinzufügen**.  
Das Fenster **Standard-App-Richtlinie hinzufügen** wird angezeigt.
5. Geben Sie den **Richtliniennamen** ein.
6. Wählen Sie aus dem Dropdownmenü **Gruppe** die Gruppe aus.
7. Wählen Sie die **Aufgabe** aus dem Dropdownmenü aus.
8. Wählen Sie aus dem Dropdownmenü **OS-Typ** das Betriebssystem aus.
9. Wählen Sie eine **Anwendung** aus dem Dropdownmenü aus.  
Wenn die Anwendungsdateien in mehreren Repositories verfügbar sind, wird neben dem Dateinamen die Anzahl der Repositories angezeigt.
10. Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
11. Geben Sie im Feld **Installationsparameter** die Installationsparameter für die ausgewählte Anwendung ein.
12. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:
  - **Nicht automatisch anwenden** – Richtlinien werden nicht automatisch auf ein Gerät angewendet.
  - **Richtlinie auf neue Geräte anwenden** – Die Richtlinie wird automatisch auf ein registriertes Gerät angewendet, das zu einer ausgewählten Gruppe gehört oder zu dem Gerät, das in eine ausgewählte Gruppe verschoben wird. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle neuen Geräte angewendet, die in der Gruppe registriert werden. Um den Job auf den vorhandenen Geräten in der Gruppe ausführen zu können, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind. Der Jobstatus der neu hinzugefügten Geräteanzahl, die registriert wurde, wird nicht angezeigt.
  - **Richtlinie beim Check-in-Vorgang auf Geräte anwenden** – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle in der Gruppe vorhandenen Geräte angewendet. Um den Job auf vorhandenen Geräten in der Gruppe sofort oder zu einem geplanten Zeitpunkt vor der Geräteanmeldung auszuführen, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind.
-  **ANMERKUNG:** Der Jobstatus der neu hinzugefügten Geräteanzahl, die bei Wyse Management Suite angemeldet wird, wird nicht angezeigt.
13. Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client im Feld **Zeitüberschreitung (1–999 Min.)** angezeigt werden soll. Die Zeitüberschreitung zeigt eine Meldung auf dem Client an, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt.
14. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an. Der Standardwert beträgt 60 Minuten.
15. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.  
Eine Meldung wird angezeigt, um dem Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu erlauben.
16. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.
17. Wählen Sie aus den folgenden Optionen aus:
  - **Sofort** – Der Server führt den Job sofort aus.
  - **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
  - **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.

18. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
19. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

## Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Dell Hybrid Clients

### Schritte


1. Kopieren Sie die Anwendung und die Skripte der Installation (falls erforderlich) zur Bereitstellung auf den Thin Clients.
 

 **ANMERKUNG:** Sie können nur von Dell signierte Anwendungen und Skripte auf Dell Hybrid Clients bereitstellen und installieren.
2. Speichern Sie die Anwendung und die Skripte der Installation im Ordner `hybridClientApps` im lokalen Repository oder dem Wyse Management Suite-Repository.
3. Gehen Sie zu **Apps & Daten > App-Bestand > Hybrid Client** und überprüfen Sie, ob die Anwendung registriert ist.
4. Gehen Sie zu **Apps & Daten > App-Richtlinien > Hybrid Client**.
5. Klicken Sie auf **Erweiterte Richtlinie hinzufügen**.  
Die Seite **Erweiterte App-Richtlinie hinzufügen** wird angezeigt.
6. Geben Sie den **Richtliniennamen** ein.
7. Wählen Sie aus dem Dropdownmenü **Gruppe** die Gruppe aus.
8. Aktivieren Sie das Kontrollkästchen **Untergruppen**, um die Richtlinie auf Untergruppen anzuwenden.
9. Wählen Sie die **Aufgabe** aus dem Dropdownmenü aus.
10. Wählen Sie aus dem Dropdownmenü **OS-Typ** das Betriebssystem aus.
11. Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
12. Klicken Sie auf **App hinzufügen** und wählen Sie einen oder mehrere Anwendungen unter **Apps**. Für jede Anwendung können Sie ein Skript vor und nach der Installation unter **Vorinstallation**, **Nachinstallation** und **Installations-Parameter** wählen.
13. Wenn Sie möchten, dass das System nach der erfolgreichen Installation der Anwendung neu starten soll, wählen Sie **Neustart**.
14. Klicken Sie auf **App hinzufügen** und wiederholen Sie den Schritt zum Hinzufügen mehrerer Anwendungen.
 

 **ANMERKUNG:** Zum Beenden der Anwendungsrichtlinie beim ersten Fehler wählen Sie **App-Abhängigkeit aktivieren**. Wenn diese Option nicht ausgewählt ist, wirkt sich der Fehler einer Anwendung auf die Richtlinienimplementierung aus.

Wenn die Anwendungsdateien in mehreren Repositories verfügbar sind, wird neben dem Dateinamen die Anzahl der Repositories angezeigt.

15. Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
16. Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client angezeigt werden soll.  
Eine Meldung auf dem Client, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt.
17. Damit eine Verzögerung bei der Implementierung der Richtlinie ermöglicht wird, aktivieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Dropdownmenüs aktiviert:
  - Wählen Sie aus der Dropdownliste **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 der Dropdownliste **Max. Verzögerungen** wie oft Sie die Ausführung der Richtlinie verzögern können (1 bis 3 Mal).
18. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:
  - **Nicht automatisch anwenden** – Richtlinien werden nicht automatisch auf ein Gerät angewendet.
  - **Richtlinie auf neue Geräte anwenden** – Die Richtlinie wird automatisch auf ein registriertes Gerät angewendet, das zu einer ausgewählten Gruppe gehört oder zu dem Gerät, das in eine ausgewählte Gruppe verschoben wird. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle neuen Geräte angewendet, die in der Gruppe registriert werden. Um den Job auf den vorhandenen Geräten in der Gruppe ausführen zu können, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind. Der Jobstatus der neu hinzugefügten Geräteanzahl, die registriert wurde, wird nicht angezeigt.
  - **Richtlinie beim Check-in-Vorgang auf Geräte anwenden** – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet. Wenn diese Option ausgewählt ist, wird die Richtlinie auf alle in der Gruppe vorhandenen Geräte angewendet. Um den Job auf vorhandenen Geräten in der Gruppe sofort oder zu einem geplanten Zeitpunkt vor der Geräteanmeldung auszuführen, müssen Sie die Richtlinie planen. Nachdem Sie die Richtlinie geplant haben, zeigt der Jobstatus die Anzahl der Geräte an, die bereits in der Gruppe vorhanden sind.

 **ANMERKUNG:** Der Jobstatus der neu hinzugefügten Geräteanzahl, die bei Wyse Management Suite angemeldet wird, wird nicht angezeigt.

19. Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client im Feld **Zeitüberschreitung (1–999 Min.)** angezeigt werden soll. Die Zeitüberschreitung zeigt eine Meldung auf dem Client an, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt.
20. Um den Installationsprozess nach einem festgelegten Wert zu stoppen, geben Sie im Feld **Zeitüberschreitung für Anwendungsinstallation** die Anzahl der Minuten an. Der Standardwert beträgt 60 Minuten.
21. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.  
Eine Meldung wird angezeigt, um dem Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu erlauben.
22. Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.
23. Wählen Sie eine der folgenden Optionen:
  - **Sofort** – Der Server führt den Job sofort aus.
  - **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
  - **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.
24. Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
25. Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

## Abbildrichtlinie

Die Wyse Management Suite unterstützt die folgenden Arten von Richtlinien zur Bereitstellung von Betriebssystemabbildern:


- Hinzufügen der Windows-eingebetteten Standard-Betriebssystem- und ThinLinux-Abbildern zum Repository
- Hinzufügen von ThinOS-Firmware zum Repository
- Hinzufügen von ThinOS-Paketdatei zu Repository
- Hinzufügen von ThinOS-BIOS-Datei zu Repository
- Hinzufügen von Teradici-Firmware zum Repository
- Erstellen von Windows-eingebetteten Standard- und ThinLinux-Abbildrichtlinien.
- Erstellen von Dell Hybrid Client-Abbildrichtlinien

## Hinzufügen von Windows-eingebetteten Standard-Betriebssystem- und ThinLinux-Abbildern zum Repository

### Voraussetzungen

- Wenn Sie die Wyse Management Suite mit Cloudbereitstellung verwenden, rufen Sie **Portalverwaltung > Konsoleneinstellungen > Datei-Repository** auf. Klicken Sie auf **Version 2.0 herunterladen** oder **Version 1.4 herunterladen**, um die Datei `WMS_Repo.exe` herunterzuladen, und installieren Sie das Wyse Management Suite-Repository-Installationsprogramm.
- Wenn Sie die Wyse Management Suite mit Bereitstellung vor Ort verwenden, wird das lokale Repository während der Installation der Wyse Management Suite installiert.

### Schritte

1. Kopieren Sie die Windows Embedded Standard-Betriebssystemabbilder oder ThinLinux-Abbilder in den Ordner `<Repository Location>\repository\osImages\zipped`.  
Die Wyse Management Suite extrahiert die Dateien aus dem komprimierten Ordner und lädt die Dateien in den Ordner `<Repository Location>\repository\osImages\valid` hoch. Das Extrahieren der Abbilder kann mehrere Minuten dauern, je nach Abbildgröße.  
 **ANMERKUNG:** Laden Sie für das ThinLinux-Betriebssystem das merlin-Abbild herunter, z. B. `1.0.7_3030LT_merlin.exe`, und kopieren Sie es in den Ordner `<Repository Location>\repository\osImages\zipped`.

Das Abbild wird zum Repository hinzugefügt.

2. Rufen Sie **Anwendungen und Daten > OS-Abbild-Repository > WES/ThinLinux** auf, um das registrierte Abbild anzuzeigen.

## Hinzufügen von ThinOS-Firmware zum Repository

### Schritte

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

**ANMERKUNG:** Die Datei wird zum Repository hinzugefügt, wenn Sie das Kontrollkästchen auswählen. Sie ist jedoch keiner Gruppe und keinem Gerät zugewiesen. Zur Bereitstellung einer Firmware auf einem Gerät oder einer Gruppe von Geräten gehen Sie zur Konfigurationsseite des jeweiligen Geräts oder der Gruppe.

## Hinzufügen von ThinOS-BIOS-Datei zum Repository

### Schritte

1. Klicken Sie in der Registerkarte **Apps & Daten** unter **OS-Abbild-Repository** auf **ThinOS**.
2. Klicken Sie auf **BIOS-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. Wählen Sie die Plattform aus der Dropdown-Liste "BIOS-Plattformtyp" aus.
7. 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. Zur Bereitstellung einer BIOS-Datei auf einem Gerät oder einer Gruppe von Geräten gehen Sie zur Konfigurationsseite des jeweiligen Geräts oder der Gruppe.

## Hinzufügen von ThinOS-Paketdatei zu Repository

### Schritte

1. Klicken Sie in der Registerkarte **Apps & Daten** unter **OS-Abbild-Repository** auf **ThinOS**.
2. Klicken Sie auf **Paketdatei 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. Klicken Sie auf **Hochladen**.

**ANMERKUNG:** Wenn die Anwendung bereits im öffentlichen Repository vorhanden ist, wird die Anwendungsreferenz dem Bestand hinzugefügt. Andernfalls wird die Anwendung in das öffentliche Repository hochgeladen und die Referenz wird dem Bestand hinzugefügt. Vom Operator hochgeladene ThinOS-Firmware und BIOS-Pakete können von den Mandanten-Administratoren nicht gelöscht werden.

# Erstellen von Windows-eingebetteten Standard- und ThinLinux-Abbildrichtlinien.

## Schritte

1. Klicken Sie auf der Registerkarte **Apps & Daten** unter **OS-Abbildrichtlinien** auf **WES/ThinLinux**.
2. Klicken Sie auf **Richtlinie hinzufügen**.  
Der Bildschirm **WES-/ThinLinux-Richtlinie hinzufügen** wird angezeigt.
3. Gehen Sie auf der Seite **WES-/ThinLinux-Richtlinie hinzufügen** folgendermaßen vor:
  - a. Geben Sie einen **Richtliniennamen** ein.
  - b. Wählen Sie im Dropdownmenü **Gruppe** eine Gruppe aus.
  - c. Wählen Sie aus dem Dropdownmenü **OS-Typ** den OS-Typ aus.
  - d. Wählen Sie aus dem Dropdownmenü **OS-Subtypfilter** einen OS-Subtypfilter aus.
  - e. Wenn Sie ein Abbild auf einem bestimmten Betriebssystem oder einer bestimmten Plattform bereitstellen möchten, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter**.
  - f. Wählen Sie aus dem Dropdownmenü **OS-Abbild** eine Abbilddatei aus.
  - g. Wählen Sie aus dem Dropdownmenü **Regel** eine der folgenden Regeln aus, die Sie für die Abbildrichtlinie einrichten möchten:
    - Nur Upgrade
    - Downgrade zulassen
    - Diese Version erzwingen
  - h. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:
    - Nicht automatisch anwenden – Die Abbildrichtlinie wird nicht automatisch auf ein Gerät angewendet, das in der Wyse Management Suite registriert ist.
    - Richtlinie auf neue Geräte anwenden – Die Abbildrichtlinie wird auf ein neues Gerät bei der Registrierung in der Wyse Management Suite angewendet.
    - Richtlinie beim Check-In-Vorgang auf Geräte anwenden – Die Abbildrichtlinie wird auf ein neues Gerät beim Check-in angewendet, wenn es in der Wyse Management Suite registriert ist.
4. Klicken Sie auf **Speichern**.

## Hinzufügen von ThinOS-Firmware zum Repository

### Schritte

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

#### ANMERKUNG:

- Die hochgeladene Firmware kann nur für das Upgrade von ThinOS 8.6 auf ThinOS 9.1 verwendet werden.
- Die Datei wird zum Repository hinzugefügt, wenn Sie das Kontrollkästchen auswählen. Sie ist jedoch keiner Gruppe und keinem Gerät zugewiesen. Zur Bereitstellung einer Firmware auf einem Gerät oder einer Gruppe von Geräten gehen Sie zur Konfigurationsseite des jeweiligen Geräts oder der Gruppe.

## Hinzufügen von ThinOS-Anwendungspaketen zum Repository

### Schritte

1. Melden Sie sich mit ihren Mandanten-Anmeldedaten bei Wyse Management Suite an.
2. Klicken Sie in der Registerkarte **Apps & Daten** unter **OS-Abbild-Repository** auf **ThinOS 9.x**.

3. Klicken Sie auf **Paketdatei hinzufügen**.  
Der Bildschirm **Paket hinzufügen** wird angezeigt.
4. Um eine Datei auszuwählen, klicken Sie auf **Durchsuchen** und wechseln Sie zum Speicherort, an dem sich die Datei befindet.
  - Wenn die EULA im Paket integriert ist, werden die EULA-Details des Pakets und der Name der Anbieter angezeigt. Sie können auf die Namen der einzelnen Anbieter klicken, um ihre jeweilige Lizenzvereinbarung zu lesen. Klicken Sie auf **Akzeptieren**, um das Paket hochzuladen. Sie können die Option **Nicht mehr anzeigen** auswählen, wenn Sie die EULA-Details desselben Anbieters nicht mehr sehen möchten. Sie müssen die Lizenzvereinbarung der Pakete einzeln akzeptieren. Das Paket wird nicht hochgeladen, wenn Sie auf **Ablehnen** klicken.
  - Wenn die EULA nicht im Paket integriert ist, fahren Sie mit Schritt 5 fort.
5. Klicken Sie auf **Hochladen**.

## Erstellen von Dell Hybrid Client-Abbildrichtlinien

Sie können eine Dell Hybrid Client-Abbildrichtlinie erstellen, um Wyse 5070 Thin Clients, auf denen das Betriebssystem Windows 10 IoT Enterprise, ThinLinux 2.x oder ThinOS 8.x ausgeführt wird, in Dell Hybrid Client-Geräte zu konvertieren.

### Schritte

1. Klicken Sie auf der Registerkarte **Apps & Daten** unter **OS-Abbildrichtlinien** auf **Hybrid Client**.
2. Klicken Sie auf **Richtlinie hinzufügen**.
3. Gehen Sie auf der Seite **Hybrid Client-Richtlinie hinzufügen** folgendermaßen vor:
  - a. Geben Sie einen **Richtliniennamen** ein.
  - b. Wählen Sie im Dropdownmenü **Gruppe** eine Gruppe aus.
  - c. Wählen Sie aus dem Dropdownmenü **OS-Typ** den OS-Typ aus.
  - d. Wählen Sie aus dem Dropdownmenü **OS-Subtypfilter** einen OS-Subtypfilter aus.
  - e. Wenn Sie ein Abbild auf einem bestimmten Betriebssystem oder einer bestimmten Plattform bereitstellen möchten, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter**.
  - f. Wählen Sie aus dem Dropdownmenü **OS-Abbild** eine Abbilddatei aus.
  - g. Wählen Sie in der Dropdownliste **Regel** die Option **Diese Version erzwingen** aus.
  - h. Wählen Sie aus dem Dropdownmenü **Richtlinie automatisch anwenden** eine der folgenden Optionen aus:
    - Nicht automatisch anwenden – Die Abbildrichtlinie wird nicht automatisch auf ein Gerät angewendet, das in der Wyse Management Suite registriert ist.
    - Richtlinie auf neue Geräte anwenden – Die Abbildrichtlinie wird auf ein neues Gerät bei der Registrierung in der Wyse Management Suite angewendet.
4. Klicken Sie auf **Speichern**.

**ANMERKUNG:** Die Anzahl der DHC-Lizenzen muss größer oder gleich der Anzahl der Wyse 5070 Thin Clients sein, die in Dell Hybrid Client konvertiert werden.

**ANMERKUNG:** Das DHC-Konvertierungs Betriebssystem-Image im ZIP- oder EXE-Format muss in den Ordner `\repository\osImages\zipped` kopiert werden. Das DHC OS-Image wird nach der Repository-Synchronisierung unter **Apps & Daten > OS-Image-Repository > Hybrid Client** angezeigt.

**ANMERKUNG:** Sie müssen eine Betriebssystem-Abbildrichtlinie erstellen, um das DHC-Konversions-Image auf Wyse 5070 Thin Clients bereitzustellen, auf denen ein Windows Embedded-, ThinLinux-, Thin- und Thin-PCoIP-Betriebssystem ausgeführt wird.

**ANMERKUNG:** Stellen Sie sicher, dass das Merlin-Paket für Thin Clients, auf denen Windows 10 IoT Enterprise- und ThinLinux 2.x-Betriebssysteme ausgeführt werden, auf 408 oder höher aktualisiert wird.

## Verwalten eines Datei-Repositorys

Dieser Abschnitt ermöglicht Ihnen das Anzeigen und Verwalten der Datei-Repository-Bestände, wie z. B. Hintergrundbild, Logo, EULA-Textdatei, Windows Wireless-Profil und Zertifikatsdateien.

### Schritte

1. Auf der Registerkarte **Apps & Daten** klicken Sie unter **Datei-Repository** auf **Bestand**.
2. Klicken Sie auf **Datei hinzufügen**.

Der Bildschirm **Datei hinzufügen** wird angezeigt.

- Um eine Datei auszuwählen, klicken Sie auf **Durchsuchen** und wechseln Sie zum Speicherort, an dem sich die Datei befindet.
- Wählen Sie aus dem Dropdownmenü **Typ** eine der folgenden Optionen, die am besten Ihrem Dateityp entspricht:

- Zertifikat
- Hintergrundbild
- Logo
- EULA-Textdatei
- Windows Wireless-Profil
- INI-Datei
- Sprache
- Druckerzuordnungen
- Schriftart
- Hosts
- Regeln

**i ANMERKUNG:** Zum Anzeigen der maximalen Größe und der unterstützten Dateiformate, die Sie hochladen können, klicken Sie auf das Symbol **Informationen (i)**.

- Wählen Sie das Kontrollkästchen aus, wenn Sie eine vorhandene Datei überschreiben möchten.

**i 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.

- Klicken Sie auf **Hochladen**.

## Ändern des Hintergrundbilds für alle Geräte, die einer Marketinggruppe angehören

### Schritte

- Navigieren Sie zur Registerkarte **Apps & Daten**.
- In der Navigationsleiste wählen Sie im linken Fenster **Bestand**.
- Klicken Sie auf die Schaltfläche **Datei hinzufügen**.
- Navigieren Sie zum Bild, das Sie als Hintergrundbild verwenden möchten, und wählen Sie es aus.
- Als Typ wählen Sie **Hintergrundbild**.
- Geben Sie die Beschreibung ein und klicken Sie auf **Hochladen**.

Zum Ändern der Konfigurationsrichtlinie für eine Gruppe durch Zuordnen eines neuen Hintergrundbilds führen Sie die folgenden Schritte aus:

- Navigieren Sie zur Seite **Gruppen & Konfiguration**.
- Wählen Sie eine Richtliniengruppe aus.
- Klicken Sie auf **Richtlinien bearbeiten** und wählen Sie **WES**.
- Wählen Sie **Desktoperlebnis** und klicken Sie auf **Dieses Element konfigurieren**.
- Wählen Sie **Desktop-Hintergrundbild** aus.
- Wählen Sie aus der Dropdownliste die Hintergrundbild-Datei.
- Klicken Sie auf **Speichern und Veröffentlichen**.

Klicken Sie auf **Jobs** zum Überprüfen des Status der Konfigurationsrichtlinie. Sie können zum Überprüfen von Geräten mit deren Status auf die Zahl neben dem Status-Flag in der Spalte **Details** klicken.

# Verwalten von Regeln

In diesem Abschnitt wird beschrieben, wie Sie Regeln der Wyse Management Suite-Konsole hinzufügen und verwalten. Es stehen folgende Filteroptionen zur Verfügung:

- **Registrierung**
- **Automatische Zuweisung nicht verwalteter Geräte**
- **Warnmeldung**

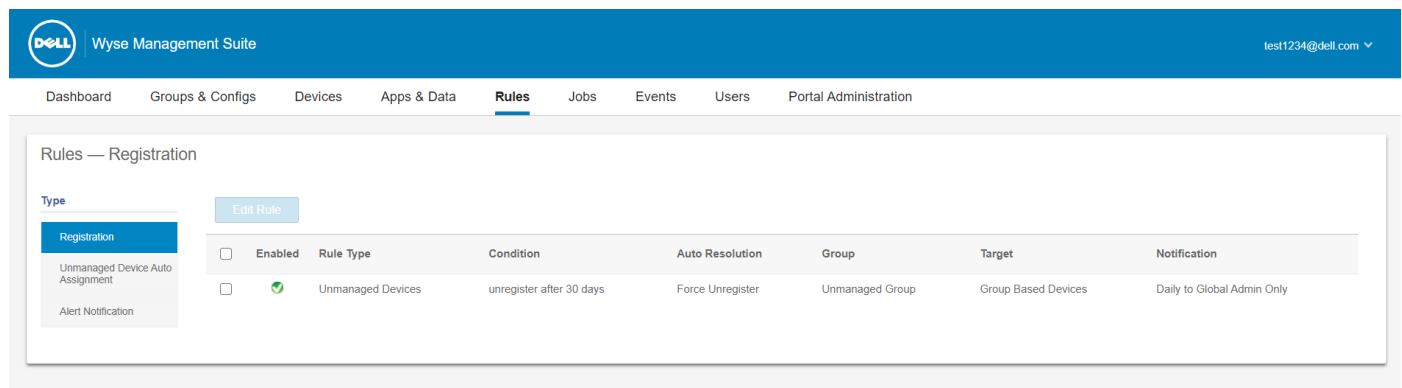


Abbildung 11. Seite „Regeln“

## Themen:


- Bearbeiten einer Registrierungsregel
- Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte
- Bearbeitung der Regel für die automatische Zuweisung nicht verwalteter Geräte
- Deaktivieren und Löschen von Regeln für die automatische Zuweisung nicht verwalteter Geräte
- Speichern der Regelreihenfolge
- Hinzufügen einer Regel für Warnmeldungen
- Bearbeiten einer Warnmeldungsregel

## Bearbeiten einer Registrierungsregel

Konfigurieren Sie die Regeln für nicht verwaltete Geräte mithilfe der Option **Registrierung**.

### Schritte

1. Klicken Sie auf **Regeln**.  
Die Seite **Regeln** wird angezeigt.
2. Klicken Sie auf **Registrierung** und wählen Sie die Option für nicht verwaltete Geräte aus.
3. Klicken Sie auf **Regel bearbeiten**.  
Das Fenster **Regel bearbeiten** wird angezeigt.  
Sie können auch folgende Details anzeigen:
  - Regel
  - Beschreibung
  - Geräteziel
  - Gruppe
4. Wählen Sie aus der Dropdownliste einen Ziel-Client zum Übernehmen der Option **Benachrichtigungsziel** und die Zeitdauer zur Anwendung der Option **Benachrichtigungsfrequenz**.

 **ANMERKUNG:** Die Benachrichtigungsfrequenz kann auf alle 4 Stunden, alle 12 Stunden, täglich oder wöchentlich für das Zielgerät konfiguriert werden.

5. Geben Sie die gewünschte Anzahl der Tage bis zur Anwendung der Regel im Feld **Regel nach (1-30 Tage) anwenden** ein.

 **ANMERKUNG:** Standardmäßig werden Registrierungen von nicht verwalteten Geräten nach 30 Tagen aufgehoben.

6. Klicken Sie auf **Speichern**.

## Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte

### Schritte

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie die Option **Automatische Zuweisung nicht verwalteter Geräte**.
3. Klicken Sie auf die Registerkarte **Regeln hinzufügen**.
4. Geben Sie den **Namen** ein und wählen Sie die **Zielgruppe**.
5. Klicken Sie auf die Option **Bedingung hinzufügen** und wählen Sie die Bedingungen für zugewiesene Regeln.
6. Klicken Sie auf **Speichern**.

Die Regel wird in der Liste der nicht verwalteten Gruppe angezeigt. Diese Regel wird automatisch angewendet und das Gerät in der Zielgruppe aufgeführt.

 **ANMERKUNG:** Die Regeln werden nicht auf Geräte im Status „Anmeldung ausstehend“ angewendet.

## Bearbeitung der Regel für die automatische Zuweisung nicht verwalteter Geräte

### Schritte

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie die Option **Automatische Zuweisung nicht verwalteter Geräte**.
3. Wählen Sie die Regel aus und klicken Sie auf die Option **Bearbeiten**.
4. Geben Sie den **Namen** ein und wählen Sie die **Zielgruppe**.
5. Klicken Sie auf die Option **Bedingung hinzufügen** und wählen Sie die Bedingungen für zugewiesene Regeln.
6. Klicken Sie auf **Speichern**.

## Deaktivieren und Löschen von Regeln für die automatische Zuweisung nicht verwalteter Geräte

### Schritte

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie die Option **Automatische Zuweisung nicht verwalteter Geräte**.
3. Wählen Sie eine Regel aus und klicken Sie auf die Option **Regel deaktivieren**.  
Die ausgewählte Regel wird deaktiviert.
4. Wählen Sie die deaktivierte Regel aus und klicken Sie auf die Option **Deaktivierte Regel(n) löschen**.  
Die Regel wird gelöscht.

# Speichern der Regelreihenfolge

## Voraussetzungen

Wenn mehrere Regeln vorhanden sind, können Sie die Reihenfolge ändern, in der eine Regel auf die Geräte angewendet wird.

## Schritte

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie die Option **Automatische Zuweisung nicht verwalteter Geräte**.
3. Wählen Sie die Regel aus, die Sie verschieben möchten, und bewegen Sie sie dann bis ganz nach oben.
4. Klicken Sie auf **Regelreihenfolge speichern**.

 **ANMERKUNG:** Die IPv6-Präfix-Regelreihenfolge kann nicht geändert werden.

# Hinzufügen einer Regel für Warnmeldungen

## Schritte

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie die Option **Warnmeldung** aus.
3. Klicken Sie auf **Regel hinzufügen**.  
Es wird das Fenster **Regel hinzufügen** angezeigt.
4. Wählen Sie in der Dropdownliste **Regel** eine Regel aus.
5. Geben Sie die **Beschreibung** ein.
6. Wählen Sie aus der Dropdownliste **Gruppe** die gewünschte Option aus.
7. Wählen Sie aus der Dropdownliste ein Zielgerät zum Übernehmen von **Benachrichtigungsziel** und die Zeitdauer zur Anwendung von **Benachrichtigungsfrequenz**.
8. Klicken Sie auf **Speichern**.

# Bearbeiten einer Warnmeldungsregel

## Schritte

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie die Option **Warnmeldung** aus.
3. Klicken Sie auf **Regel bearbeiten**.  
Das Fenster **Regel bearbeiten** wird angezeigt.
4. Wählen Sie in der Dropdownliste **Regel** eine Regel aus.
5. Geben Sie die **Beschreibung** ein.
6. Wählen Sie in der Dropdownliste **Gruppen** eine Gruppe aus.
7. Wählen Sie in der Dropdownliste ein Zielgerät zum Anwenden des **Benachrichtigungsziels** und die Zeitdauer zum Anwenden der **Benachrichtigungsfrequenz** aus.
8. Klicken Sie auf **Speichern**.

## Aufträge verwalten

In diesem Abschnitt wird beschrieben, wie Sie Jobs in der Managementkonsole planen und verwalten.

Auf dieser Seite können Sie Jobs auf der Grundlage der folgenden Filteroptionen anzeigen:

- **Konfigurationsgruppen** – Wählen Sie aus dem Dropdownmenü den Konfigurationsgruppentyp aus.
- **Geplant von** – Wählen Sie aus dem Dropdownmenü den Planer, der die Planungsaktivität ausführt. Die verfügbaren Optionen sind:
  - Admin
    - App-Richtlinie
    - Abbildrichtlinie
    - Gerätebefehle
  - System
    - Gruppenkonfiguration veröffentlichen
    - Andere
- **Betriebssystemtyp** – Wählen Sie das Betriebssystem aus dem Dropdownmenü. Die verfügbaren Optionen sind:
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse Software Thin Client
  - Hybrid Client
- **Status** – Wählen Sie aus dem Dropdownmenü den Status des Jobs aus. Die verfügbaren Optionen sind:
  - Geplant
  - Wird ausgeführt/In Verarbeitung
  - Abgeschlossen
  - Abgebrochen
  - Fehlgeschlagen
- **Detailstatus** – Wählen Sie aus dem Dropdownmenü den Status im Detail. Die verfügbaren Optionen sind:
  - 1 oder mehr fehlgeschlagen
  - 1 oder mehr ausstehend
  - 1 oder mehr in Verarbeitung
  - 1 oder mehr abgebrochen
  - 1 oder mehr abgeschlossen
- **Weitere Maßnahmen** – Wählen Sie aus dem Dropdownmenü die Option **BIOS-Administratorkennwort synchronisieren**. Das Job-Fenster BIOS-Administratorkennwort synchronisieren wird angezeigt

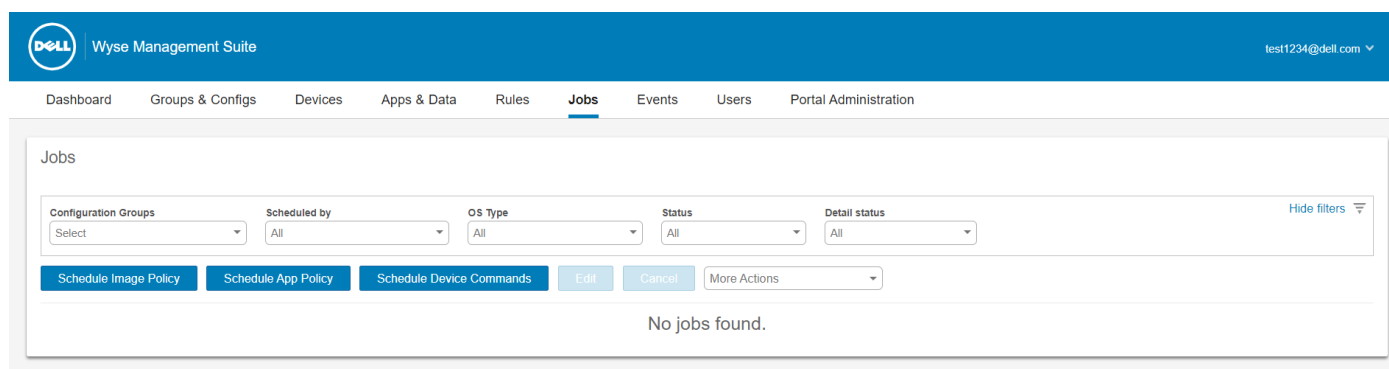


Abbildung 12. Seite „Jobs“

## Themen:

- BIOS-Administratorkennwort synchronisieren
- Suchen eines geplanten Jobs mithilfe von Filtern
- Planen des Gerätebefehlsjobs
- Planen der Abbildrichtlinie
- Planen einer Anwendungsrichtlinie

# BIOS-Administratorkennwort synchronisieren

## Schritte

1. Klicken Sie auf **Jobs**.  
Die Seite **Jobs** wird angezeigt.
2. Wählen Sie aus dem Dropdownmenü **Weitere Maßnahmen** die Option **BIOS-Administratorkennwort synchronisieren**.  
Das Job-Fenster **BIOS-Administratorkennwort synchronisieren** wird angezeigt.
3. Geben Sie das Kennwort ein. Das Kennwort muss mindestens 4 und maximal 32 Zeichen enthalten.
4. Wählen Sie das Kontrollkästchen **Kennwort anzeigen** zum Anzeigen des Kennworts.
5. Wählen Sie aus dem Dropdownmenü **Betriebssystemtyp** Ihre bevorzugte Option.
6. Wählen Sie aus dem Dropdownmenü **Plattform** Ihre bevorzugte Option.
7. Geben Sie den Job-Namen ein.
8. Wählen Sie aus dem Dropdownmenü **Gruppe** Ihre bevorzugte Option.
9. Wählen Sie das Kontrollkästchen **Alle Untergruppen einschließen**, um Untergruppen einzuschließen.
10. Geben Sie eine Beschreibung in das Feld **Beschreibung** ein.
11. Klicken Sie auf **Vorschau**.

# Suchen eines geplanten Jobs mithilfe von Filtern

In diesem Abschnitt wird beschrieben, wie Sie geplante Jobs in der Managementkonsole suchen und verwalten.

## Schritte

1. Klicken Sie auf **Jobs**.  
Die Seite **Jobs** wird angezeigt.
2. Wählen Sie aus der Dropdownliste **Konfigurationsgruppen** entweder die Standardrichtliniengruppe oder die Gruppen, die durch einen Administrator hinzugefügt wurden.
3. Wählen Sie aus der Dropdownliste **Geplant von** den Planer aus, der die Planungsaktivität ausführt.  
Die verfügbaren Optionen sind:
  - Admin
    - App-Richtlinie
    - Abbildrichtlinie
    - Gerätebefehle
  - System
    - Gruppenkonfiguration veröffentlichen
    - Andere
4. Wählen Sie aus der Dropdownliste **Betriebssystemtyp** das Betriebssystem aus.  
Die verfügbaren Optionen sind:
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse Software Thin Client
  - Teradici – private Cloud

- Dell Hybrid Client
5. Wählen Sie aus der Dropdownliste **Status** den Status des Jobs aus.  
Die verfügbaren Optionen sind:
    - Geplant
    - Wird ausgeführt/In Verarbeitung
    - Abgeschlossen
    - Abgebrochen
    - Fehlgeschlagen
  6. Wählen Sie aus der Dropdownliste **Detailstatus** den Status im Detail aus.  
Die verfügbaren Optionen sind:
    - 1 oder mehr fehlgeschlagen
    - 1 oder mehr ausstehend
    - 1 oder mehr in Verarbeitung
    - 1 oder mehr abgebrochen
    - 1 oder mehr abgeschlossen
  7. Wählen Sie aus dem Dropdownmenü **Weitere Maßnahmen** die Option **BIOS-Administratorkennwort synchronisieren**.  
Das Job-Fenster **BIOS-Administratorkennwort synchronisieren** wird angezeigt. Weitere Informationen finden Sie unter [BIOS-Administratorkennwort synchronisieren](#).

## Planen des Gerätebefehlsjobs

### Schritte

1. Klicken Sie auf der Seite **Jobs** auf **Gerätebefehlsjob planen**.  
Der Bildschirm **Gerätebefehlsjob** wird angezeigt.
2. Wählen Sie einen Befehl aus der Dropdown-Liste **Befehl** aus. Die verfügbaren Optionen sind:
  - Neustart
  - Wake on LAN (Reaktivieren von LAN)
  - Herunterfahren
  - Abfrage

Gerätebefehle sind wiederkehrende Jobs. An ausgewählten Wochentagen und zu einem bestimmten Zeitpunkt werden die Befehle an die ausgewählten Geräte gesendet.
3. Wählen Sie aus der Dropdownliste den Betriebssystemtyp aus.
4. Geben Sie den Job-Namen ein.
5. Wählen Sie einen Gruppennamen aus der Dropdownliste aus.
6. Geben Sie eine Jobbeschreibung ein.
7. Wählen Sie aus der Dropdownliste das Datum oder die Uhrzeit aus.
8. Geben/wählen Sie folgende Informationen ein/aus:
  - **Gültig** – Geben Sie das Start- und Enddatum ein.
  - **Start zwischen** – Geben Sie die Start- und Endzeit ein.
  - **An Tag(en)** – Wählen Sie die Wochentage aus.
9. Klicken Sie auf die Option **Vorschau**, damit Ihnen Einzelheiten des geplanten Jobs angezeigt werden.
10. Klicken Sie auf der nächsten Seite auf die Option **Zeitplan festlegen** zum Einleiten des Jobs.

## Planen der Abbildrichtlinie

Die Abbildrichtlinie ist kein wiederkehrender Job. Jeder Befehl ist spezifisch für ein Gerät.

### Schritte

1. Klicken Sie auf der Seite **Jobs** auf die Option **Abbildrichtlinie planen**.  
Der Bildschirm **Abbild-Uploadjob** wird angezeigt.
2. Wählen Sie eine Richtlinie aus der Dropdownliste aus.

3. Geben Sie eine Jobbeschreibung ein.
4. Wählen Sie aus der Dropdownliste das Datum oder die Uhrzeit aus.
5. Geben/wählen Sie folgende Informationen ein/aus:
  - **Gültig** – Geben Sie das Start- und Enddatum ein.
  - **Start zwischen** – Geben Sie die Start- und Endzeit ein.
  - **An Tag(en)** – Wählen Sie die Wochentage aus.
6. Klicken Sie auf die Option **Vorschau**, damit Ihnen Einzelheiten des geplanten Jobs angezeigt werden.
7. Klicken Sie auf die Option **Zeitplan festlegen** zum Initiieren des Jobs.

## Planen einer Anwendungsrichtlinie

Die Anwendungsrichtlinie ist kein wiederkehrender Job. Jeder Befehl ist spezifisch für ein Gerät.

### Schritte

1. Klicken Sie auf der Seite **Jobs** auf die Option **Anwendungsrichtlinie planen**.  
Der Bildschirm **App-Richtlinienjob** wird angezeigt.
2. Wählen Sie eine Richtlinie aus der Dropdownliste aus.
3. Geben Sie eine Jobbeschreibung ein.
4. Wählen Sie aus der Dropdownliste das Datum oder die Uhrzeit aus.
5. Geben/wählen Sie folgende Informationen ein/aus:
  - **Gültig** – Geben Sie das Start- und Enddatum ein.
  - **Start zwischen** – Geben Sie die Start- und Endzeit ein.
  - **An Tag(en)** – Wählen Sie die Wochentage aus.
6. Klicken Sie auf die Option **Vorschau**, damit Ihnen Einzelheiten des geplanten Jobs angezeigt werden.
7. Klicken Sie auf der nächsten Seite auf die Option **Zeitplan festlegen** zum Einleiten des Jobs.

# Verwalten von Ereignissen

Im Abschnitt **Ereignisse** können Sie alle Ereignisse und Warnungen im Verwaltungssystem mithilfe der Managementkonsole anzeigen. Darüber hinaus enthält er Anweisungen zum Anzeigen der Überprüfungsereignisse und Warnungen zu Systemüberwachungszwecken.

Eine Zusammenfassung der Ereignisse und Warnungen wird zum Abrufen einer einfach zu lesenden täglichen Zusammenfassung der Ereignisse im System verwendet. Das Fenster **Überwachung** bereitet die Informationen in einer typischen Auditprotokollansicht auf. Sie können den Zeitstempel, den Ereignistyp, die Quelle und eine Beschreibung der einzelnen Ereignisse in der Reihenfolge des Auftretens anzeigen.

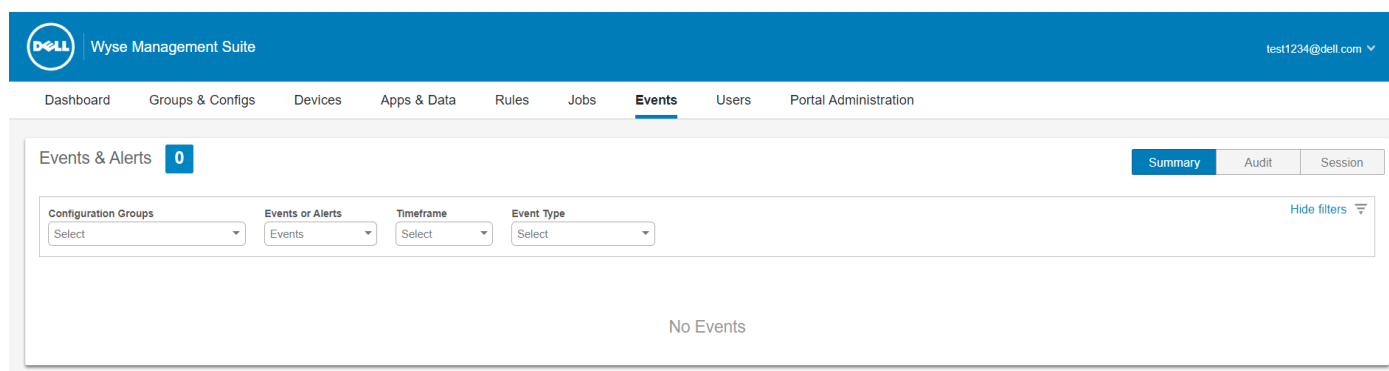


Abbildung 13. Seite „Ereignisse“

## Themen:

- Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern
- Anzeigen einer Zusammenfassung der Ereignisse
- Anzeigen des Überwachungsprotokolls
- Reporting für Endnutzer-Sitzungen

## Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern

### Schritte

1. Klicken Sie auf **Ereignisse**.  
Die Seite **Ereignisse** wird angezeigt.
2. Wählen Sie aus der Dropdownliste **Konfigurationsgruppen** entweder die Standardrichtliniengruppe oder die Gruppen, die durch einen Administrator hinzugefügt wurden.
3. Wählen Sie in der Dropdownliste **Ereignisse oder Warnungen** eine beliebige der folgenden Optionen aus:
  - Ereignisse
  - Aktuelle Warnungen
  - Warnverlauf
4. Wählen Sie von der Dropdownliste **Zeitspanne** eines der folgenden Betriebssysteme aus:  
Diese Option ermöglicht das Anzeigen der Ereignisse innerhalb eines bestimmten Zeitrahmens. Die verfügbaren Optionen im Dropdownmenü sind:
  - Heute
  - Gestern
  - Diese Woche
  - Benutzerdefiniert

- Wählen Sie aus dem Dropdownmenü **Ereignistyp** das Betriebssystem aus.

Alle Ereignisse werden in bestimmte Gruppen klassifiziert. Die verfügbaren Optionen im Dropdownmenü sind:

- Zugriff
- Registrierung
- Konfiguration
- Remote-Befehle
- Verwaltung
- Konformität

## Anzeigen einer Zusammenfassung der Ereignisse


Das Fenster **Ereignisse und Warnungen** zeigt alle Ereignisse und Warnungen an, die im System aufgetreten sind. Gehen Sie zu **Ereignisse > Zusammenfassung**.

## Anzeigen des Überwachungsprotokolls

Das Fenster **Überwachung** bereitet die Informationen in einer typischen Überwachungsprotokollansicht auf. Sie können den Zeitstempel, den Ereignistyp, die Quelle und eine Beschreibung der einzelnen Ereignisse in der Reihenfolge des Auftretens anzeigen.

### Schritte

- Gehen Sie zu **Ereignisse Überprüfung**.
- Wählen Sie aus der Dropdownliste **Konfigurationsgruppen** die Gruppe aus, für die Sie das Überwachungsprotokoll anzeigen möchten.
- Wählen Sie aus der Dropdownliste **Zeitspanne** den Zeitraum, für den Sie die Ereignisse anzeigen lassen wollen.

 **ANMERKUNG:** Die Protokolldateien werden nicht übersetzt und sind nur in englischer Sprache verfügbar.

## Reporting für Endnutzer-Sitzungen

Sie können die Reporting-Option für Endnutzer-Sitzungen verwenden, um die Benutzersitzung in unterschiedlichen Zeitintervallen zu melden.

### Voraussetzungen

Die Option **Sitzungs-Reporting aktivieren** muss aktiviert sein. Weitere Informationen finden Sie unter [Konfigurieren von Wyse Management Suite Clienteinstellungen für Dell Hybrid Client](#).

### Schritte

- Klicken Sie auf **Ereignisse**.  
Die Seite **Ereignisse** wird angezeigt.
- Klicken Sie auf **Sitzung**.  
Daraufhin wird die Seite **Endnutzersitzung** angezeigt.
- Wählen Sie aus dem Drop-Down-Menü **Zeitraumen** eine Option aus, um die Ereignisse anzuzeigen. Die verfügbaren Optionen im Dropdownmenü sind:
  - Heute
  - Gestern
  - Diese Woche
  - Benutzerdefiniert

# Verwalten von Benutzern

In diesem Abschnitt wird die Durchführung routinemäßiger Nutzermanagementaufgaben in der Managementkonsole beschrieben. Es gibt folgende drei Typen von Benutzern:

- **Administratoren** – Dem Wyse Management Suite-Administrator kann die Rolle eines globalen Administrators, Gruppenadministrators oder Betrachters zugewiesen werden.
  - Ein globaler Administrator hat Zugriff auf alle Wyse Management Suite-Funktionen.
  - Ein Gruppenadministrator hat Zugriff auf alle Ressourcen und Funktionen für spezifische Gruppen, die ihm zugewiesen sind.
  - Ein Betrachter hat Nur-Lese-Zugriff auf alle Daten und kann Berechtigungen zugewiesen bekommen, um spezifische Echtzeitbefehle auszuführen, wie z. B. Herunterfahren und Neu starten.

Wenn Sie Administrator auswählen, können Sie eine der folgenden Maßnahmen ausführen:

- Administrator hinzufügen
  - Administrator bearbeiten
  - Administrator(en) aktivieren
  - Administrator(en) deaktivieren
  - Administrator(en) löschen
  - Administrator(en) entsperren
- **Nicht zugewiesene Administratoren** – Benutzer, die vom AD-Server importiert wurden, werden auf der Seite **Nicht zugewiesene Administratoren** angezeigt. Sie können diesen Benutzern zu einem späteren Zeitpunkt im Portal eine Rolle zuweisen.

Für bessere und schnellere Verwaltung von Benutzern, wählen Sie die Benutzer Ihrer Wahl auf der Grundlage der verfügbaren Filteroptionen. Wenn Sie **Nicht verwaltete Benutzer** auswählen, können Sie eine der folgenden Maßnahmen ausführen:

- Benutzer hinzufügen
  - Benutzer bearbeiten
  - Benutzer aktivieren
  - Benutzer deaktivieren
  - Benutzer löschen
- **Endnutzer** – Sie können mithilfe der Registerkarte **Endnutzer** einzelne Benutzer zu Wyse Management Suite hinzufügen. Sie können Einstellungen für einen einzelnen Nutzer konfigurieren und bereitstellen. Die Einstellungen werden auf das Nutzerkonto angewendet und auf den Thin Client angewendet, wenn sich der Nutzer anmeldet. Diese Option wird nur für Thin Clients unterstützt, auf denen ThinOS 9.x als Betriebssystem und Dell Hybrid Clients ausgeführt werden.

**ANMERKUNG:** Sie können nur aus der .CSV Datei Benutzer mit einem Massenimport importieren. Sie können Massenimport von Endnutzern nicht von einem Active Directory aus durchführen.

The screenshot shows the 'Users' management interface in the Wyse Management Suite. The top navigation bar includes 'Dashboard', 'Groups & Configs', 'Devices', 'Apps & Data', 'Rules', 'Jobs', 'Events', 'Users' (selected), and 'Portal Administration'. The main content area is titled 'Users — Unassigned Admins / Cloud Connect Users' and displays a table with the following data:

Type	Name	Group	Created	Active
Administrator(s)	<input type="checkbox"/>			
Unassigned Admins / Cloud Connect Users	<input type="checkbox"/>	Default Device Policy Group	07/09/20	Yes
End Users	<input type="checkbox"/>			

Abbildung 14. Seite „Benutzer“

## Themen:

- [Hinzufügen eines neuen Administratorprofils](#)

- Erstellen einer benutzerdefinierten WMS-Rolle in Wyse Management Suite
- Massenimport nicht zugewiesener Administratoren oder Cloud Connect-Nutzer
- Bearbeiten eines Administratorprofils
- Aktivieren eines Administratorprofils
- Deaktivieren eines Administratorprofils
- Löschen eines Administratorprofils
- Entsperren eines Administratorprofils
- Deaktivieren eines Administratorprofils
- Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte
- Hinzufügen eines Endnutzers
- Bearbeiten eines Endnutzers
- Konfigurieren der Benutzerrichtlinie
- Massenimport von Endnutzern
- Endnutzer löschen
- Bearbeiten eines Nutzerprofils

## Hinzufügen eines neuen Administratorprofils

### Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Administrator(en)**.
3. Klicken Sie auf **Administrator hinzufügen**.  
Das Fenster **Neuer Administrator-Benutzer** wird angezeigt.
4. Geben Sie Ihre E-Mail-ID und den Nutzernamen in die entsprechenden Felder ein.
5. Wählen Sie das Kontrollkästchen zur Verwendung des gleichen Nutzernamens, der in der E-Mail genannt wird.
6. Führen Sie eine der folgenden Aktionen aus:
  - Wenn Sie auf die Registerkarte **Personenbezogene Daten** klicken, geben Sie die folgenden Details ein:
    - Vorname
    - Nachname
    - Titel
    - Mobiltelefonnummer
  - Wenn Sie auf die Registerkarte **Rollen** klicken, geben Sie die folgenden Details ein:
    - a. Wählen Sie im Abschnitt **Rollen** aus der Dropdown-Liste **Rolle** die Option **Administratorrolle**.
      - Globaler Administrator
      - Gruppenadministrator
      - Viewer

**i ANMERKUNG:** Wenn Sie die **Administratorrolle** als **Betrachter** festlegen, werden die folgenden administrativen Aufgaben angezeigt:

    - Gerät abfragen
    - Registrierung des Geräts aufheben
    - Gerät neu starten/herunterfahren
    - Gruppenzuweisung ändern
    - Remote-Spiegelung
    - Gerät sperren
    - Gerät löschen
    - Nachricht senden
    - WOL-Gerät
  - b. Geben Sie im Abschnitt **Kennwort** das benutzerdefinierte Kennwort ein. Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche **Zufälliges Kennwort generieren**.
7. Klicken Sie auf **Speichern**.

# Erstellen einer benutzerdefinierten WMS-Rolle in Wyse Management Suite

Mit Wyse Management Suite 3.1 oder neueren Versionen kann ein globaler Administrator eine neue Administratorrolle erstellen und granulare Berechtigungen für verschiedene Funktionen von Wyse Management Suite bereitstellen. Sie können mehrere Benutzer mit der benutzerdefinierten globalen Administratorrolle erstellen.

## Schritte

1. Rufen Sie die Registerkarte **Benutzer** auf.
2. Klicken Sie auf **Administrator(en)**.
3. Klicken Sie auf **Administrator hinzufügen**.  
Das Fenster **Neuer Administrator-Benutzer** wird angezeigt.
4. Geben Sie Ihre E-Mail-ID und den Nutzernamen in die entsprechenden Felder ein.
5. Klicken Sie auf **Rollen**.
6. Wählen Sie aus der Dropdown-Liste **Rollebenutzerdefinierte WMS-Rolle** aus.
7. Wählen Sie unter jeder Kategorie die entsprechende Funktion aus, die der Benutzer durchführen darf.
8. Klicken Sie auf **Speichern**.

Die folgende Tabelle enthält Details zu den unterstützten und nicht unterstützten Berechtigungen, die einer benutzerdefinierten Rolle zugewiesen werden können:

**Tabelle 8. Berechtigungen für eine benutzerdefinierte Rolle**

Unterstützt	Nicht unterstützt
Konfiguration bearbeiten oder entfernen	Massenspeichergeräte-Ausnahme
Gruppen hinzufügen, bearbeiten und löschen	Erstellen des Gruppenadministrators
Referenzdateien hochladen	Erstellen des globalen Administrators
Gerätedetail-Ausnahme erstellen	Erstellung des Viewer-Administrators
Regeln	Zuweisen von Rollen zu nicht zugewiesenen Administratoren
Anwendungen und Daten	Abonnement (Lizenz exportieren und importieren)
Massenimport von Endnutzern	Ändern der WMS-Server-URL
Remote-Repository verwalten	Ändern der MQTT-URL
Berichte	Hochladen der Konfigurationsbenutzeroberfläche
Andere	Benutzerdefiniertes Branding
Active Directory auf der Portaladministrator-Seite	

# Massenimport nicht zugewiesener Administratoren oder Cloud Connect-Nutzer


## Schritte

1. Klicken Sie auf **Benutzer**.  
Die Seite **Benutzer** wird angezeigt.
2. Wählen Sie die Option **Nicht zugewiesenen Administratoren**.
3. Klicken Sie auf **Massenimport**.  
Das Fenster **Massenimport** wird angezeigt.
4. Klicken Sie auf **Durchsuchen** und wählen Sie die CSV-Datei aus.
5. Wählen Sie die Nutzergruppe aus, der die importierten Nutzer zugewiesen werden sollen.

6. Klicken Sie auf **Importieren**.

## Bearbeiten eines Administratorprofils

### Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Administrator(en)**.
3. Klicken Sie auf **Administrator bearbeiten**.  
Das Fenster **Administratorbenutzer bearbeiten** wird angezeigt.
4. Geben Sie Ihre E-Mail-ID und den Nutzernamen in die entsprechenden Felder ein.  
 **ANMERKUNG:** Beim Aktualisieren des Anmeldenamens, sind Sie gezwungen, sich von der Konsole abzumelden. Melden Sie sich bei der Konsole unter Verwendung des aktualisierten Konto-Anmeldenamens an.
5. Führen Sie eine der folgenden Aktionen aus:
  - Wenn Sie auf die Registerkarte **Personenbezogene Daten** klicken, geben Sie die folgenden Details ein:
    - Vorname
    - Nachname
    - Titel
    - Mobiltelefonnummer
  - Wenn Sie auf die Registerkarte **Rollen** klicken, geben Sie die folgenden Details ein:
    - a. Wählen Sie im Abschnitt **Rollen** aus der Dropdown-Liste **Rolle** die Option **Administratorrolle**.
    - b. Geben Sie im Abschnitt **Kennwort** das benutzerdefinierte Kennwort ein. Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche **Zufälliges Kennwort generieren**.
6. Klicken Sie auf **Speichern**.

## Aktivieren eines Administratorprofils

### Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Administrator(en)**.
3. Wählen Sie das Gerät aus, das Sie aktivieren möchten.
4. Klicken Sie auf **Admin aktivieren**.

## Deaktivieren eines Administratorprofils

Die Deaktivierung des Administratorprofils verhindert, dass Sie sich bei der Konsole anmelden können und entfernt Ihr Konto von der Liste der registrierten Geräte.

### Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Administrator(en)**.
3. Wählen Sie in der Liste einen Benutzer aus und klicken Sie auf **Administrator(en) deaktivieren**.  
Es wird ein Benachrichtigungsfenster angezeigt.
4. Klicken Sie auf **OK**.

# Löschen eines Administratorprofils

## Info über diese Aufgabe

Administratoren müssen deaktiviert werden, bevor Sie sie löschen können. Gehen Sie beim Löschen von Administratoren folgendermaßen vor:

### Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Administrator(en)**.
3. Aktivieren Sie das Kontrollkästchen neben dem/den Administrator/en, den/die Sie löschen möchten.
4. Klicken Sie auf **Administrator(en) löschen**.  
Es wird ein Fenster mit einer **Warnung** angezeigt.
5. Geben Sie einen Grund für den Löschvorgang ein, um die Verknüpfung **Löschen** zu aktivieren.
6. Klicken Sie auf **Löschen**.

# Entsperren eines Administratorprofils

## Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Administrator(en)**.
3. Wählen Sie die Administratoren aus, die Sie entsperren möchten.
4. Klicken Sie auf **Administrator(en) entsperren**.

# Deaktivieren eines Administratorprofils

## Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Administrator(en)**.
3. Wählen Sie die Administratoren aus, die Sie deaktivieren möchten.
4. Klicken Sie auf **Administrator(en) deaktivieren**.

# Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte

## Schritte

1. Klicken Sie auf die Registerkarte **Regeln**.
2. Wählen Sie die Option **Automatische Zuweisung nicht verwalteter Geräte**.
3. Klicken Sie auf die Registerkarte **Regeln hinzufügen**.
4. Geben Sie den **Namen** ein und wählen Sie die **Zielgruppe**.
5. Klicken Sie auf die Option **Bedingung hinzufügen** und wählen Sie die Bedingungen für zugewiesene Regeln.
6. Klicken Sie auf **Speichern**.

Die Regel wird in der Liste der nicht verwalteten Gruppe angezeigt. Diese Regel wird automatisch angewendet und das Gerät in der Zielgruppe aufgeführt.

# Hinzufügen eines Endnutzers

## Schritte

1. Klicken Sie auf die Registerkarte **Benutzer**.
2. Klicken Sie auf **Endnutzer**.
3. Klicken Sie auf **Benutzer hinzufügen**.
4. Geben Sie den Nutzernamen, die Domain, den Vornamen, den Nachnamen, die E-Mail-Adresse, den Titel und die Telefonnummer ein.
5. Klicken Sie auf **Speichern**.

# Bearbeiten eines Endnutzers

## Schritte

1. Klicken Sie auf die Registerkarte **Benutzer**.
2. Klicken Sie auf **Endnutzer**.
3. Klicken Sie auf **Nutzer bearbeiten**.
4. Geben Sie Ihre E-Mail-ID und den Benutzernamen in die entsprechenden Felder ein.
5. Klicken Sie auf **Speichern**.

# Konfigurieren der Benutzerrichtlinie

Sie können Einstellungen für einen einzelnen Nutzer konfigurieren und bereitstellen. Die Einstellungen werden auf das Nutzerkonto angewendet und auf den Thin Client angewendet, wenn sich der Nutzer anmeldet. Diese Option wird nur für Thin Clients unterstützt, auf denen ThinOS 9.x als Betriebssystem und Dell Hybrid Clients ausgeführt werden.

## Schritte

1. Klicken Sie auf die Registerkarte **Benutzer**.
2. Klicken Sie auf **Endnutzer**.
3. Wählen Sie einen Nutzer aus.  
Daraufhin wird die Seite **Endnutzerdetails** angezeigt.
4. Wählen Sie aus dem Dropdownmenü **Richtlinien bearbeiten** das Betriebssystem aus.
5. Konfigurieren Sie die erforderlichen Richtlinien und klicken Sie auf **Speichern und veröffentlichen**.



**ANMERKUNG:** Die Anzahl der Nutzer in einer On-Premise-Umgebung ist unbegrenzt. Sie können 10.000 Nutzer zu einer öffentlichen Cloud hinzufügen.


# Massenimport von Endnutzern

## Schritte

1. Klicken Sie auf die Registerkarte **Benutzer**.
2. Klicken Sie auf **Endnutzer**.
3. Klicken Sie auf **Massenimport**.
4. Klicken Sie auf **Durchsuchen** und wählen Sie die .csv-Datei aus.
5. Wählen Sie die Option **CSV-Datei hat Kopfzeile**, wenn die .csv-Datei eine Kopfzeile enthält.
6. Wählen Sie aus der Drop-Down-Liste **Nutzergruppe auswählen** die Nutzergruppe aus, der Sie die Benutzer hinzufügen möchten.
7. Klicken Sie auf **Importieren**.



**ANMERKUNG:** Sie können pro Datei bis zu 100 Benutzer zur Wyse Management Suite hinzufügen und die Dateigröße der .CSV-Datei darf 150 KB nicht überschreiten.

 **ANMERKUNG:** Sie können maximal 10.000 Benutzer in der öffentlichen Cloud hinzufügen. Es gibt keine Begrenzung für die Anzahl der Benutzer, die in einer privaten Cloud hinzugefügt werden können.


## Endnutzer löschen

### Schritte

1. Klicken Sie auf die Registerkarte **Endnutzer**.
2. Klicken Sie auf **Endnutzer löschen**.  
Es wird ein Fenster mit einer Warnung angezeigt. Geben Sie einen Grund für den Löschvorgang ein, um die Verknüpfung Löschen zu aktivieren.
3. Klicken Sie auf **Löschen**.

## Bearbeiten eines Nutzerprofils

### Schritte

1. Klicken Sie auf **Benutzer**.
2. Klicken Sie auf **Nicht zugewiesene Administratoren**.
3. Klicken Sie auf **Benutzer bearbeiten**.  
Das Fenster **Administratorbenutzer bearbeiten** wird angezeigt.
4. Geben Sie Ihre E-Mail-ID und den Nutzernamen in die entsprechenden Felder ein.  
 **ANMERKUNG:** Beim Aktualisieren des Anmeldenamens, sind Sie gezwungen, sich von der Konsole abzumelden. Melden Sie sich bei der Konsole unter Verwendung des aktualisierten Konto-Anmeldenamens an.
5. Führen Sie eine der folgenden Aktionen aus:
  - Klicken Sie auf die Registerkarte **Personenbezogene Daten** und geben Sie die folgenden Details ein:
    - Vorname
    - Nachname
    - Titel
    - Mobiltelefonnummer
  - Klicken Sie auf die Registerkarte **Rollen** und geben Sie die folgenden Details ein:
    - a. Wählen Sie im Abschnitt **Rollen** aus der Dropdown-Liste **Rolle** die Option **Administratorrolle**.
    - b. Geben Sie im Abschnitt **Kennwort** das benutzerdefinierte Kennwort ein. Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche **Zufälliges Kennwort generieren**.
6. Klicken Sie auf **Speichern**.

# Portalverwaltung

Dieser Abschnitt enthält eine kurze Übersicht über die Systemverwaltungsaufgaben, die erforderlich sind, um das System einzurichten und zu verwalten.

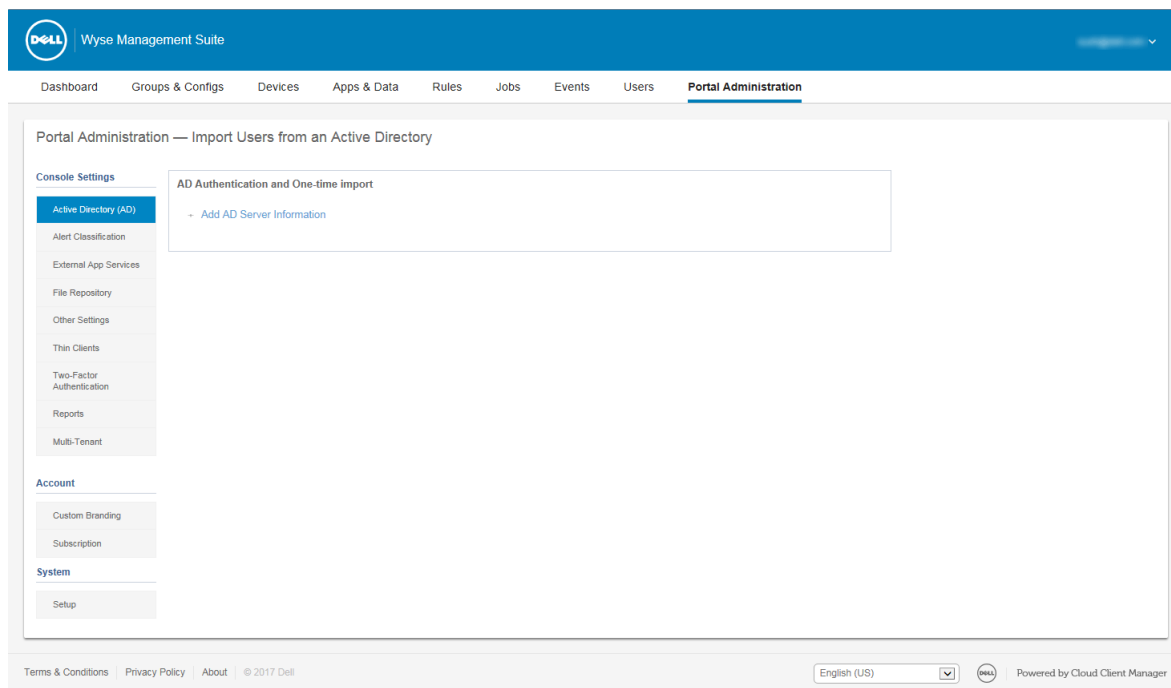


Abbildung 15. Portaladministrator

## Themen:

- Importieren von nicht zugewiesenen Nutzern oder Nutzergruppen in die Public Cloud über Active Directory
- Hinzufügen der Active Directory-Serverinformationen
- Warnungsklassifizierungen
- Erstellen eines API-Kontos (Application Programming Interface)
- Zugreifen auf Wyse Management Suite Datei-Repository
- Andere Einstellungen konfigurieren
- Verwalten von Teradici-Konfigurationen
- Aktivieren der Zwei-Faktor-Authentifizierung
- Aktivieren von Multi-Tenant Konten
- Generieren von Berichten
- Aktivieren von benutzerdefiniertem Branding
- Verwalten des System-Setups

# Importieren von nicht zugewiesenen Nutzern oder Nutzergruppen in die Public Cloud über Active Directory

## Schritte

1. Informationen zum Herunterladen und Installieren des Datei-Repositorys finden Sie unter [Zugriff auf Datei-Repository](#). Das Repository muss unter Verwendung des Firmennetzwerks installiert werden und muss Zugriff auf den AD-Server haben, um Benutzer abzurufen.
2. Registrieren Sie das Repository in der Public Cloud. Nach der Registrierung befolgen Sie die Schritte in der UI zum Importieren der Nutzer in die Public Cloud der Wyse Management Suite. Sie können die Rollen des AD-Nutzers nach dem Import in die Public Cloud der Wyse Management Suite bearbeiten.
3. Richten Sie ADFS in einer Public Cloud ein.

## Hinzufügen der Active Directory-Serverinformationen

Sie können Active Directory-Nutzer in die private Cloud der Wyse Management Suite importieren.

## Schritte

1. Melden Sie an der Private Cloud der Wyse Management Suite an.
2. Gehen Sie zu **Portaladministrator** > **Konsoleneinstellungen** > **Active Directory (AD)**.
3. Klicken Sie auf den Link **AD-Serverinformationen hinzufügen**.
4. Geben Sie die Servereinstellungen, wie z. B. **AD-Servername**, **Domainname**, **Server-URL** und **Port** ein.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Importieren**.
7. Geben Sie den Benutzernamen und das Kennwort ein.



**ANMERKUNG:** Für die Suche nach Gruppen und Benutzern können Sie Filter basierend auf den Optionen **Suchbasis** und **Gruppenname enthält** verwenden. Sie können Sie die Werte wie folgt eingeben:

- OU=<OU Name>, zum Beispiel OU=TestOU
- DC=<Child Domain>, DC=<Parent Domain>, DC=com,, zum Beispiel DC=Skynet, DC=Alpha, DC=Com

Sie können ein Leerzeichen nach einem Komma einfügen, aber keine einfachen oder doppelten Anführungszeichen verwenden.

8. Klicken Sie auf **Anmelden**.
9. Klicken Sie auf der Seite **Benutzergruppe** auf **Gruppenname** und geben Sie den Gruppennamen ein.
10. Im Feld **Suche** geben Sie den Gruppennamen ein, den Sie auswählen möchten.
11. Wählen Sie eine Gruppe aus.  
Die ausgewählte Gruppe wird in den rechten Fensterbereich auf der Seite verschoben.
12. Geben Sie den Nutzernamen in das **Textfeld „Nutzername“** ein.
13. Klicken Sie auf **Nutzer importieren** oder **Gruppen importieren**.



**ANMERKUNG:** Wenn Sie einen ungültigen Namen oder keinen Nachnamen oder eine E-Mail-Adresse als Namen eingeben, können die Einträge nicht in die Wyse Management Suite importiert werden. Diese Einträge werden während des Benutzer-Importvorgangs übersprungen.

Das Wyse Management Suite-Portal zeigt eine Bestätigungsmeldung mit der Anzahl der importierten Active Directory-Benutzer an. Die importierten Active Directory-Benutzer werden unter der **Registerkarte Benutzer Nicht zugewiesene Administratoren**.

14. Zum Zuweisen unterschiedlicher Rollen oder Berechtigungen wählen Sie einen Benutzer aus und klicken Sie auf **Benutzer bearbeiten**.

Nach der Zuweisung der Rollen zum Active Directory-Benutzer, werden sie auf die Registerkarte **Administratoren** auf der Seite **Benutzer** verschoben.

## Nächste Schritte

Active Directory-Benutzer können sich am Verwaltungsportal der Wyse Management Suite mithilfe der Domain-Anmeldeinformationen anmelden. So melden Sie sich am Wyse Management Suite-Portal an:

1. Starten Sie das Wyse Management Suite-Verwaltungsportal.
2. Klicken Sie auf dem Anmeldebildschirm auf den Link **Mit Ihren Domain-Anmeldeinformationen anmelden**.
3. Geben Sie die Domain-Nutzeranmeldedaten ein und klicken Sie auf **Anmelden**.

Um sich mit untergeordneten Domänen-Nutzeranmeldedaten am Wyse Management Suite-Portal anzumelden, gehen Sie wie folgt vor:

1. Starten Sie das Wyse Management Suite-Verwaltungsportal.
2. Klicken Sie auf dem Anmeldebildschirm auf den Link **Mit Ihren Domain-Anmeldeinformationen anmelden**.
3. Klicken Sie auf **Benutzerdomäne ändern**.
4. Geben Sie die Nutzeranmeldedaten und den vollständigen Domännennamen ein.
5. Klicken Sie auf **Anmelden**.

Die importierten Active Directory-Nutzer können auf der Seite **Nutzer** mit der globalen Administratoranmeldung aktiviert oder deaktiviert werden. Wenn Ihr Konto deaktiviert ist, können Sie sich nicht am Wyse Management Suite-Verwaltungsportal anmelden.

**i ANMERKUNG:** So importieren Sie die Benutzer mithilfe des LDAPS-Protokolls:

1. Importieren Sie das AD-Domänen-Server-Stammzertifikat mit dem Schlüssel-Tool manuell in den Java-Schlüsselspeicher. Zum Beispiel: `<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe -importcert -alias "WIN-0358EA52H8H" -keystore "<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\lib\security\cacerts>" -storepass changeit -file "Root Certificate Path"`
2. Starten Sie den Tomcat-Dienst neu.

## Funktion "Active Directory-Verbunddienste" in einer Public Cloud konfigurieren

Sie können Active Directory-Verbunddienste in einer Public Cloud konfigurieren

### Schritte

1. Klicken Sie auf der Seite **Portaladministrator** unter **Konsoleneinstellungen** auf **Active Directory (AD)**.
2. Geben Sie die Einzelheiten der Wyse Management Suite unter ADFS ein. Um die Standortdetails des ADFS-Servers zu erfahren, auf den Sie die .xml-Dateien der Wyse Management Suite hochladen müssen, fahren Sie mit dem Mauszeiger über das **Informationssymbol (i)**.

**i ANMERKUNG:** Klicken Sie zum Herunterladen der .xml-Datei für die Wyse Management Suite auf den Downloadlink.

3. Legen Sie die Wyse Management Suite-Regeln für ADFS fest. Um die Einzelheiten der benutzerdefinierten Anspruchsregel zu erfahren, fahren Sie mit der Maus über das **Informationssymbol (i)**.

**i ANMERKUNG:** Zum Anzeigen der Wyse Management-Richtlinien klicken Sie auf den Link **WMS-Regeln anzeigen**. Sie können auch die Wyse Management Suite-Regeln durch Klicken auf den Link im Fenster **Wyse Management Suite-Regeln** herunterladen.

4. Zum Konfigurieren der ADFS-Einzelheiten klicken Sie auf **Konfiguration hinzufügen** und führen Sie die folgenden Schritte aus:

**i ANMERKUNG:** Damit Mandanten die ADFS-Konfiguration befolgen, laden Sie die ADFS-Metadatendatei hoch.

- a. Klicken Sie zum Hochladen der auf Ihrem Thin Client gespeicherten .XML-Datei auf **XML-Datei laden**. Die Datei finden Sie unter `https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml`.
- b. Geben Sie die Einzelheiten der Instanz-ID und des X.509-Signierungszertifikat in die entsprechenden Felder ein.
- c. Geben Sie die ADFS-Anmelde-URL-Adresse und die ADFS-Abmelde-URL-Adresse in die entsprechenden Felder ein.
- d. Damit Mandanten das "Einmalige Anmelden" mithilfe von ADFS konfigurieren können, wählen Sie das Kontrollkästchen **SSO-Anmeldung mit ADFS aktivieren**. Diese Funktion folgt der SAML-Standardspezifikation (Security Assertion and Markup Language).

- e. Zum Validieren der Konfigurationsinformationen klicken Sie auf **ADFS-Anmeldung testen**. Dies ermöglicht Mandanten das Testen ihres Setups vor dem Speichern.

**ANMERKUNG:** Mandanten können die SSO-Anmeldung unter Verwendung von ADFS aktivieren/deaktivieren.

5. Klicken Sie auf **Speichern**.

6. Nach dem Speichern der Metadatenfile klicken Sie auf **Konfiguration aktualisieren**.

**ANMERKUNG:** Mandanten können sich durch die Verwendung ihrer AD-Anmeldeinformationen, die in ihren ADFS konfiguriert sind, an- und abmelden. Sie müssen sicherstellen, dass die AD-Benutzer auf den Wyse Management Suite-Server importiert wurden. Klicken Sie auf der Anmeldeseite auf **Anmelden** und geben Sie Ihre Domänenanmeldeinformationen ein. Sie müssen die E-Mail-Adresse Ihres AD-Benutzers eingeben und sich anmelden. Um einen Nutzer in die Public Cloud zu importieren, muss ein Remote-Repository installiert sein. Weitere Informationen zur ADFS Dokumentation finden Sie unter [Technet.microsoft.com](https://technet.microsoft.com).

## Ergebnisse

Nachdem die ADFS-Testverbindung erfolgreich war, importieren Sie die Benutzer über den im Remote-Repository vorhandenen AD Connector.

# Warnungsklassifizierungen

Die Warnungsseite kategorisiert die Warnungen als **Kritisch**, **Warnung** oder **Info**.

**ANMERKUNG:** Für den Empfang von Warnungen per E-Mail wählen Sie die Option **Warneinstellungen** aus dem Benutzernamenmenü, das in der oberen rechten Ecke angezeigt wird.

Wählen Sie den bevorzugten Benachrichtigungstyp wie z. B. **Kritisch**, **Warnung** oder **Info** für die folgenden Warnungen:

- Warnung über Gerätezustand
- Gerät nicht eingecheckt

# Erstellen eines API-Kontos (Application Programming Interface)

## Info über diese Aufgabe

In diesem Bereich können Sie gesicherte API-Konten (Application Programming Interface) erstellen. Dieser Dienst bietet die Möglichkeit zur Erstellung speziellen Konten. Zum Konfigurieren des externen Anwendungsdiensts führen Sie die folgenden Schritte aus:

## Schritte

1. Melden Sie sich am Wyse Management Suite-Portal an und klicken Sie auf die Registerkarte **Portaladministrator**.
2. Wählen Sie **Externe App-Dienste** unter **Konsoleneinstellungen**.
3. Wählen Sie die Registerkarte **Hinzufügen**, um einen API-Dienst hinzuzufügen. Das Dialogfeld **Externen App-Dienst hinzufügen** wird angezeigt.
4. Geben Sie die folgenden Details zum Hinzufügen eines externen Anwendungsdiensts ein.
  - Name
  - Beschreibung
5. Aktivieren Sie das Kontrollkästchen **Automatisch zulassen**.  
Wenn Sie das Kontrollkästchen auswählen, ist die Genehmigung der globalen Administratoren nicht erforderlich.
6. Klicken Sie auf **Speichern**.

# Zugreifen auf Wyse Management Suite Datei-Repository

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

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

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

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

Die Image `pull`-Vorlagen werden nicht automatisch in anderen Repositorys 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 Public-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 Public Cloud der Wyse Management Suite registrieren.
5. Klicken Sie auf die Option **Dateien synchronisieren** zum Senden des Dateisynchronisierungsbefehls.
6. Klicken Sie auf **Check in** und klicken Sie dann auf **Befehl senden**, um den Geräteinformationsbefehl an das Gerät zu senden.
7. Klicken Sie auf die Option **Registrierung aufheben**, um die Registrierung am vor Ort-Dienst aufzuheben.
8. Klicken Sie auf **Bearbeiten**, um die Datei zu bearbeiten.
9. Wählen Sie aus der 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 Public Cloud.  
**i 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**.

## Subnetz-Zuordnung

In der Wyse Management Suite 2.0 können Sie ein Subnetz einem Datei-Repository zuweisen. Sie können ein Datei-Repository mit bis zu 25 Subnetzen oder Bereichen verknüpfen. Sie können auch die mit dem Repository verknüpften Subnetze priorisieren.

Sie können die BIOS-Pakete mithilfe der Subnetzzuordnung der Wyse Management Suite 2.1 bereitstellen. Sie können mehrere Firmware-Pakete aus dem Remote-Repository, dem Mandanten-Cloud-Repository oder dem Operator-Cloud-Repository hochladen und bereitstellen. Diese Funktion gilt nur für die Pro-Lizenz der Wyse Management Suite.

**ANMERKUNG:** Die Subnetz-Annäherung wird für ThinOS-9.x-Geräte nicht unterstützt.

## Konfigurieren der Subnetz-Zuordnung

### Schritte

1. Gehen Sie zu **Portalverwaltung > Datei-Repository**.

Portal Administration — File Repositories

Console Settings | User instructions

Active Directory (AD) | Download version 3.0.0

Alert Classification | Automatic Replication

Edge Gateway & Embedded PC Registration

External App Services

**File Repository**

Other Settings

Thin Clients

Two-Factor Authentication

Reports

Account

Custom Branding

Subscription

Sync Files | Check-In | Unregister | Edit | Delete | **App Filter Mapping** | Subnet Mapping

<input type="checkbox"/>	Active	Name/URL	Last Check-in	Version	Files	Notes	Others
<input type="checkbox"/>	<input checked="" type="checkbox"/>	WMS Repo - WIN-I4S2SLMCJUA	23 days ago	3.1.0	44		Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Subnets:
<input type="checkbox"/>	<input checked="" type="checkbox"/>	WMS Repo - ADServer1	20 days ago	3.0.0	48		Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Subnets:
<input type="checkbox"/>	<input checked="" type="checkbox"/>	WMS Repo - S-SERVER	21 days ago	3.0.0	45		Concurrent File Downloads: 5 Wake on LAN: Yes Fast File Upload & Download (HTTP): No Certificate Validation: No Subnets:

Abbildung 16. Datei-Repository

2. Wählen Sie ein Datei-Repository aus.
3. Klicken Sie auf die Option **Subnetz-Zuordnung**.
4. Geben Sie Subnetze oder Bereiche ein, pro Linie einen Wert. Sie müssen Bindestrich für die Bereichstrennung verwenden.
5. Deaktivieren Sie optional das Kontrollkästchen **Geräten erlauben aus Subnetzen, die diesem Datei-Repository nicht zugeordnet sind, Dateien aus diesem Repository als Fallback-Methode unter Verwendung der Subnetznähe herunterzuladen**, wenn Sie möchten, dass auf das Datei-Repository nur über die konfigurierten Subnetze oder Bereiche zugegriffen wird.

**ANMERKUNG:** Das Kontrollkästchen **Geräten erlauben aus Subnetzen, die diesem Datei-Repository nicht zugeordnet sind, Dateien aus diesem Repository als Fallback-Methode unter Verwendung der Subnetznähe herunterzuladen** ist standardmäßig ausgewählt. Diese Funktion wird auf Geräten mit Thin-OS 9.x nicht unterstützt.

## Andere Einstellungen konfigurieren

Sie können die folgenden Einstellungen verwenden, um **APNS-Warnungen**, **Lizenzablaufwarnungen** und andere **Rechtsgültige Verträge für Self-Service** durchzusetzen.

- **Lizenzablaufwarnung auf Dashboardseite verwerfen** – Markieren Sie dieses Kontrollkästchen zum Deaktivieren der Anzeige der Lizenzablaufwarnung auf der Seite **Dashboard**.
- **Optionen für Advanced Dell Wyse Cloud Connect auf Seite zur Konfiguration der Android Einstellungsrichtlinie aktivieren (Hinweis: nur professionelle Ebene)** – Wählen Sie diese Option zum Aktivieren der erweiterten Dell Wyse Cloud Connect-Optionen auf der Richtlinienkonfigurationsseite für Android-Einstellungen.
- **Taktintervall** – Geben Sie die Zeit ein. Das Gerät sendet alle 60 bis 360 Minuten ein Taktsignal.
- **Check-in-Intervall** – Geben die Zeit ein. Das Gerät sendet ein vollständiges Überprüfungssignal alle 8 bis 24 Stunden.
- **Konformitätswarnung "Nicht eingecheckt"** – Geben Sie die Anzahl an Tagen an, bevor ein Gerät eine **Konformitätswarnung "Nicht eingecheckt"** auslöst. Der Bereich liegt zwischen 1 und 99.

- **Zeitüberschreitung WMS-Konsole:** Geben Sie die Leerlaufzeit in Minuten ein, nach der der Benutzer von der Konsole abgemeldet wird. Diese Einstellung kann von jedem globalen Administrator konfiguriert werden. Der Standardwert beträgt 30 Minuten.
- **Anmeldungsvalidierung** – wenn die **Option zur Anmeldungsvalidierung** aktiviert ist, befinden sich die automatisch ermittelten Geräte auf der Seite **Geräte** im Status **Validierung ausstehend**. Der Mandant kann ein einzelnes Gerät oder mehrere Geräte auf der Seite **Geräte** auswählen und die Registrierung validieren. Die Geräte werden nach deren Validierung in die vorgesehene Gruppe verschoben.

## Verwalten von Teradici-Konfigurationen

Gehen Sie folgendermaßen vor, um einen Teradici-Server hinzuzufügen:

### Schritte

1. Klicken Sie in der Registerkarte **Portalverwaltung** unter **Konsoleneinstellungen** auf **Teradici**.
2. Klicken Sie auf **Add Server** (Server hinzufügen).  
Der Bildschirm **Server hinzufügen** wird angezeigt.
3. Geben Sie den **Servernamen** ein. Die Portnummer wird automatisch ausgefüllt.
4. Wählen Sie das Kontrollkästchen **CA-Validierung** zum Aktivieren der CA-Validierung aus.
5. Klicken Sie auf **Testen**.


## Aktivieren der Zwei-Faktor-Authentifizierung

Sie müssen mindestens zwei aktive globale Administratorbenutzer im System haben.

### Voraussetzungen

Erstellen Sie zwei oder mehrere globale Administratoren vor dem Fortfahren mit der Aufgabe.

### Info über diese Aufgabe

1. Melden Sie sich am Wyse Management Suite-Portal an und klicken Sie auf die Registerkarte **Portaladministrator**.
2. Klicken Sie auf **Zweifaktor-Authentifizierung** unter **Konsoleneinstellungen**.
3. Sie müssen das Kontrollkästchen zum Aktivieren der Zwei-Faktor-Authentifizierung auswählen.  
 **ANMERKUNG:** Administratoren müssen den zweiten Authentifizierungsfaktor über Einmal-Passcodes für die Anmeldung am Management Portal überprüfen.
4. Sie erhalten einen Einmal-Passcode an Ihre E-Mail-Adresse. Geben Sie den Einmal-Passcode ein.

Standardmäßig haben Sie acht Versuche, um den Einmal-Passcode zu verifizieren. Wenn Sie den Passcode nicht verifizieren können, wird das Konto gesperrt. Nur globale Administratoren können gesperrte Konten entsperren.

## Aktivieren von Multi-Tenant Konten

In diesem Abschnitt können Sie Tenant-Konten erstellen, die unabhängig voneinander verwaltet werden können. Sie können die Organisationen unabhängig voneinander verwalten. Jedes Konto muss einen eigenen Lizenzschlüssel haben und kann einen eigenen Satz von Administratorkonten, Richtlinien, Betriebssystemabbildern, Anwendungen, Regeln, Warnmeldungen usw. einrichten. Der übergeordnete Operator erstellt diese Organisationen.

Gehen Sie wie folgt vor, um Multi-Tenant Konten zu aktivieren:

1. Melden Sie sich am Wyse Management Suite-Portal an und klicken Sie auf die Registerkarte **Portaladministrator**.
2. Wählen Sie **Multi-Tenant** unter **Konsoleneinstellungen** aus.
3. Wählen Sie das Kontrollkästchen aus, um die Multi-Tenant-Option zu aktivieren.
4. Geben Sie folgende Informationen ein:
  - Benutzername
  - Kennwort
  - Kennwort bestätigen
  - E-Mail

5. Klicken Sie auf **Einstellungen speichern**.

## Generieren von Berichten

Sie können Berichte zu Jobs, Geräten, Gruppen, Ereignissen, Warnmeldungen und Richtlinien herunterladen. Die Berichte können für den Administrator freigegeben werden, wenn Sie Fehler an den Endpunkten beheben möchten.

### Schritte


1. Gehen Sie zu **Portaladministrator > Berichte**.
2. Klicken Sie auf die Option **Bericht generieren**.  
Das Fenster **Bericht generieren** wird angezeigt.
3. Wählen Sie aus der Dropdownliste **Typ** den Berichtstyp aus.
4. Wählen Sie aus der Dropdownliste **Gruppe** die Gruppe aus.
5. Wählen Sie das Trennzeichen aus.
6. Klicken Sie auf **Speichern**.

## Aktivieren von benutzerdefiniertem Branding

### Info über diese Aufgabe

Diese Option ermöglicht das Hinzufügen des Namens Ihres Unternehmens und seines Logos oder seiner Marke. Sie können zum Anpassen des Wyse Management Suite-Portals Ihr eigenes Kopfzeilenlogo und Favicon hochladen, einen Kopfzeilentitel hinzufügen und die Kopfzeilenfarben ändern. Für den Zugriff auf und Eingeben eines benutzerdefinierten Brandings:

### Schritte

1. Gehen Sie zu **Portal-Administrator > Konto > Benutzerdefiniertes Branding**.
2. Klicken Sie auf **Benutzerdefiniertes Branding aktivieren**.
3. Klicken Sie unter **Kopfzeilenlogo** auf **Durchsuchen** und wählen Sie das Kopfzeilenlogobild aus dem Ordner, in dem es gespeichert wurde.  
Die maximale Größe des Kopfzeilenlogos beträgt 500 x 50 Pixel.
4. Geben Sie den Titel unter der Option **Titel** ein.
5. Wählen Sie das Kontrollkästchen **Titel in Browserfenster/-registerkarte anzeigen** zum Anzeigen des Titels im Browser.
6. Geben Sie die Farbcodes für die **Kopfzeilen-Hintergrundfarbe** und die **Kopfzeilen-Textfarbe** an.
7. Klicken Sie auf **Durchsuchen** und wählen Sie das **Favicon** aus.  
Das Favicon wird in der Adresszeile des Browsers neben der Website-URL angezeigt.  
 **ANMERKUNG:** Sie dürfen die Bilder nur als **.ico**-Dateien speichern.
8. Klicken Sie auf **Einstellungen speichern**.

## Verwalten des System-Setups

Sie können die SMTP-Details, Zertifikate, MQTT-Details und externe Wyse Management Suite URL-Details ändern, die während der Installation konfiguriert wurden.

Ab Wyse Management Suite 2.1 wird die **dynamische Schema-Konfiguration** für ThinOS-9.x-Geräte unterstützt, die es Ihnen ermöglicht, die neuesten Konfigurationseinstellungen ohne Änderungen auf der Serverseite zu aktualisieren. In der Public Cloud kann der Wyse Management Suite-Operator die Benutzeroberfläche der 9.x-Konfiguration aktualisieren. Für die Private Cloud– nur pro-Funktion – kann der globale Benutzer eine Aktualisierung der 9.x-Konfigurationsbenutzeroberfläche durchführen. Wenn die Funktion **Multi-Tenant** aktiviert ist, kann der Wyse Management Suite-Operator das neueste Schema aus dem Abschnitt **Administration** hochladen.

### Schritte

1. Melden Sie sich am Wyse Management Suite-Portal an und klicken Sie auf die Registerkarte **Portaladministrator**.
2. Klicken Sie auf **Setup** unter **Systeme**.

3. Wählen Sie das Kontrollkästchen zur Durchführung der Validierung von Serverzertifikaten für jegliche Kommunikation zwischen Geräten und Servern.

4. Geben Sie die folgenden Details im Bereich **SMTP für E-Mail-Warnungen aktualisieren** ein:

- SMTP-Server
- Von Adresse senden
- Benutzername
- Kennwort
- Testadresse

**Aktuelles Zertifikat** – wählen Sie das Kontrollkästchen **Zertifikatsvalidierung** zur Aktivierung der CA-Validierung für die private Cloud aus. Für sämtliche Kommunikation vom Server und Client, einschließlich Dateidownload und BS-Abbilddownload vom lokalen Repository, wird das Zertifikat verwendet.

**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.

5. Wählen Sie die folgenden Optionen aus und geben Sie die Einzelheiten ein:

- **Schlüssel/Zertifikat** – Dateipaar für HTTPS-Schlüssel/-Zertifikat hochladen (nur PEM-Format wird unterstützt).
- **PKCS-12** – HTTPS-PKCS-12 hochladen (pfx, .p12). Ein Apache-Zwischenzertifikat ist für IIS pfx erforderlich.

6. Um die Details für externen MQTT zu aktualisieren, klicken Sie auf die Option **Externen MQTT ändern** und konfigurieren Sie die Informationen.

7. Um die externe URL der Wyse Management Suite zu aktualisieren, klicken Sie auf die Option **Externe WMS-URL ändern** und konfigurieren Sie die Informationen.

**ANMERKUNG:** Um zu den vorherigen Konfigurationen zurückzukehren, klicken Sie auf die Option **Letzte URLs zurücksetzen** und dann auf **Speichern**.

8. Wenn Sie eine Aktualisierung der Benutzeroberfläche der 9.x-Konfiguration durchführen möchten, klicken Sie im Feld **Konfigurations-UI-Paket** auf **Dateien auswählen** und navigieren Sie zu der .zip-Datei.

**ANMERKUNG:** Diese Option ist nicht verfügbar, wenn die **Multi-Tenant**-Funktion aktiviert ist.

9. Klicken Sie auf **Speichern**.

# Konvertieren von Dell Wyse 5070-Geräten und Dell OptiPlex 7070 Ultra in Dell Hybrid-Client

Sie können die Dell Wyse 5070-Geräte, auf denen 10 IoT Enterprise LTSB, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x und ThinOS 8.6 ausgeführt wird, unter Verwendung von Wyse Management Suite Pro 3.1 oder neuerer Versionen in Dell Hybrid Client konvertieren. Sie können auch die Dell OptiPlex 7070 Ultra-Systeme, auf denen Ubuntu 18.04 und Windows 10 ausgeführt wird, mit Wyse Management Suite pro 3.1 oder neueren Versionen in Dell Hybrid Client konvertieren.

## Themen:

- [Dell Wyse 5070-Konvertierung](#)
- [Dell OptiPlex 7070 Ultra-Konvertierung](#)

## Dell Wyse 5070-Konvertierung

### Voraussetzungen

- Wenn das Wyse 5070-Gerät, auf dem entweder Windows 10 oder ThinLinux 2.x ausgeführt wird, nicht über den neuesten Boot Agent verfügt, der gleich oder höher als 4.0.8 ist, laden Sie ihn von der [Dell Support-Website](#) herunter.
- Wenn das Wyse 5070-Gerät, auf dem Thin-8.6\_511 ausgeführt wird, nicht über den neuesten Boot Agent verfügt, der gleich oder höher als 4.0.8 ist, laden Sie ihn von der [Dell Support-Website](#) herunter.
- Wenn Sie Windows 10 IoT Enterprise-Geräte konvertieren möchten, laden Sie das Dell Hybrid Client-Image DHC\_Wyse\_5070\_Conversion\_Merlin\_Image\_xxxx\_32GB.exe von der [Dell Support-Website](#) herunter.
- Wenn Sie ThinLinux 2.x- oder ThinOS 8.6-Geräte konvertieren möchten, laden Sie das Dell Hybrid Client-Image DHC\_Wyse\_5070\_Conversion\_Merlin\_Image\_xxxx\_16GB.exe von der [Dell Support-Website](#) herunter.
- Stellen Sie sicher, dass Sie Wyse Management Suite Pro 3.1 oder höher verwenden.
- Stellen Sie sicher, dass die Anzahl der Hybrid Client-Lizenzen gleich oder höher ist als die Anzahl der Geräte, die in Dell Hybrid Client konvertiert werden müssen. Die Dell Hybrid Client-Lizenzen können in Wyse Management Suite importiert werden.
- Wenn Wyse Management Suite in einer öffentlichen Cloud eingerichtet ist und Sie das Konvertierungs-Image in einer öffentlichen Cloud registrieren möchten, sollte das lokale Repository eingerichtet und lokal konfiguriert werden. Weitere Informationen finden Sie unter [Remote-Repository](#).

### Info über diese Aufgabe

Der Prozess der Konvertierung von Windows 10 IoT Enterprise LTSC, Windows 10 IoT Enterprise LTSC, ThinLinux 2.x und ThinOS 8.6 auf Dell Hybrid Client entfernt die Inhalte und die Partitionsstruktur des vorhandenen Laufwerks. Beim Konvertierungsprozess werden nur die Zertifikate und Einstellungen beibehalten, die für die Registrierung des Geräts bei Wyse Management Suite relevant sind. Alle anderen Daten, Zertifikate und Konfigurationseinstellungen werden nicht beibehalten. Nach der Konvertierung auf Dell Hybrid Client ist es nicht möglich, das Gerät in den ursprünglichen Zustand zurückzusetzen. Sie können das ursprüngliche Betriebssystem jedoch mithilfe der Dell Wyse USB Imaging-Tools von der [Dell Support-Website](#) wiederherstellen. Die vorhandenen Daten und Einstellungen werden nicht wiederhergestellt.

### Schritte

1. Registrieren Sie das Dell Hybrid Client-Image bei Wyse Management Suite. Weitere Informationen zur Registrierung finden Sie unter [Hinzufügen von Hybrid Client-Images zum Repository](#).
  - Wenn die Speichergröße des Geräts mehr als 16 GB beträgt, verwenden Sie DHC\_CONVERSION\_5070.exe.
  - Wenn die Speichergröße des Geräts 16 GB beträgt, verwenden Sie DHC\_CONVERSION\_5070\_16GB.exe.
2. Erstellen Sie die Richtlinie für das Dell Hybrid Client-Image. Weitere Informationen zum Erstellen einer Hybrid Client-Abbildrichtlinie finden Sie unter [Erstellen von Hybrid Client-Abbildrichtlinien](#).
3. Konvertieren Sie das Gerät in Dell Hybrid Client. Details zum Planen eines Images finden Sie unter [Planen der Abbildrichtlinie](#).
  - Das Gerät erhält eine Benachrichtigung zur Image-Aktualisierung. Der Boot Agent lädt das Image aus dem Wyse Management Suite-Repository herunter und installiert das Dell Hybrid Client-Image, indem es intern das Dell Recovery Tool auslöst. Nach Abschluss des Imaging startet das Gerät auf Dell Hybrid Client.

- Der Dell Client-Agent registriert das Gerät als Dell Hybrid Client bei Wyse Management Suite.
- Wyse Management Suite verwaltet das Gerät als Dell Hybrid Client-Gerät.

## Hinzufügen von Dell Hybrid Client-Images zum Repository

### Schritte

1. Kopieren Sie das Dell Hybrid Client-Konvertierungs-Image mithilfe von Wyse Management Suite in den Repository-Speicherort oder in den Betriebssystem-Images-Ordner.

**ANMERKUNG:** Dell Technologies empfiehlt, die Image-Datei auf das lokale System zu kopieren und die Datei dann an den Wyse Management Suite-Repository-Speicherort zu kopieren. Wyse Management Suite extrahiert die Dateien aus dem komprimierten Ordner und lädt die Dateien am Repository-Speicherort oder in den Betriebssystem-Images-Ordner hoch.

Das Abbild wird zum Repository hinzugefügt.

2. Navigieren Sie zu **Apps & Daten** > **BS-Image-Repository** > **Hybrid Client**, um das gespeicherte Image anzuzeigen.

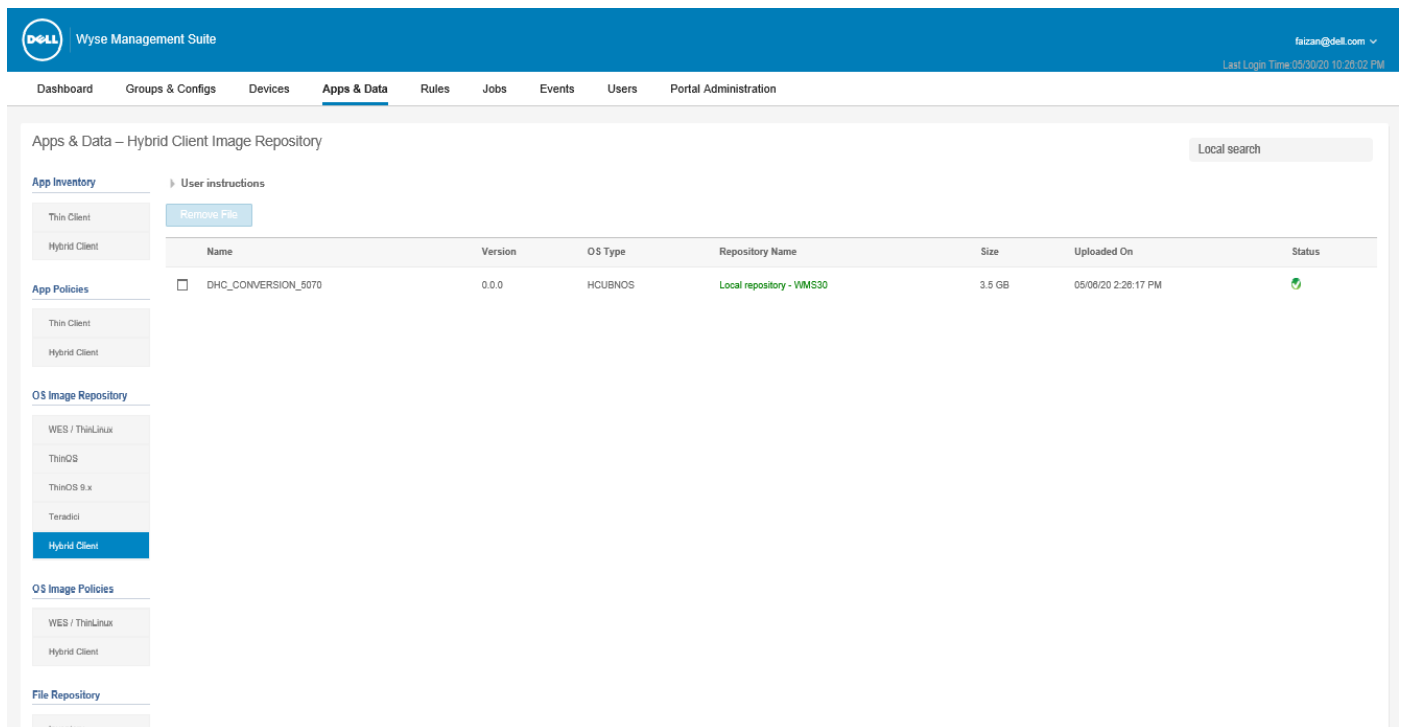


Abbildung 17. Hinzufügen von Dell Hybrid Client-Images zum Repository

## Erstellen von Hybrid Client-Abbildrichtlinien

### Schritte

1. Gehen Sie zu **Apps & Daten** und klicken Sie auf **Hybrid Client** unter **OS-Abbildrichtlinien**.
2. Klicken Sie auf **Richtlinie hinzufügen** und wechseln Sie zur Registerkarte **Hybrid Client-Richtlinie bearbeiten**.
3. Geben Sie den **Richtliniennamen** ein und wählen Sie eine Gruppe aus dem Dropdown-Menü der Registerkarte **Gruppe** aus.
4. Wählen Sie den Betriebssystemtyp aus dem Dropdown-Menü der Registerkarte **BS-Typ** aus.
5. Wählen Sie im Dropdown-Menü der Registerkarte **BS-Subtypfilter** einen Betriebssystem-Untertyp Filter aus.

**ANMERKUNG:** Wenn Sie ein Abbild auf einem bestimmten Betriebssystem oder einer bestimmten Plattform bereitstellen möchten, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter**.

6. Wählen Sie im Dropdown-Menü der Registerkarte **BS-Image** eine Imagedatei aus.
7. Wählen Sie **Diese Version erzwingen** aus dem Dropdown-Menü der Registerkarte **Regel** aus.

8. Wählen Sie eine der folgenden Optionen aus dem Dropdown-Menü der Registerkarte **Richtlinien automatisch anwenden** aus:
  - **Nicht automatisch anwenden** – Die Abbildrichtlinie wird nicht automatisch auf ein Gerät angewendet, das in der Wyse Management Suite registriert ist.
  - **Richtlinie auf neue Geräte anwenden** – Die Abbildrichtlinie wird auf ein neues Gerät bei der Registrierung in der Wyse Management Suite angewendet.
9. Klicken Sie auf **Speichern**.

Abbildung 18. Erstellen von Hybrid Client-Abbildrichtlinien

## Planen der Abbildrichtlinie

### Schritte

1. Wechseln Sie zu **Jobs** und klicken Sie auf die Registerkarte **Abbildrichtlinie planen**. Der Bildschirm **Image-Aktualisierungsjob** wird angezeigt.
2. Wählen Sie eine Richtlinie aus dem Dropdown-Menü der Registerkarte **Richtlinie** aus.
3. Geben Sie die Jobbeschreibung auf der Registerkarte **Beschreibung** ein.
4. Wählen Sie in der Dropdown-Liste der Registerkarte **Ausführen** das Folgende aus:
  - **Gültig** – Geben Sie das Start- und Enddatum ein.
  - **Start zwischen** – Geben Sie die Start- und Endzeit ein.
  - **An Tag(en)** – Wählen Sie die Wochentage aus.
5. Klicken Sie auf **Vorschau**, damit Ihnen Einzelheiten des geplanten Jobs angezeigt werden.
6. Klicken Sie auf **Zeitplan festlegen** zum Initiieren des Jobs.

Abbildung 19. Einen Job planen


# Dell OptiPlex 7070 Ultra-Konvertierung

## Voraussetzungen

- Die DCA Enabler-Version 1.1 oder 1.0 ist erforderlich, um Ubuntu 18.04 auf Dell OptiPlex 7070 Ultra-Geräten in Dell Hybrid Client zu konvertieren.
- Wenn DCA Enabler-Version 1.0 auf Ihrem Gerät installiert ist, müssen Sie ein Upgrade auf 1.1 durchführen. Zum Upgrade von DCA Enabler müssen Sie das Gerät bei Wyse Management Suite 3.1 registrieren und `DCA_Enabler_Package 1.1.0-17` mithilfe von Wyse Management Suite auf das Gerät übertragen und dann `DCA-Enabler 1.1.0-17` bereitstellen.

## Schritte

1. Registrieren Sie das Gerät bei Wyse Management Suite mithilfe von DCA Enabler 1.1.
2. Erstellen Sie ein neues Image Ihres OptiPlex 7070 Ultra-Geräts – siehe [Erstellen eines neuen Image Ihres Dell Hybrid Client](#). Sie können eine Anwendungsrichtlinie für die Bereitstellung des Dell Hybrid Client-Pakets planen. Weitere Informationen finden Sie unter [Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Dell Hybrid Clients](#)

 **ANMERKUNG:** Um eine Standard-Anwendungsrichtlinie für Dell Hybrid Client-Geräte bereitzustellen, müssen Sie das neueste Dell Hybrid Client 1.1- oder 1.0-Bundle in das lokale oder Remote-Repository hochladen.

# Sicherheitskonfigurationen

In diesem Abschnitt werden die wichtigsten Sicherheitsfunktionen von Wyse Management Suite beschrieben. Außerdem werden die Verfahren beschrieben, die erforderlich sind, um die Datensicherheit und die entsprechende Zugriffskontrolle zu gewährleisten.

## Themen:

- Unterstützung für die Konfiguration von TLS-Versionen im Wyse Management Suite-Installationsprogramm
- Konfigurieren der Funktion Active Directory-Verbunddienste in einer Public Cloud
- Konfigurieren der Secure LDAP- oder LDAPS-Setups
- Veraltetes Protokoll

## Unterstützung für die Konfiguration von TLS-Versionen im Wyse Management Suite-Installationsprogramm

Ab Wyse Management Suite 3.0 ist das lokale Installationsprogramm derart verbessert, dass die TLS-Version (Transport Layer Security) während der Installation oder des Upgrades der Wyse Management Suite ausgewählt werden kann.

**i ANMERKUNG:** Die empfohlene Version von Transport Layer Security ist 1.2. Stellen Sie sicher, dass Sie alle geeigneten Versionen von TLS basierend auf dem Device-Agent und dem Merlin-Image auswählen. Ältere Versionen von Windows Embedded-Systemen, Wyse Device Agent (Versionen unter WDA\_14.4.0.135\_Unified) und 32-Bit-Merlin-Image-Versionen sind nur kompatibel mit TLSv1.0. Auch das Importtool ist nur mit TLSv1.0 kompatibel.

## Konfigurieren der Funktion Active Directory-Verbunddienste in einer Public Cloud

### Voraussetzungen

- Notepad++ oder eine entsprechende Anwendung muss auf dem Server installiert sein.
- ADFS muss auf dem Server installiert sein.

### Schritte

1. Klicken Sie auf der Seite **Portaladministrator** unter **Konsoleneinstellungen** auf **Active Directory (AD)**.
2. Klicken Sie auf **WMS-XML-Datei herunterladen** im Abschnitt **WMS-Details zu ADFS bereitstellen**.  
CCM\_SP\_Metadata.xml Die Datei wird heruntergeladen.
3. Klicken Sie mit der rechten Maustaste auf die heruntergeladene Datei und wählen Sie **Mit Notepad++ bearbeiten** aus.
4. Kopieren Sie den ID-Wert aus der Datei. Beispiel: ccm-sq3.
5. Navigieren Sie zur ADFS-Setup-Konsole.
6. Klicken Sie mit der rechten Maustaste auf **Vertrauensstellungen der vertrauenden Seite** und wählen Sie **Vertrauensstellungen der vertrauenden Seite hinzufügen** aus.  
Das Fenster **Vertrauensstellungen der vertrauenden Seite hinzufügen** wird angezeigt.
7. Klicken Sie auf **Start**.  
Die Seite **Datenquelle auswählen** wird angezeigt.
8. Wählen Sie das Kontrollkästchen **Daten über die vertrauende Seite aus einer Datei importieren** aus und durchsuchen Sie die heruntergeladene CCM\_SP\_Metadata.xml-Datei.
9. Klicken Sie auf **Weiter**.
10. Geben Sie den ID-Wert (CCM-sq3) in das Feld **Anzeigename** ein und klicken Sie auf **Weiter**.
11. Klicken Sie auf der Seite **Zugriffsteuerungsrichtlinie auswählen** auf **Weiter**.

12. Klicken Sie auf der Seite **Bereit zum Hinzufügen der Vertrauensstellung** auf **Weiter**.
13. Klicken Sie auf **Schließen**.  
Die erstellte Vertrauensstellung wird in der Konsole **Vertrauensstellung der vertrauenden Seite** aufgeführt.
14. Melden Sie sich beim öffentlichen Cloud-Server der Wyse Management Suite an.
15. Navigieren Sie zu **Portalverwaltung > Active Directory** und klicken Sie auf **WMS-Regeln anzeigen**.
16. Kopieren Sie den Inhalt, der im Fenster **WMS-Regeln** angezeigt wird.
17. Navigieren Sie zur ADFS-Konsole, klicken Sie mit der rechten Maustaste auf die Vertrauensstellung und wählen Sie **Anspruchsausstellungsrichtlinie bearbeiten**.
18. Klicken Sie auf der Registerkarte **Ausstellungstransformationsregeln** auf **Regel hinzufügen**.
19. Klicken Sie auf **OK**.  
Es wird das Fenster **Regelvorlage auswählen** angezeigt.
20. Wählen Sie aus der Dropdown-Liste **Anspruchsregelvorlage** die Option **Ansprüche mithilfe einer benutzerdefinierten Regel senden** aus und klicken Sie auf **Weiter**.
21. Klicken Sie auf **Regel hinzufügen**.
22. Geben Sie den **Anspruchsregelnamen** ein und fügen Sie den Inhalt, der in Schritt 16 kopiert wurde, in das Feld **Benutzerdefinierte Regel** ein.
23. Klicken Sie auf **Fertigstellen**.
24. Klicken Sie auf **Anwenden** und dann auf **OK**.
25. Navigieren Sie zu **Portalverwaltung > Active Directory** und klicken Sie auf **Konfiguration hinzufügen**.
26. Klicken Sie zum Hochladen der auf Ihrem Thin Client gespeicherten XML-Datei auf **XML-Datei laden**.  
Die Datei steht unter `https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml` zur Verfügung.
27. Klicken Sie auf **Konfiguration aktualisieren**.
28. Damit Mandanten das "Einmalige Anmelden" mithilfe von ADFS konfigurieren können, wählen Sie das Kontrollkästchen **SSO-Anmeldung mit ADFS aktivieren**. Diese Funktion folgt der SAML-Standardspezifikation (Security Assertion Markup Language).
29. Zum Validieren der Konfigurationsinformationen klicken Sie auf **ADFS-Anmeldung testen**. Dies ermöglicht Mandanten das Testen ihres Setups vor dem Speichern.
30. Geben Sie die ADFS-Anmeldedaten ein und klicken Sie auf **Anmelden**.  
Nachdem ADFS konfiguriert wurde, wird die Meldung **Test war erfolgreich** angezeigt.
31. Importieren Sie die AD-Domänenbenutzer aus dem Remote-Repository in die Wyse Management Suite-Public Cloud.
32. Navigieren Sie zur Seite **Benutzer** und weisen Sie den importierten AD-Domänenbenutzern Rollen zu.
33. Gehen Sie zum Wyse Management Suite-Public-Cloud-Portal und klicken Sie auf den Link **Mit Ihren Domain-Anmeldeinformationen anmelden**.
34. Geben Sie die e-Mail-Adresse des importierten AD-Domänenbenutzers ein und klicken Sie auf **Anmelden**.  
Sie werden nach der Anmeldung bei ADFS auf den Wyse Management Suite-Server umgeleitet.

## Konfigurieren der Secure LDAP- oder LDAPS-Setups

Gehen Sie wie folgt vor, um das Stammzertifikat von den Active Directory-Zertifikatdiensten anzufordern und ein sicheres LDAP- oder LDAPS-Setup zu konfigurieren:

### Schritte

1. Navigieren Sie zum Active Directory-Domänenserver.
2. Navigieren Sie zu **Start > Ausführen**.
3. Geben Sie **mmc** ein und klicken Sie auf **OK**.  
Das Fenster **Konsole1** wird angezeigt.
4. Klicken Sie auf **Datei > Snap-Ins hinzufügen oder entfernen**.
5. Fügen Sie die Zertifikate zum lokalen System hinzu und klicken Sie auf **OK**.
6. Blenden Sie den Ordner **Personal** im linken Fensterbereich ein.
7. Klicken Sie mit der rechten Maustaste auf die Zertifikate und gehen Sie zu **Alle Aufgaben > Neues Zertifikat anfordern**.  
Das Fenster **Zertifikatregistrierung** wird angezeigt.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie auf der Registerkarte **Zertifikatregistrierungsrichtlinie auswählen** auf **Weiter**.

10. Wählen Sie den **Domain Controller** aus und klicken Sie auf **Weiter**.  
Das Domänenzertifikat ist auf dem DomainController installiert.
11. Klicken Sie auf **Fertigstellen**.  
Das Zertifikat, das an Ihren Domain-Controller ausgegeben wurde, wird auf Ihrer Zertifikatsseite angezeigt.
12. Klicken Sie mit der rechten Maustaste auf das Zertifikat und exportieren Sie das Zertifikat auf Ihren Desktop.
13. Importieren Sie das AD-Domänenserverzertifikat manuell in den Wyse Management Suite-Java-Schlüsselspeicher auf dem Wyse Management Suite-Server-Setup. Um das Zertifikat zu importieren, gehen Sie wie folgt vor:
  - a. Navigieren Sie zu dem Server, auf dem Wyse Management Suite installiert ist.
  - b. Öffnen Sie die **Eingabeaufforderung** und führen Sie den Befehl `<C:\Program Files\DELL\WMS\jdk-11.0.7\bin>keytool.exe -importcert -alias <certificate name> -keystore "<C:\Program Files\Dell\WMS\jdk-11.0.7\lib\security\cacerts>" -storepass changeit -file "C:\<certificate name> aus.`
14. Starten Sie nach der Installation des Zertifikats den Tomcat-Dienst von Wyse Management Suite neu.
15. Melden Sie sich beim Wyse Management Suite-Server an.
16. Navigieren Sie zu **Portalverwaltung > Active Directory (AD)**.
17. Klicken Sie auf den Link **AD-Serverinformationen hinzufügen**.
18. Geben Sie den AD-Domänennamen ein.
19. Geben Sie die Server-URL als `ldaps://hostname.domain.com` ein. Beispiel: `ldaps://WMS-DC97.WMSAD97.com`.
20. Geben Sie den Portnamen als `636` ein.
21. Klicken Sie auf **Speichern**.
22. Klicken Sie auf **Importieren**.
23. Geben Sie den Nutzernamen und das Kennwort ein.
24. Klicken Sie auf **Anmelden**.
25. Klicken Sie auf der Seite **Nutzergruppe** auf **Gruppenname** und geben Sie den Gruppennamen ein.
26. Im Feld **Suche** geben Sie den Gruppennamen ein, den Sie auswählen möchten.
27. Wählen Sie eine Gruppe aus.  
Die ausgewählte Gruppe wird in den rechten Fensterbereich auf der Seite verschoben.
28. Geben Sie den Nutzernamen in das Feld **Nutzernameninhalte** ein.
29. Klicken Sie auf **Nutzer importieren** oder **Gruppen importieren**.  
Das Wyse Management Suite-Portal zeigt eine Bestätigungsmeldung mit der Anzahl der importierten Active Directory-Benutzer an. Die importierten Active Directory-Benutzer werden auf der Registerkarte **Benutzer > Nicht zugewiesene Administratoren** aufgeführt.

## Veraltetes Protokoll

SMB-Protokollversion (Die Server Message Block) 2.0 ist veraltet.

# Teradici-Geräteverwaltung

Der Abschnitt zur Teradici-Geräteverwaltung enthält Informationen zur Verwaltung und zur Ermittlung von Teradici-Geräten. Die Teradici-Verwaltungskonsole verwendet SDKs zur Unterstützung der Verwaltung und Konfiguration von Tera-Geräten. Dies gilt nur für die private Cloud der Wyse Management Suite mit einer Pro-Lizenz.

## Themen:

- [Ermittlung von Teradici-Geräten](#)
- [CIFS-Anwendungsszenarien](#)

## Ermittlung von Teradici-Geräten

### Vorbedingungen

- Installieren Sie die neueste Version der Wyse Management Suite auf dem Microsoft Windows 2012 Server oder neueren Versionen. Threadx-5.x- und -6.x-Geräte arbeiten mit der neuesten Version des Betriebssystems.
- Installieren und aktivieren Sie die **EMSDK**-Komponente.
- Der FQDN des Wyse Management Suite-Servers muss für **DHCP**- oder **DNS**-Konfigurationen zur Verfügung stehen.
- `cert.pem` muss unter dem Standardpfad `C:\Program Files\Dell\WMS\Teradici\EMSDK` abgelegt sein. Dies dient der Erkennung von Threadx-Geräten.

## Sicherheitsstufe

Abhängig von der konfigurierten Sicherheitsstufe eines Endpunkts müssen Sie für Endpunkte möglicherweise auch ein EBM/EM-Zertifikat bereitstellen.

Endgeräte, die für mittlere oder hohe Sicherheit konfiguriert sind, müssen ein vertrauenswürdigen Zertifikat in ihrem Zertifikatsspeicher haben, bevor sie eine Verbindung zu einem EBM oder EM herstellen können. Für einige Endpunkte können Zertifikate vom Lieferanten als werkseitige Einstellung vorinstalliert werden. Andernfalls können Sie Zertifikate manuell über die AWI eines Endpunkts hochladen.


Endpunkte, die für geringe Sicherheit konfiguriert sind, benötigen kein MC-Zertifikat in ihren vertrauenswürdigen Zertifikatsspeichern, wenn einer der folgenden Punkte zutrifft:

- Sie verwenden DHCP-Erkennung oder DNS-Erkennung und der DHCP- oder DNS-Server hat sie mit dem Fingerabdruck des EBM-Zertifikats versehen.
- Sie werden unter Verwendung der manuellen Ermittlungsmethode erkannt.

**Tabelle 9. Zertifikatsanforderungen für Endpunkte**

Erkennungsmethode	Niedrige Sicherheit	Mittlere Sicherheit	Hohe Sicherheit
DHCP/DNS-Ermittlung ohne Bereitstellung eines EBM-Fingerabdrucks	Zertifikat erforderlich	Zertifikat erforderlich	Nicht zutreffend
DHCP/DNS-Ermittlung mit Bereitstellung eines EBM-Fingerabdrucks	Zertifikat nicht erforderlich	Zertifikat erforderlich	Nicht zutreffend
Ermittlung durch einen Endpunkt ausgelöst, der für eine Hochsicherheitsumgebung konfiguriert ist	Nicht zutreffend	Nicht zutreffend	Zertifikat erforderlich
Manuelle Ermittlung durch den MC initiiert	Zertifikat nicht erforderlich	Nicht zutreffend	Nicht zutreffend

## Manuelle Ermittlung über den Client

1. Gehen Sie zu `https://<clientIP>`.
2. Bestätigen Sie die Zertifikat-Warnmeldung.
3. Geben Sie das Administratorkennwort ein (Standardkennwort lautet „Administrator“) und melden Sie sich an.
4. Gehen Sie zu **Hochladen > Zertifikat**. Wählen Sie die Datei `Cert.pem` aus dem Standardpfad aus und klicken Sie auf **Hochladen**.
5. Gehen Sie zu **Konfiguration > Verwaltung**. Klicken Sie auf die Schaltfläche **Verwaltungsstatus löschen**, um das Gerät beim neuen Verwaltungsserver zu registrieren.
6. Stellen Sie den **Manager-Erkennungsmodus** auf manuell ein
7. Geben Sie die **Endpoint Bootstrap Manager-URL** in folgendem Format ein: **wss://<IP-Adresse des WMS-Servers>**  
 **ANMERKUNG:** Wenn EMSDK mit einem benutzerdefinierten Port installiert ist, geben Sie die **Endpoint Bootstrap Manager-URL** in folgendem Format ein: **wss://<IP-Adresse:benutzerdefinierter Port>**.
8. Klicken Sie auf **Anwenden** und dann auf **Weiter**.
9. Für den **Verwaltungsstatus** wird „Verbunden mit dem Endpunktserver“ angezeigt.

## Hinzufügen der PCoIP-Endpoint-Anbieterklasse zum DHCP-Server


1. Melden Sie sich beim DHCP-Server an.
2. Klicken Sie im Fensterbereich **SERVER** mit der rechten Maustaste auf den DHCP-Server und wählen Sie **DHCP-Manager** aus.
3. Klicken Sie mit der rechten Maustaste auf die Option **IPv4** und wählen Sie dann **Anbieter-Klassen definieren**.
4. Klicken Sie auf **Hinzufügen**, um eine neue DHCP-Anbieterklasse hinzuzufügen.
5. Geben Sie den **PCoIP-Endpoint** in das Feld **Anzeigename** ein.
6. Geben Sie als Hersteller-ID den **PCoIP-Endpoint** in der Spalte **ASCII** ein.
7. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

## Konfigurieren von DHCP-Optionen

1. Klicken Sie mit der rechten Maustaste auf die Option **IPv4** und wählen Sie dann **Vordefinierte Optionen festlegen** aus.
2. Wählen Sie den **PCoIP-Endpoint** als **Options-Klasse** aus und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Optionstyp** den Namen **EBM URI**, den Datentyp **Zeichenfolge**, den Code **10** und die Beschreibung **Endpoint Bootstrap Manager URI** ein und klicken Sie auf **OK**.
4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
5. Erweitern Sie den DHCP-Bereich, auf den Sie die Optionen anwenden möchten.
6. Klicken Sie mit der rechten Maustaste auf **Bereichsoptionen** und wählen Sie anschließend **Optionen konfigurieren** aus.
7. Klicken Sie auf die Registerkarte **Erweitert** und wählen Sie anschließend die Herstellerklasse **PCoIP-Endpoint** aus.
8. Aktivieren Sie das Kontrollkästchen **010 EBM URI** und geben Sie dann eine gültige Verwaltungskonsolen-URI im Feld **Zeichenkette** ein. Klicken Sie auf **Anwenden**. Diese URI erfordert ein gesichertes WebSocket-Präfix, z. B., `wss://<MC IP address>:[port number]. „5172“` ist der Überwachungsport des MC. Die Eingabe dieser Portnummer ist ein optionaler Schritt.
9. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
10. Wählen Sie **PCoIP-Endpoint** als Klasse **Option** aus und klicken Sie auf **Hinzufügen**.
11. Geben Sie im Dialogfeld **Optionstyp** den Namen als **Fingerabdruck EBM X.509 SHA-256**, den Datentyp **Zeichenkette**, den Code **11** und die Beschreibung **Fingerabdruck EBM X.509 SHA-256** ein und klicken Sie dann auf **OK**.
12. Erweitern Sie den DHCP-Bereich, auf den Sie die Optionen anwenden möchten.
13. Klicken Sie mit der rechten Maustaste auf **Bereichsoptionen** und wählen Sie anschließend **Optionen konfigurieren** aus.

14. Klicken Sie auf die Registerkarte **Erweitert** und wählen Sie anschließend die Herstellerklasse **PCoIP-Endpunkt** aus.
15. Aktivieren Sie das Kontrollkästchen **Fingerabdruck 011 EBM X.509 SHA-256** und fügen Sie den SHA-256-Fingerabdruck ein.
16. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
17. Gehen Sie zum Webbrowser des Clients.
18. Gehen Sie zu **Konfiguration > Verwaltung** und legen Sie den **Manager-Erkennungsmodus** auf **Automatisch** fest.
19. Der Client ist mit dem Server verbunden, der auf dem DHCP-Server angegeben ist.

## Erstellen des DNS-SRV-Eintrags

1. Melden Sie sich beim **DNS-Server** an.
  2. Klicken Sie im Fensterbereich **SERVER** mit der rechten Maustaste auf den DNS-Server und wählen Sie **DNS-Manager** aus dem Kontextmenü aus.
  3. Klicken Sie in der Domain mit der rechten Maustaste auf die Option **Forward-Lookupzonen** und wählen Sie **Weitere neue Einträge** aus dem Kontextmenü aus.
  4. Wählen Sie im Dialogfeld **Ressourceneintragstyp** die Option **Dienstidentifizierung (SRV)** aus der Liste aus und klicken Sie auf **Eintrag erstellen**.
  5. Legen Sie den **Service** auf **\_pcoip-bootstrap**, das Protokoll auf **\_tcp** und die **Portnummer** auf **5172** fest, welches der Standard-Überwachungsport des MC ist. Geben Sie unter **Host, der diesen Dienst bietet** die FQDN des MC ein.
-  **ANMERKUNG:** Die FQDN des MC muss eingegeben werden, da die DNS-Spezifikation keine IP-Adressen in den SRV-Einträgen zulässt.
6. Klicken Sie auf **OK**.

## Hinzufügen eines DNS-TXT-Eintrags

1. Klicken Sie in der Domain mit der rechten Maustaste auf die Option **Forward-Lookupzonen** und wählen Sie **Weitere neue Einträge** aus dem Kontextmenü aus.
2. Wählen Sie im Dialogfeld **Ressourceneintragstyp** die Option **Text (TXT)** aus der Liste aus und klicken Sie auf **Eintrag erstellen**.
3. Geben Sie folgende Informationen ein:
  - a. Geben Sie im Feld **Eintragsname** den Hostnamen des Wyse Management Suite-Servers an, der den Dienst anbietet. Das Feld FQDN wird automatisch ausgefüllt. Dies sollte mit der FQDN des Wyse Management Suite-Servers übereinstimmen.
  - b. Geben Sie im Feld **Text** **pcoip-bootstrap-cert=** ein und fügen Sie dann den SHA-256-Fingerabdruck des Wyse Management Suite-Serverzertifikats ein.
4. Klicken Sie auf **OK**.
5. Gehen Sie zum Webbrowser des Clients.
6. Der Client ist mit dem Wyse Management Suite-Server verbunden, der auf dem DHCP-Server angegeben ist.

## Erstellen eines SHA-256-Fingerabdrucks

1. Starten Sie Mozilla Firefox.
2. Navigieren Sie zur Registerkarte **Erweiterte Optionen**.
3. Klicken Sie auf **Zertifikate**, um die Zertifikate anzuzeigen.
4. Klicken Sie unter **Zertifikat-Manager** auf **Zertifizierungsstellen** und klicken Sie auf **Importieren**.
5. Durchsuchen Sie das Zertifikat und klicken Sie auf **Ansicht**.
6. Kopieren Sie den Fingerabdruck **SHA-256**.

# CIFS-Anwendungsszenarien

Die folgenden Anwendungsfälle werden in der Wyse Management Suite unterstützt:

- Wenn Sie **Wyse Management Suite** als **Setup-Typ** während der Installation der privaten Cloud der Wyse Management Suite auswählen.
  - Die Seite „CIFS-Konfiguration“ wird angezeigt. Diese Seite ist erforderlich zum Konfigurieren des freigegebenen Ordners.
    - ⓘ **ANMERKUNG:** Die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** ist standardmäßig deaktiviert.
- Wenn Sie **Teradici EMSDK** als **Setup-Typ** während der Installation der privaten Cloud der Wyse Management Suite auswählen.
  - Als CIFS-Anmeldeinformationen können Sie ein vorhandenes Konto verwenden oder ein neues erstellen.
- Wenn Sie **Wyse Management Suite** und **Teradici EMSDK** als **Setup-Typ** während der Installation der privaten Cloud der Wyse Management Suite auswählen.
  - Die Seite „CIFS-Konfiguration“ wird angezeigt. Diese Seite ist erforderlich zum Konfigurieren des freigegebenen Ordners.
    - ⓘ **ANMERKUNG:** Die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** ist standardmäßig deaktiviert.
  - Als CIFS-Anmeldeinformationen können Sie ein vorhandenes Konto verwenden oder ein neues erstellen.
- Wenn Sie nur EMSDK auf einem System installieren, auf dem bereits der EMSDK-Dienst installiert ist.
  - Wenn Teradici EMSDK ausgewählt ist, wird eine Warnmeldung angezeigt, wenn Sie auf **Weiter** auf der Seite **Setup-Typ** klicken. Die Meldung lautet: **Das Installationsprogramm hat erkannt, dass Teradici EMSDK bereits installiert ist. EMSDK wird bei Bedarf aktualisiert.** Es ist keine Portnummer erforderlich.
    - Wenn die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** ausgewählt ist (standardmäßig)
      1. Halten Sie den Dienst an.
      2. Aktualisieren Sie den EMSDK-Dienst.
      3. Starten Sie den Dienst neu. Er wird unter demselben vorkonfigurierten Benutzer ausgeführt.
    - Wenn die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** mit der Option **Verwenden eines vorhandenen Benutzers** ausgewählt ist.
      1. Halten Sie den Dienst an.
      2. Aktualisieren Sie den EMSDK-Dienst.
      3. Aktualisieren Sie den Benutzer für die Anmeldung beim Dienst auf den ausgewählten Benutzer.
      4. Starten Sie den Dienst neu. Er wird unter demselben vorkonfigurierten Benutzer ausgeführt.
    - Wenn die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** mit der Option **Einen neuen Benutzer erstellen** ausgewählt ist.
      1. Halten Sie den Dienst an.
      2. Aktualisieren Sie den EMSDK-Dienst.
      3. Aktualisieren Sie den Benutzer für die Anmeldung beim Dienst auf den neu erstellten Benutzer.
      4. Starten Sie den Dienst neu. Er wird unter demselben vorkonfigurierten Benutzer ausgeführt.
- Wenn Sie **Wyse Management Suite** und **Teradici EMSDK** auf einem System installieren, auf dem bereits der EMSDK-Dienst installiert ist.
  - Die Vorgehensweise entspricht **Wenn Sie nur EMSDK auf einem System installieren, auf dem bereits der EMSDK-Dienst installiert ist.** mit Ausnahme dessen, dass die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** standardmäßig ausgewählt und ausgegraut ist. Sie müssen CIFS-Anmeldeinformationen eingeben.

# Verwalten des Lizenzabonnements

Dieser Abschnitt ermöglicht Ihnen das Anzeigen und Verwalten des Lizenzabonnements der Verwaltungskonsolle und dessen Verwendung.

Auf der Seite **Portaladministrator** können Sie die Option **Abonnement** anzeigen. Auf dieser Seite werden die folgenden Informationen bereitgestellt:

- Lizenzabonnement
- Lizenzbestellungen
- Lizenznutzung – registrierte Thin Client-Geräte
- Server-Informationen
- Lizenz importieren (private Cloud)
- Lizenz für private Cloud exportieren (öffentliche Cloud)

## Themen:

- [Importieren von Lizenzen von der öffentlichen Cloud-Konsole der Wyse Management Suite](#)
- [Exportieren von Lizenzen in die private Cloud-Konsole der Wyse Management Suite](#)
- [Thin Client-Lizenzzuweisung](#)
- [Lizenzbestellungen](#)

## Importieren von Lizenzen von der öffentlichen Cloud-Konsole der Wyse Management Suite

So importieren Sie Lizenzen von der öffentlichen Cloud-Konsole der Wyse Management Suites in die private Cloud-Konsole der Wyse Management Suite:

### Schritte

1. Melden Sie sich bei der privaten Cloud-Konsole der Wyse Management Suite an.
2. Gehen Sie zu **Portalverwaltung** > **Konten** > **Abonnement**.
3. Geben Sie die Details der öffentlichen Cloud der Wyse Management Suite ein:
  - Nutzernamen
  - Kennwort
  - Rechenzentrum
  - Anzahl an TC-Plätzen
  - Anzahl der Edge Gateway & Embedded PC Plätzen
  - Anzahl der Wyse Software Thin Client Arbeitsplätze
  - Anzahl der Hybrid-Client-Arbeitsplätze
4. Klicken Sie auf **Importieren**.



**ANMERKUNG:** Die private Cloud der Wyse Management Suite muss mit der öffentlichen Cloud der Wyse Management Suite verbunden sein.

## Exportieren von Lizenzen in die private Cloud-Konsole der Wyse Management Suite

So exportieren Sie Lizenzen von der öffentlichen Cloud-Konsole der Wyse Management Suites in die private Cloud-Konsole der Wyse Management Suite:

## Schritte

1. Melden Sie sich bei der öffentlichen Cloud-Konsole der Wyse Management Suite an.
2. Gehen Sie zu **Portalverwaltung > Konten > Abonnement**.
3. Geben Sie die Anzahl der Thin Client Arbeitsplätze ein, die in die private Cloud-Konsole der Wyse Management Suite exportiert werden muss.
4. Klicken Sie auf **Exportieren**.
5. Kopieren Sie den generierten Lizenzschlüssel.
6. Melden Sie sich bei der privaten Cloud-Konsole der Wyse Management Suite an.
7. Gehen Sie zu **Portalverwaltung > Konten > Abonnement**.
8. Geben Sie den erzeugten Lizenzschlüssel in das Textfeld ein.
9. Klicken Sie auf **Importieren**.

# Thin Client-Lizenzzuweisung

Zur Zuweisung der Thin Client-Lizenzen zwischen dem privaten Wyse Management Suite Cloud-Konto und dem öffentlichen Wyse Management Suite Cloud-Konto, gehen Sie wie folgt vor:

## Schritte

1. Melden Sie sich bei der öffentlichen Cloud-Konsole der Wyse Management Suite an.
2. Gehen Sie zu **Portalverwaltung > Konten > Abonnement**.
3. Geben Sie die Anzahl der Thin Client Plätze an.  
 **ANMERKUNG:** Die Thin Client Arbeitsplätze sollten in der öffentlichen Cloud verwaltet werden können. Die eingegebene Anzahl der Thin Client Arbeitsplätze darf nicht höher sein als die in der Option **Verwaltbar** angezeigte Anzahl.
4. Klicken Sie auf **Exportieren**.  
 **ANMERKUNG:** Die Anzahl der öffentlichen Cloud Lizenzen wird basierend auf der Anzahl der in die private Cloud exportierten Thin Client Arbeitsplätze angepasst.
5. Kopieren Sie den generierten Lizenzschlüssel.
6. Melden Sie sich bei der privaten Cloud-Konsole der Wyse Management Suite an.
7. Gehen Sie zu **Portalverwaltung > Konten > Abonnement**.
8. Importieren Sie den exportierten Lizenzschlüssel in die private Cloud.  
 **ANMERKUNG:** Die Lizenz kann nicht importiert werden, wenn sie nicht über ausreichend Thin Client Arbeitsplätze verfügt, um die Anzahl von aktuell verwalteten Geräten in der privaten Cloud zu verwalten. In diesem Fall wiederholen Sie die Schritte 3-8 zur Zuweisung der Thin Client Arbeitsplätze.

# Lizenzbestellungen

In der öffentlichen Cloud zeigt der Bereich **Lizenzbestellungen** die Liste der aufgegebenen Bestellungen, einschließlich der abgelaufenen Lizenzen, an. Standardmäßig werden abgelaufene Bestellungen nicht angezeigt. Aktivieren Sie das Kontrollkästchen **Abgelaufene Bestellungen einschließen**, um die abgelaufenen Bestellungen anzuzeigen. Abgelaufene Bestellungen sind rot gekennzeichnet, Bestellungen, die in 30 Tagen oder weniger ablaufen, sind orange gekennzeichnet.

-  **ANMERKUNG:** Diese Funktion gilt nicht für die Vor-Ort-Bereitstellung, da sie den Bestellverlauf nicht anzeigt. Der Bestellverlauf für Vor-Ort-Lizenzen ist verfügbar, wenn Sie sich im öffentlichen Cloud-Portal als Mandanten-Administrator anmelden.

# Firmware-Upgrade

Sie können Wyse Management Suite verwenden, um die Firmware zu aktualisieren.

## Themen:

- [Aktualisieren von ThinLinux 1.x auf 2.1 und neuere Versionen](#)
- [Aktualisieren von ThinOS 8.x auf 9.0](#)

## Aktualisieren von ThinLinux 1.x auf 2.1 und neuere Versionen



Wenn Sie vor dem Upgrade ein benutzerdefiniertes Abbild von TL 2.x abrufen möchten, müssen Sie das ThinLinux 2.x-Abbild vorbereiten und dann das ThinLinux 1.x-Abbild aktualisieren.

### Vorbereiten des ThinLinux 2.x-Abbilds

#### Voraussetzungen

Verwenden Sie Wyse Management Suite Version 1.4 oder höher, um die ThinLinux-Build-Version 2.0.19 oder 2.1 auf 2.2 zu aktualisieren.

#### Schritte

1. Rufen Sie die Website [www.dell.com/support](http://www.dell.com/support) auf.
2. Klicken Sie auf **Produkt-Support**, geben Sie die **Service-Tag-Nummer** Ihres Thin Clients ein, und drücken Sie dann die **Eingabetaste**.
  -  **ANMERKUNG:** Wenn Sie über keine **Service-Tag-Nummer** verfügen, suchen Sie manuell nach Ihrem Thin Client-Modell.
3. Klicken Sie auf **Treiber und Downloads**.
4. Wählen Sie in der Dropdown-Liste **Betriebssystem** die Option **ThinLinux**.
5. Laden Sie die Add-ons `merlin_nonpxe-4.0.1-0_0.04.amd64.deb` und `wda_3.4.6-05_amd64.tar` herunter.
6. Kopieren Sie das heruntergeladene Add-on zu `<Laufwerk C>/wms/localrepo/repository/thinClientsApps/`.
7. Gehen Sie auf dem Thin Client mit ThinLinux 2.x zu **Einstellungen > Verwaltung > Wyse-Geräte-Agent**.
8. Registrieren Sie das Gerät auf dem Wyse Management Suite-Server.
9. Schließen Sie das Fenster **Einstellungen**.
  -  **ANMERKUNG:** Wenn das Fenster "Einstellungen" nicht geschlossen wird, wird der Fehler **Profil gesperrt** angezeigt, nachdem Sie das Abbild bereitgestellt haben.
10. Melden Sie sich bei der Wyse Management Suite-Konsole an.
11. Erstellen Sie die Anwendungsrichtlinie für die Add-ons `merlin_nonpxe-4.0.1-0_0.04.amd64.deb` und `wda_3.4.6-05_amd64.tar` und stellen Sie sie bereit.
12. Starten Sie den Thin Client neu.
13. Melden Sie sich beim Wyse Management Suite-Server an.
14. Navigieren Sie zur Seite "Gerät" und stellen Sie sicher, dass die Merlin- und WDA-Versionen aktualisiert werden.
15. Klicken Sie auf das registrierte Gerät und navigieren Sie zu **Weitere Maßnahmen > OS-Abbild abrufen**. Das Fenster **OS-Abbild abrufen** wird angezeigt.
16. Geben Sie den Namen des Abbilds ein.
17. Wählen Sie in der Dropdown-Liste "Datei-Repository" das Datei-Repository aus.
18. Wählen Sie die Pull-Operation aus, die Sie durchführen möchten.

- **Standard:** Aktivieren Sie das Kontrollkästchen **OS + Wiederherstellung** und rufen Sie das Abbild ab (komprimiert/unkomprimiert).
- **Erweitert:** Wählen Sie die Vorlage `Compress_OS_Recovery_Commands.xml/uncompress_OS_Recovery_Commands.xml` und rufen Sie das Abbild ab.




## Ergebnisse

### ANMERKUNG:

- Wenn Sie das Remote-Repository der Wyse Management Suite 1.3 verwenden, ist die xml-Datei im Repository nicht verfügbar. Sie müssen die Wyse Management Suite auf Version 1.4 oder höher aktualisieren, um auf die Datei zugreifen zu können.
- Bei der Wiederherstellungs-Pull-Operation werden die Benutzereinstellungen nicht beibehalten.

## ThinLinux 1.x auf 2.x aktualisieren

### Schritte

1. Rufen Sie die Website [www.dell.com/support](http://www.dell.com/support) auf.
2. Klicken Sie auf **Produkt-Support**, geben Sie die **Service-Tag-Nummer** Ihres Thin Clients ein, und drücken Sie dann die **Eingabetaste**.
  -  **ANMERKUNG:** Wenn Sie über keine **Service-Tag-Nummer** verfügen, suchen Sie manuell nach Ihrem Thin Client-Modell.
3. Klicken Sie auf **Treiber und Downloads**.
4. Wählen Sie in der Dropdown-Liste **Betriebssystem** die Option **ThinLinux**.
5. Blättern Sie auf der Seite nach unten und gehen Sie wie folgt vor:
  - Laden Sie die Add-ons `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm` und `merlin-nonpxe_3.7.7-00.05_amd64.deb` herunter.
  - Laden Sie die neueste `2.1.0.01_3040_16GB_merlin.exe` oder `2.2.0.00_3040_merlin_16GB.exe` ThinLinux Version 2.x Image-Datei herunter ().
6. Navigieren Sie auf dem Thin Client zu **Einstellungen > Verwaltung > Wyse-Geräte-Agent**.
7. Registrieren Sie das Gerät auf dem Wyse Management Suite-Server.
8. Melden Sie sich bei der Wyse Management Suite-Konsole an.
9. Erstellen Sie eine Anwendungsrichtlinie für `Platform_util-1.0.26-0.3.x86_64.rpm`, `wda-2.1.23-00.01.x86_64.rpm` und `merlin-nonpxe_3.7.7-00.05_amd64.deb` und stellen Sie sie bereit.
10. Starten Sie den Thin Client neu.
11. Melden Sie sich beim Wyse Management Suite-Server an.
12. Kopieren Sie das heruntergeladene Abbild (Datei `2.2.0.00_3040_merlin_16GB.exe`) nach Laufwerk `C:/wms/localrepo/repository/osimages/zipped/`.
  -  **ANMERKUNG:** Das Abbild im komprimierten Ordner wird in einen gültigen Ordner extrahiert. Der Extrahierungsvorgang kann 10–15 Minuten dauern.
13. Melden Sie sich bei der Wyse Management Suite-Konsole an.
14. Rufen Sie **Apps und Daten > OS-Abbild-Repository > WES/ThinLinux** auf und überprüfen Sie, ob das ThinLinux-Abbild verfügbar ist.
15. Navigieren Sie zu **Apps und Daten > OS-Abbildrichtlinien (WES/ThinLinux)** und klicken Sie auf **Richtlinie hinzufügen**.
16. Konfigurieren Sie im Fenster "Richtlinie hinzufügen" die folgenden Optionen:
  - **OS-Typ:** ThinLinux
  - **OS-Subfilter:** ThinLinux (ThinLinux)
  - **Regel:** Nur Upgrade/Diese Version erzwingen
  -  **ANMERKUNG:** Wählen Sie das abgerufene/neue Abbild, das beim Erstellen der Richtlinie in das Repository kopiert wurde.
17. Aktualisieren Sie die anderen erforderlichen Felder nach Bedarf, und klicken Sie auf **Speichern**.
18. Planen Sie den Job.
19. Klicken Sie auf dem Client auf **Jetzt aktualisieren**, um das Abbild zu aktualisieren.

# Aktualisieren von ThinOS 8.x auf 9.0

Sie müssen Wyse Management Suite Version 2.0 oder höher verwenden, um Ihre ThinOS-Firmware auf 9.0 zu aktualisieren.

In der folgenden Tabelle sind die ThinOS-Firmware-Abbilder aufgeführt:

**Tabelle 10. Firmware-Abbild**

Plattform	ThinOS-Firmware-Abbild
Wyse 3040 Thin Client	A10Q_wnos
Wyse 5070 Thin Client mit Celeron-Prozessor	X10_wnos
Wyse 5070 Thin Client mit Pentium-Prozessor	X10_wnos
Wyse 5070 Extended Thin Client mit Pentium-Prozessor	X10_wnos
Wyse 5470 Thin Client	X10_wnos
Wyse 5470 All-in-One Thin Client	X10_wnos

## Hinzufügen von ThinOS-Firmware zum Repository

### Schritte

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

### ANMERKUNG:

- Die hochgeladene Firmware kann nur für das Upgrade von ThinOS 8.6 auf ThinOS 9.1 verwendet werden.
- Die Datei wird zum Repository hinzugefügt, wenn Sie das Kontrollkästchen auswählen. Sie ist jedoch keiner Gruppe und keinem Gerät zugewiesen. Zur Bereitstellung einer Firmware auf einem Gerät oder einer Gruppe von Geräten gehen Sie zur Konfigurationsseite des jeweiligen Geräts oder der Gruppe.

## Upgrade von ThinOS 8.6 auf ThinOS 9.x


### Voraussetzungen

- Das ThinOS-Conversion-Abbild muss zum ThinOS-Firmware-Repository hinzugefügt werden. Weitere Informationen finden Sie unter [ThinOS-Paketdatei zu Repository hinzufügen](#).
- Erstellen Sie eine Gruppe in der Wyse Management Suite mit einem Gruppentoken. Verwenden Sie dieses Gruppentoken, um die ThinOS-8.6-Geräte zu registrieren.
- Der Thin Client muss bei Wyse Management Suite registriert sein.
- Konfigurieren Sie keine Einstellungen für ein Hintergrundbild in Wyse Management Suite.

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **ThinOS**.  
Es wird das Fenster **ThinOS-Konfigurationsmodus auswählen** angezeigt.
3. Wählen Sie **Erweiterter Konfigurationsmodus** aus.
4. Wechseln Sie zu **Firmware-Upgrade** und klicken Sie auf **Dieses Element konfigurieren**.

5. Deaktivieren Sie die Optionen **Live-Upgrade deaktivieren** und **Signatur überprüfen**.
6. Wählen Sie eine Plattform aus dem Dropdownmenü **Plattformtyp** aus.
7. Wählen Sie aus dem Dropdownmenü **Firmware zur automatischen Bereitstellung** die dem Repository hinzugefügte Firmware aus.
8. Klicken Sie auf **Speichern und Veröffentlichen**.  
Die Konfiguration wird auf dem Ziel-Thin Client bereitgestellt. Der Konvertierungsprozess dauert 15 – 20 s und der Thin Client wird automatisch neu gestartet.


 **ANMERKUNG:** Nachdem Sie die Firmware aktualisiert haben, wird das Gerät automatisch bei Wyse Management Suite registriert. Die Konfigurationen des 8.6-Buildvorgangs werden nach dem Upgrade der Firmware nicht übernommen.

## Aktualisieren von ThinOS 9.x auf spätere Versionen mit der Wyse Management Suite

### Voraussetzungen

- Stellen Sie sicher, dass Sie das Image von ThinOS v9.1.1036 auf dem Thin Client installiert haben.
- Stellen Sie sicher, dass Sie eine Gruppe in der Wyse Management Suite mit einem Gruppentoken erstellt haben. Verwenden Sie dieses Gruppentoken, um die ThinOS-9.x-Geräte zu registrieren.
- Stellen Sie sicher, dass der Thin Client bei Wyse Management Suite registriert ist.

### Schritte

1. Navigieren Sie zur Seite **Gruppen & Konfigurationen** und wählen Sie eine Gruppe aus.
  2. Klicken Sie im Dropdownmenü **Richtlinien bearbeiten** auf **ThinOS 9.x**.  
Das Fenster **Konfigurationssteuerelement | ThinOS** wird angezeigt.
  3. Klicken Sie auf **Erweitert**.
  4. Wählen Sie im Feld **Firmware** die Option **OS-Firmware-Updates** aus.
  5. Klicken Sie auf **Durchsuchen**, um die Firmware zu durchsuchen und hochzuladen.  
Es werden die EULA Details des Pakets und der Name der Anbieter angezeigt.
  6. Klicken Sie auf die Namen der einzelnen Anbieter, um die Lizenzvereinbarung für jeden Anbieter zu lesen, und klicken Sie dann auf **Akzeptieren**, um das Paket hochzuladen.  
Sie können die Option **Nicht mehr anzeigen** auswählen, wenn Sie die EULA-Details desselben Anbieters nicht mehr sehen möchten.
-  **ANMERKUNG:** Wenn Sie mehrere Pakete hochladen, werden die EULA-Details jedes Pakets angezeigt. Sie müssen die Lizenzvereinbarung der Pakete einzeln akzeptieren. Die Firmware wird nicht hochgeladen, wenn Sie auf **Ablehnen** klicken.
7. Wählen Sie aus dem Dropdownmenü **Bereitstellung von ThinOS-Firmware auswählen** die hochgeladene Firmware aus.
  8. Klicken Sie auf **Speichern und Veröffentlichen**.  
Der Thin Client lädt die Firmware herunter und startet sie neu. Die Firmware-Version wird aktualisiert.

# Remote-Repository

Wyse Management Suite ermöglicht Ihnen sowohl lokale als auch Remote-Repositories für Anwendungen, Betriebssystem-Images und so weiter. Wenn die Benutzerkonten geografisch verteilt sind, ist es effizient, ein lokales Repository für jedes der verteilten Nutzerkonten zu haben, damit die Geräte Images vom lokalen Repository herunterladen können. Diese Flexibilität liefert die Software `WMS_Repo.exe`. Die Datei `WMS_Repo.exe` ist eine Repository-Software von Wyse Management Suite zum Erstellen verteilter Remote-Repositories, die mit Wyse Management Suite registriert werden können. Die Datei `WMS_Repo.exe` ist nur für **Pro**-Lizenz-Abonnenten verfügbar.

## Voraussetzungen

- Wenn Sie die Wyse Management Suite mit Cloudbereitstellung verwenden, rufen Sie **Portalverwaltung > Konsoleinstellungen > Datei-Repository** auf. Klicken Sie auf **Version x.x herunterladen** und laden Sie die Datei `WMS_Repo.exe` herunter.
- Die Anforderungen an den Server zum Installieren von Wyse Management Suite Repository-Software sind:
  - Windows 2012 R2 oder Windows Server 2016 Standard
  - 4 CPUs
  - 8 GB RAM
  - 40 GB Speicherplatz

## Info über diese Aufgabe

Führen Sie die folgenden Schritte durch, um **WMS-Repo**-Software zu installieren:

## Schritte

1. Melden Sie sich als **Administrator** an und installieren Sie die Datei `WMS_Repo.exe` auf dem Repository-Server.
2. Klicken Sie auf **Weiter** und folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.
3. Klicken Sie auf **Starten** zum Starten des Bildschirms **WMS Repository Registrierung** auf dem Webbrowser.
4. Wählen Sie **Im öffentlichen WMS Management Portal registrieren** für die Registrierung in der Public Cloud.

## Wyse Management Suite Repository


### Registration

Register to Public WMS Management Portal

WMS Server

WMS Repository URL  
 \*  
[Change Repository URL?](#)

Admin Name  
 \*

Admin Password  
 \* 


Repository Location  
 \*

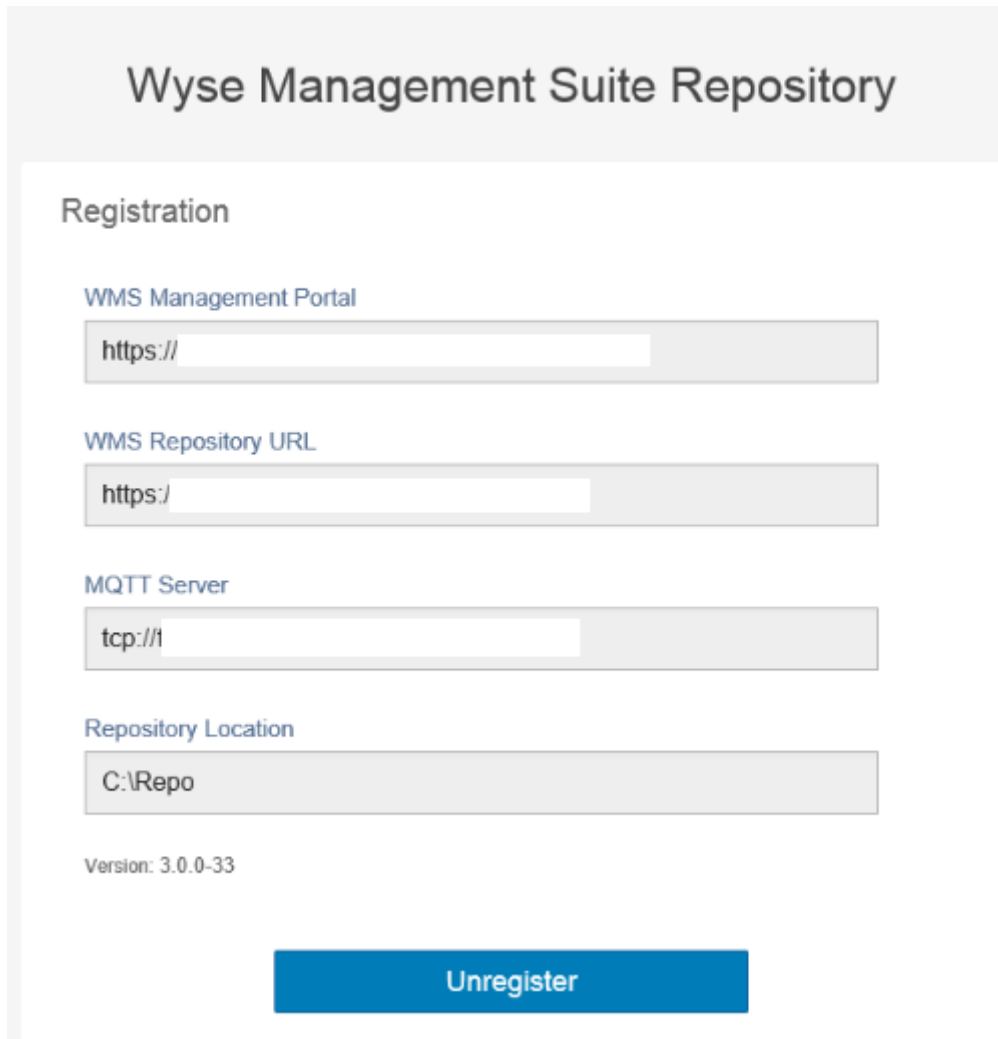
Version: 3.0.0-33

**Register**

**Abbildung 20. Registrieren in einer Public Cloud**

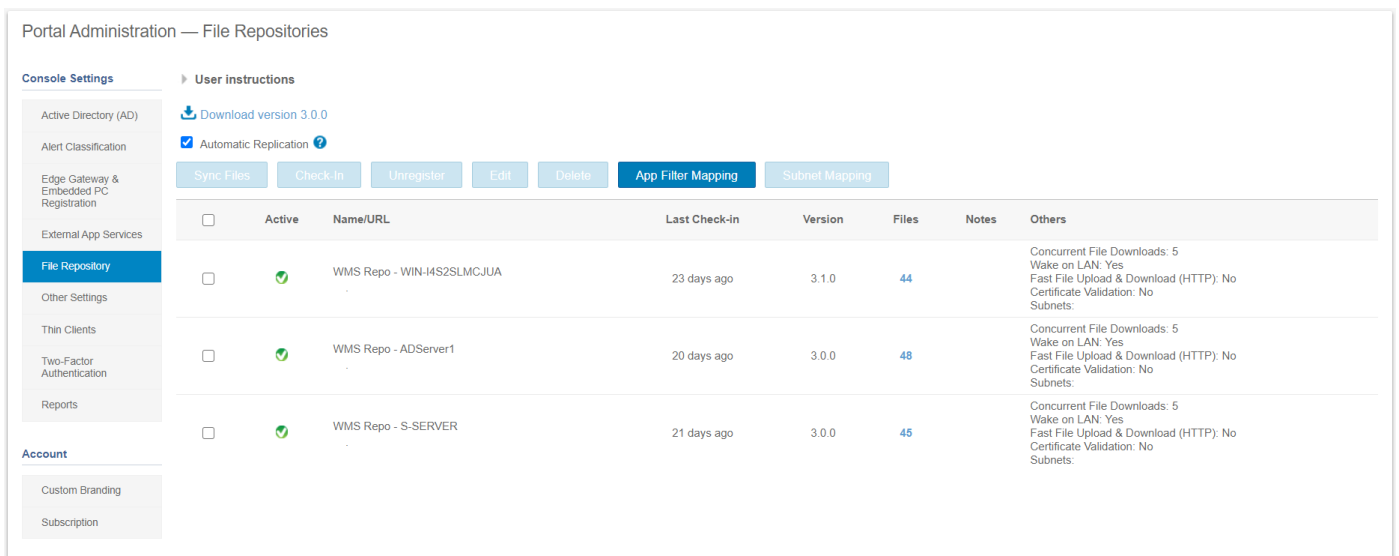
5. Geben Sie folgende Informationen ein:
  - a. Server-URL von Wyse Management Suite
 

 **ANMERKUNG:** Wenn Sie sich nicht für Wyse Management Suite Version 1.0 registrieren, können Sie MQTT-Server-URL nicht verwenden.
  - b. WMS-Repository-URL (aktualisieren Sie die URL mit dem Domainnamen)
  - c. Benutzername zum Anmelden des Administrators der Wyse Management Suite
  - d. Kennwort zum Anmelden des Administrators der Wyse Management Suite
  - e. Repository-Pfadinformationen
6. Klicken Sie auf **Registrieren**.
7. Wenn die Registrierung erfolgreich ist, wird das **Registrierung** Fenster angezeigt.



**Abbildung 21. Registrierung erfolgreich**

8. Der folgende Bildschirm auf dem Wyse Management Suite Portal bestätigt die erfolgreiche Registrierung des Remote-Repositorys:



**Abbildung 22. Registrierung beim Portal erfolgreich**

9. HTTPS ist standardmäßig bei `WMS_Repo.exe` aktiviert und die Installation erfolgt mit selbstsigniertem Zertifikat. Zum Installieren Ihres eigenen domänenspezifischen Zertifikats scrollen Sie auf der Registrierungsseite nach unten, um die SSL-Zertifikate hochzuladen.

The screenshot displays a web interface for managing SSL certificates. At the top, it shows 'Server SSL Certificates: Enabled' and a link to the 'SSL Certificate Guide'. Below this, the 'Current Certificate' section is visible, showing details like 'Issued to: [redacted].com', 'Issued from: [redacted].com', and 'Valid to: August 18, 2118'. The main section is titled 'PKCS-12 Key/Certificate Pair'. It contains instructions: 'Upload HTTPS PKCS-12 (.pfx, .p12). Apache intermediate certificate is needed for IIS pfx.' There are three input fields: 'PKCS-12 file' with a 'Browse...' button, 'Password for PKCS file' with a masked password field, and 'Intermediate certificate' with a 'Browse...' button. An 'Upload' button is located at the bottom of the form.

**Abbildung 23. Zertifikat hochladen**

10. Der Server wird neu gestartet und das hochgeladene Zertifikat wird angezeigt.

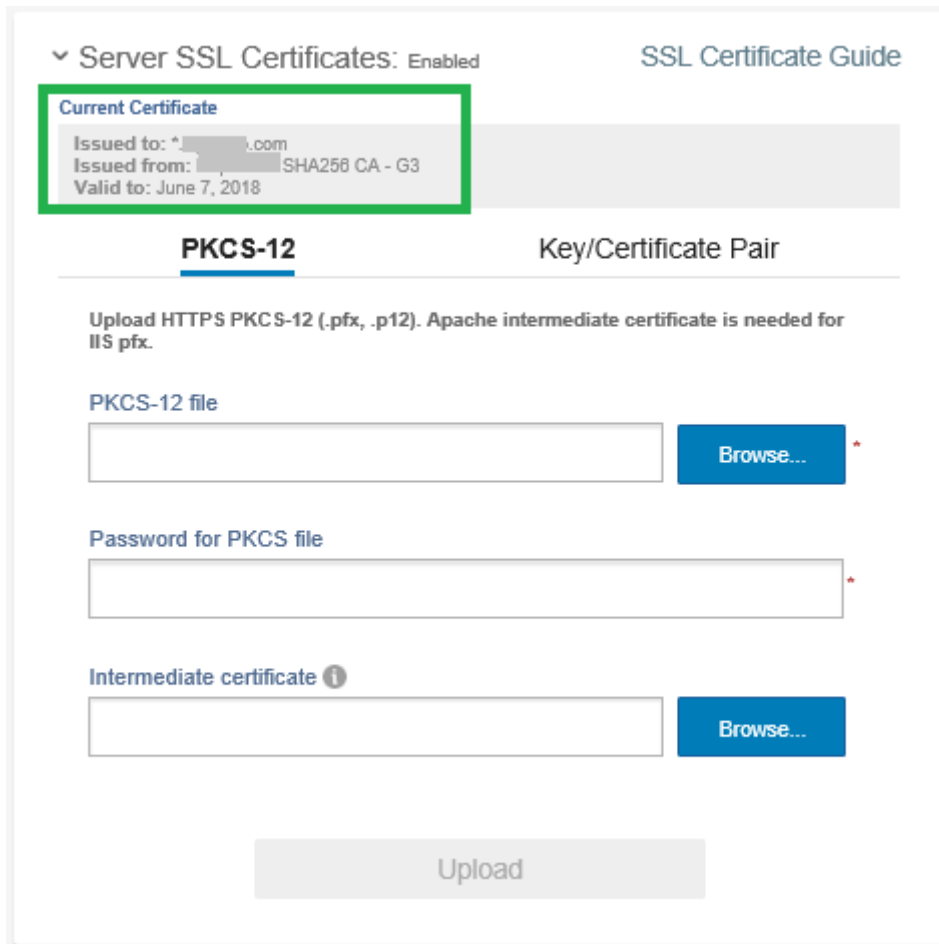


Abbildung 24. SSL-Zertifikat aktiviert

11. Wenn die Wyse Management Suite mit einem selbstsigniertem oder einem privaten Domänenzertifikat aktiviert wird, können Sie das Zertifikat auf den Wyse Management Suite Repository-Server hochladen, um die Wyse Management Suite CA-Anmeldeinformationen zu überprüfen.

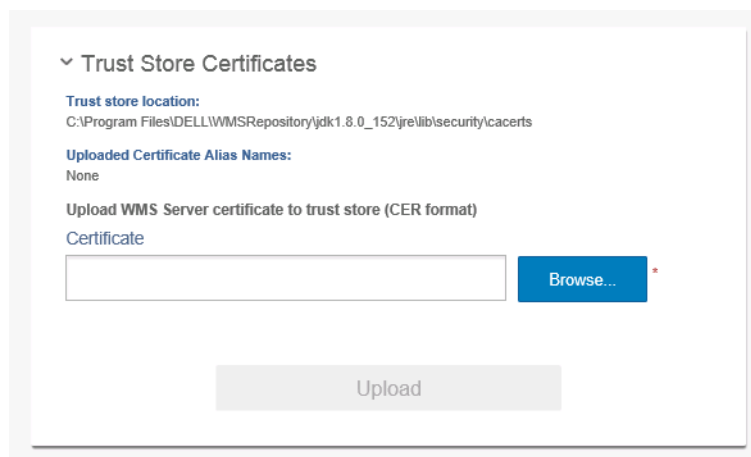


Abbildung 25. Truststore-Zertifikate

12. Navigieren Sie zu `C:\wmsrepo`, das Sie bei der Registrierung angegeben haben. Sie können die Ordner, in denen alle Repository-Dateien gespeichert und verwaltet werden, ansehen.

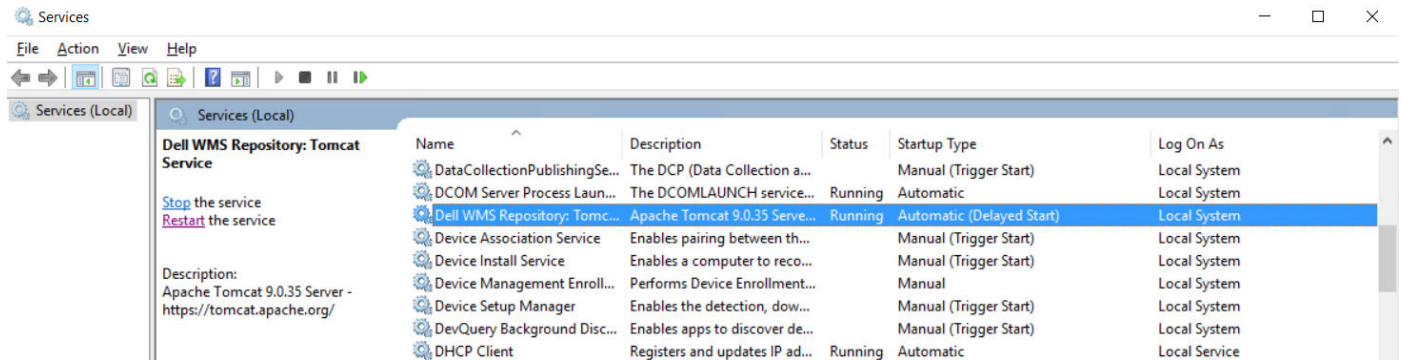
**Themen:**

- [Verwalten des Wyse Management Suite Repository-Dienstes](#)

- Proxy-Unterstützung für Wyse Management Suite-Remote-Repositorys

## Verwalten des Wyse Management Suite Repository-Dienstes

Das Wyse Management Suite Repository wird als **Dell Repository WMS: Tomcat Service** im Fenster der lokalen Dienste von Windows angezeigt und ist so konfiguriert, dass es automatisch startet, wenn der Server neu gestartet wird.



## Proxy-Unterstützung für Wyse Management Suite-Remote-Repositorys

Ab Wyse Management Suite 3.1 unterstützen Remote-Repositorys SOCKS5-Proxy für alle HTTPS- und MQTT-Kommunikationen zu Wyse Management Suite.

Nur systemweite Proxys werden unterstützt, da das Remote-Repository als Windows-Dienst ausgeführt wird. Außerdem werden nur Proxys mit AD-Authentifizierung oder ohne Authentifizierung unterstützt. Sie können die Proxyserver über eine beliebige Methode konfigurieren. Im Folgenden finden Sie einige Beispiele für die Konfiguration der Proxyserver-Informationen:

- Mithilfe des Befehls netsh: Sie können den folgenden Befehl verwenden, um die Proxyserver-Informationen zu konfigurieren.

```
netsh winhttp set proxy proxy-server="socks=localhost:9090" bypass-list="localhost"

C:\Users\administrator.WMSAD61>netsh winhttp set proxy proxy-server="socks=<proxy server
IP>" bypass-list="localhost"

Current WinHTTP proxy settings:

Proxy Server(s) : socks=<proxy server IP>
Bypass List     : localhost
```

- Verwenden der in DHCP konfigurierten WPAD-Datei: Wyse Management Suite Repository-Server muss mit DHCP-IP-Adresse konfiguriert werden und Internet Explorer muss mit Einstellungen automatisch erkennen konfiguriert werden. Sie müssen das DHCP-Options-Tag 252 mit der WPAD.pac-Datei konfigurieren. Nachfolgend finden Sie ein Beispiel für einen PAC-Dateinhalt:

```
function FindProxyForURL(url, host)
{
    if (shExpMatch(host, "*wysemanagementsuite.com*")) {
        return "SOCKS <proxy server IP>";
    }
    return "DIRECT";
}
```

Sie können die Proxyeinstellungen auch mithilfe von Gruppenrichtlinien konfigurieren.

- **ANMERKUNG:** Proxy-Einstellungen werden gelesen, wenn der Repository-Dienst gestartet wird. Wenn Sie zu einem späteren Zeitpunkt Änderungen an den Proxy-Einstellungen vornehmen, müssen Sie den Repository-Dienst neu starten.
- **ANMERKUNG:** Die Hostnamensauflösung wird nicht festgelegt, wenn SOCKS4-Proxy verwendet wird. Sie müssen die in vorhandene Hostdatei in C:\Windows\System32\drivers\etc aktualisieren, um die URL/den Hostnamen der Public Cloud auf

dem Server aufzulösen, auf dem das Wyse Management Suite-Repository installiert ist. Wenn SOCKS5-Proxy verwendet wird, wird die Hostnamen-Auflösung mithilfe der in den Netzwerkeinstellungen des Servers konfigurierten DNS aufgelöst.

# Fehlerbehebung auf Ihrem Gerät

Sie können die Fehlerbehebungs-Informationen über die Seite **Geräte** anzeigen und verwalten.

## Schritte

1. Klicken Sie auf der Seite **Gerätedetails** auf die Registerkarte **Fehlerbehebung**.
2. Klicken Sie auf **Screenshot anfordern**.  
Sie können den Screenshot des Thin Client mit oder ohne Zustimmung des Clients erstellen. Wenn das Kontrollkästchen **Zustimmung des Benutzers erforderlich machen** ausgewählt ist, wird auf dem Client eine Meldung angezeigt. Diese Option gilt nur für Windows Embedded Standard-, Linux- und ThinLinux-Geräte.
3. Klicken Sie auf **Prozessliste anfordern**, um die Liste der ausgeführten Verfahren auf dem Thin Client anzufordern.
4. Klicken Sie auf **Dienstliste anfordern**, um die Liste der ausgeführten Dienste auf dem Thin Client anzufordern.
5. Klicken Sie auf **Überwachung starten** für den Zugriff auf die Konsole Leistungsmetrik.  
Auf der Konsole **Leistungsmetrik** werden die folgenden Details angezeigt:
  - Durchschnittliche CPU-Last in der letzten Minute.
  - Durchschnittliche Speichernutzung in der letzten Minute

## Themen:

- [Anfordern einer Protokolldatei mithilfe von Wyse Management Suite](#)
- [Anzeigen von Prüfprotokollen mithilfe von Wyse Management Suite](#)
- [Gerät kann nicht bei Wyse Management Suite registriert werden, wenn der WinHTTP-Proxy konfiguriert ist](#)
- [RemoteFX USB-Umleitungsrichtlinie wird für USB-Massenspeichergeräte nicht angewendet.](#)
- [In der Wyse Management Suite konfigurierte WLAN-Einstellungen sind nicht über mehrere Wyse 5070 Thin Clients persistent](#)

## Anfordern einer Protokolldatei mithilfe von Wyse Management Suite

### Voraussetzungen

Das Gerät muss aktiviert sein, um einen Pull für eine Protokolldatei auszuführen.

### Schritte

1. Gehen Sie auf die Seite **Geräte** und klicken Sie auf ein bestimmtes Gerät.  
Die Gerätedetails werden angezeigt.
2. Klicken Sie auf die Registerkarte **Geräteprotokoll**.
3. Klicken Sie auf **Protokolldatei anfordern**.
4. Nachdem die Protokolldateien auf den Wyse Management Suite-Server hochgeladen wurden, klicken Sie auf den Link **Klicken Sie hier** und laden Sie die Protokolle herunter.

 **ANMERKUNG:** Das ThinOS-Gerät lädt die Systemprotokolle hoch.

# Anzeigen von Prüfprotokollen mithilfe von Wyse Management Suite

## Schritte

1. Gehen Sie zu **Ereignisse Überprüfung**.
2. Wählen Sie aus der Dropdownliste **Konfigurationsgruppen** die Gruppe aus, für die Sie das Überwachungsprotokoll anzeigen möchten.
3. Wählen Sie aus der Dropdownliste **Zeitspanne** den Zeitraum, für den Sie die Ereignisse anzeigen lassen wollen. Das Fenster **Überwachung** bereitet die Informationen in einer typischen Überwachungsprotokollansicht auf. Sie können den Zeitstempel, den Ereignistyp, die Quelle und eine Beschreibung der einzelnen Ereignisse in der Reihenfolge des Auftretens anzeigen.

## Gerät kann nicht bei Wyse Management Suite registriert werden, wenn der WinHTTP-Proxy konfiguriert ist

WDA ist ein WinHTTP-Client und ruft WinHTTP-Proxyinformationen vom lokalen System ab.

Wenn Sie den WinHTTP-Proxy konfiguriert haben und das Gerät den Wyse Management Suite-Server nicht kontaktieren kann, gehen Sie wie folgt vor, um die auf Systemebene verfügbaren Proxy-Informationen zu aktivieren:

- **Fall 1:** Wenn das Gerät zu einer Domain hinzugefügt wird, aktivieren Sie die IE-Proxy-Konfigurationen für jeden Benutzer, der die Gruppenrichtlinie aus der Domain verwendet. Sie müssen die Gruppenrichtlinie vom Domain-Controller konfigurieren, um die IE-Proxy-Konfigurationen für jeden Client und nicht für jeden Benutzer zu aktivieren.

Navigieren Sie zu `Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Internet Explorer\Proxy-Einstellungen pro Computer` vornehmen (anstelle von pro Benutzer) und wählen Sie **Aktivieren** aus. Navigieren Sie außerdem im Internet Explorer zu den `IE-Einstellungen > Internetoptionen > Verbindungen > LAN-Einstellungen` und aktivieren Sie die Option **Einstellungen automatisch erkennen**.

- **Fall 2:** Wenn das Gerät nicht zu einer Domain hinzugefügt wird, navigieren Sie in der Windows-Registrierung zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings`. Erstellen Sie ein **32-Bit-DWORD** mit dem Namen **ProxySettingsPerUser** und setzen Sie es auf den Wert 0. Navigieren Sie außerdem im Internet Explorer zu den `IE-Einstellungen > Internetoptionen > Verbindungen > LAN-Einstellungen` und aktivieren Sie die Option **Einstellungen automatisch erkennen**.

## RemoteFX USB-Umleitungsrichtlinie wird für USB-Massenspeichergeräte nicht angewendet.

### Schritte

1. Melden Sie sich als Administrator beim Gerät an.
2. Deaktivieren Sie den Write Filter.
3. Gehen Sie zu **Ausführen** und geben Sie **Regedit** ein.
4. Fahren Sie mit `HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces` fort.
5. Fügen Sie den Registrierungsschlüssel String als **100** hinzu und legen Sie den Wert für das Massenspeichergerät fest auf `{53F56307-B6BF-11D0-94F2-00A0C91EFB8B} for CD ROM : {53F56308-B6BF-11D0-94F2-00A0C91EFB8B}`.

 **ANMERKUNG:** Geschweifte Klammern sind obligatorisch.

# In der Wyse Management Suite konfigurierte WLAN-Einstellungen sind nicht über mehrere Wyse 5070 Thin Clients persistent

Wenn Sie eine WLAN-Verbindung auf einem Wyse 5070 Thin Client konfigurieren, wird eine Verbindung zu einem bestimmten Drahtlosnetzwerk (SSID) hergestellt, ohne dass Sie nach dem Passwort gefragt werden. Wenn dieselbe Konfiguration in die Wyse Management Suite exportiert und auf anderen Wyse 5070 Thin Clients bereitgestellt wird, wird die Konfiguration angewendet und Sie werden zur Eingabe eines Kennworts aufgefordert, um eine Verbindung zum selben Drahtlosnetzwerk herzustellen. Gehen Sie wie folgt vor, um die WLAN-Einstellungen persistent zu machen:

## Schritte

1. Verbinden Sie den Wyse 5070 Thin Client mit dem Drahtlosnetzwerk.
2. Führen Sie die Datei `DWirelessProfileEditor.exe` aus.  
Das Fenster **Funknetzwerkprofil-Kennworteditor** wird angezeigt.
3. Navigieren Sie zum Zielpfad, um das Profil als XML-Datei zu speichern, und klicken Sie auf **Speichern**.
4. Klicken Sie auf die Schaltfläche **WLAN-Profil exportieren** im Fenster **Funknetzwerkprofil-Kennworteditor**.
5. Wählen Sie aus der Drop-Down-Liste **Profile** das Profil aus, um die Konfiguration bereitzustellen.
6. Löschen Sie das Feld **Passwort** und geben Sie das Passwort erneut ein.
7. Klicken Sie auf **Kennwort ändern**.  
 **ANMERKUNG:** Klicken Sie nicht erneut auf die Schaltfläche **WLAN-Profil exportieren**.
8. Schließen Sie das Fenster **Funknetzwerkprofil-Kennworteditor**.
9. Melden Sie sich bei der Wyse Management Suite an.
10. Navigieren Sie zu **Apps & Daten > Datei-Repository > Bestand**.
11. Klicken Sie auf **Datei hinzufügen**.
12. Navigieren Sie zu der XML-Datei.
13. Wählen Sie in der **Typ**-Dropdown-Liste **Windows Wireless-Profil** aus.
14. Geben Sie die Beschreibung ein.
15. Aktivieren Sie die Option **Vorhandene Datei überschreiben**, wenn Sie die gegenwärtige Konfiguration überschreiben möchten.
16. Klicken Sie auf **Hochladen**.
17. Navigieren Sie zu **Gruppen & Konfigurationen > Profile bearbeiten > WES > Netzwerk**.
18. Klicken Sie auf **Dieses Element konfigurieren**.
19. Wählen Sie aus der Dropdownliste **Windows Wireless-Profile** die hochgeladene Datei aus.
20. Klicken Sie auf **Speichern und Veröffentlichen**.

## Häufig gestellte Fragen

### Themen:

- Was hat Vorrang zwischen Wyse Management Suite und der ThinOS-Benutzeroberfläche, wenn in Konflikt stehende Einstellungen durchgesetzt werden?
- Wie verwende ich das Wyse Management Suite Datei-Repository?
- Wie kann ich Benutzer aus einer .csv-Datei importieren?
- Wie prüfe ich die Version von Wyse Management Suite
- Wie Sie DHCP-Options-Tags erstellen und konfigurieren
- Wie Sie DNS-SRV-Einträge erstellen und konfigurieren
- Schritte zum Ändern des Hostnamens zur IP-Adresse
- Wie kann ich das Gerät mit einem selbstsignierten Remote-Repository abbilden?

## Was hat Vorrang zwischen Wyse Management Suite und der ThinOS-Benutzeroberfläche, wenn in Konflikt stehende Einstellungen durchgesetzt werden?

Alle Einstellungen, die mit Wyse Management Suite konfiguriert wurden, haben Vorrang vor den Einstellungen, die lokal auf dem ThinOS-Client konfiguriert oder mithilfe des Administratorrichtlinien-Tools veröffentlicht wurden.

In der folgenden Reihenfolge wird das Prioritätsset für ThinOS-Konfigurationen definiert:

**Wyse Management Suite-Richtlinien > Administratorrichtlinien-Tool > lokales ThinOS-UI**

## Wie verwende ich das Wyse Management Suite Datei-Repository?

### Schritte

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. Aktivieren Sie zum Registrieren des Repositorys für die öffentliche Cloud der Wyse Management Suite die Option **Registrieren auf öffentlichem WMS-Verwaltungsportal**.
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.
  - a. Wählen Sie aus der Dropdownliste der Option **Gleichzeitige Dateidownloads** die Anzahl der Dateien aus.
  - b. Aktivieren oder deaktivieren Sie die Option **Wake-on-LAN**.
  - c. 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.
  - d. Wählen Sie das Kontrollkästchen **Zertifikatsvalidierung** zur Aktivierung der CA-Zertifikatsvalidierung 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, Abbildpush/-pull, sind erfolgreich. Wenn das Zertifikat nicht im Client vorhanden ist, bietet der Wyse Management Suite-Server eine generische Prüfereignisbenachrichtigung **Validierung der Zertifizierungsstelle fehlgeschlagen** auf der Seite **Ereignisse**. Alle Vorgänge, wie z. B., Apps und Daten, Abbildpush/-pull, 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.

- Fügen Sie einen Hinweis in dem angegebenen Feld hinzu.
- Klicken Sie auf **Einstellungen speichern**.

## Wie kann ich Benutzer aus einer .csv-Datei importieren?

### Schritte

1. Klicken Sie auf **Benutzer**.  
Die Seite **Benutzer** wird angezeigt.
2. Wählen Sie die Option **Nicht zugewiesenen Administratoren**.
3. Klicken Sie auf **Massenimport**.  
Das Fenster **Massenimport** wird angezeigt.
4. Klicken Sie auf **Durchsuchen** und wählen Sie die .csv-Datei aus.
5. Klicken Sie auf **Importieren**.

## Wie prüfe ich die Version von Wyse Management Suite

### Schritte

1. Melden Sie sich bei der Wyse Management Suite an.
2. Gehen Sie zu **Portalverwaltung > Abonnement**.  
Die Wyse Management Suite-Version wird im Feld **Serverinformation** angezeigt.

## Wie Sie DHCP-Options-Tags erstellen und konfigurieren

### Schritte

1. Öffnen Sie den Server-Manager.
2. Gehen Sie zu **Tools** und klicken Sie auf **DHCP-Option**.
3. Gehen Sie zu **FQDN > IPv4** und klicken Sie mit der rechten Maustaste auf **IPv4**.
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.
6. Klicken Sie auf **Hinzufügen**.  
Das Fenster **Optionstyp** wird angezeigt.
7. Konfigurieren der erforderlichen DHCP-Option-Tags.
  - Zum Erstellen des Option-Tags 165 Wyse Management Suite Server-URL gehen Sie wie folgt vor:
    - a. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
      - Name – WMS
      - Datentyp – Zeichenfolge
      - Code – 165

- Beschreibung – WMS\_Server
- b. Geben Sie den folgenden Wert ein und klicken Sie auf **OK**.  
Zeichenfolge –WMS FQDN
- Zum Erstellen des Option-Tags 166 MQTT-Server-URL gehen Sie wie folgt vor:
  - a. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
    - Name – MQTT
    - Datentyp – Zeichenfolge
    - Code – 166
    - Beschreibung – MQTT-Server
  - b. Geben Sie den folgenden Wert ein und klicken Sie auf **OK**.  
Zeichenfolge –MQTT FQDN  
Zum Beispiel **WMSServerName.YourDomain.Com:1883**.
- Zum Erstellen des Option-Tags 167 Wyse Management Suite CA-Validation-Server-URL gehen Sie wie folgt vor:
  - a. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
    - Name – CA-Validation
    - Datentyp – Zeichenfolge
    - Code – 167
    - Name – CA-Validation
  - b. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.  
Zeichenfolge – WAHR/FALSCH
- Zum Erstellen des Option-Tags 199 Wyse Management Suite Gruppentoken-Server-URL gehen Sie wie folgt vor:
  - a. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
    - Name – Gruppentoken
    - Datentyp – Zeichenfolge
    - Code – 199
    - Beschreibung – Gruppentoken
  - b. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.  
Zeichenfolge – defa-Quarantäne



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

## Wie Sie DNS-SRV-Einträge erstellen und konfigurieren

### Schritte

1. Öffnen Sie den Server-Manager.
2. Gehen Sie zu **Tools** und klicken Sie auf **DNS**.
3. Gehen Sie zu **DNS > DNS-Server-Host-Name > Forward-Lookupzonen > Domain > \_tcp** und klicken Sie mit der rechten Maustaste auf die Option **\_tcp**.
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:
  - 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
- 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
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:
    - 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
    - b. Zum Erstellen eines CA-Validierungsdatensatzes für die Wyse Management Suite geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
      - Datensatzname—\_WMS\_CAVALIDATION
      - Text–TRUE/FALSE

## Schritte zum Ändern des Hostnamens zur IP-Adresse

### Info über diese Aufgabe

Sie müssen den Hostnamen in die IP-Adresse ändern, wenn die Hostname-Auflösung fehlschlägt.

### Schritte

1. Öffnen Sie die DOS-Eingabeaufforderung im erhöhten Administratormodus
2. Ändern Sie das Verzeichnis zu **C:\Program Files\DELL\WMS\MongoDB\bin**.
3. Geben Sie den folgenden Befehl ein: **mongo localhost -username stratus -p --authenticationDatabase admin**  
Ausgabe: MongoDB Shell Version v3.4.10
4. Geben Sie das Kennwort ein.  
Ausgabe:
  - connecting to: mongod://127.0.0.1:27017/localhost
  - MongoDB-Serverversion: 3.4.10
5. Geben Sie Folgendes ein: **use stratus**  
Ausgabe: switched to db stratus
6. Geben Sie den folgenden Befehl ein: **> db.bootstrapProperties.updateOne( {'name': 'stratusapp.server.url'}, {\$set : {'value' : "https://IP:443/ccm-web"}} )**  
Ausgabe: { "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }
7. Geben Sie den folgenden Befehl ein: **> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})**  
Ausgabe: { "\_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }

## Wie kann ich das Gerät mit einem selbstsignierten Remote-Repository abbilden?

Sie können die Abbilderstellung von Windows-integrierten Standard- und ThinLinux-Geräten aus dem lokalen Repository der privaten Cloud oder aus dem Remote-Repository der öffentlichen Cloud durchführen.

## Voraussetzungen

Wenn das Abbild aus dem lokalen Repository der privaten Cloud oder aus dem Remote-Repository der öffentlichen Cloud mit einem selbstsignierten Zertifikat bereitgestellt wird, muss der Administrator das selbstsignierte Zertifikat an die Thin Clients übertragen, um die Abbilderstellung durchzuführen, wenn die CA-Validierung aktiviert ist.

## Schritte

1. Exportieren Sie das selbstsignierte Zertifikat von Internet Explorer oder MMC.
2. Laden Sie das Zertifikat in Wyse Management Suite hoch – siehe [Abbildrichtlinie](#).
3. Übertragen Sie das Zertifikat mithilfe der Sicherheitsrichtlinie an die Zielclients oder Gruppen von Clients. Warten Sie, bis der **Konfigurationsrichtlinienjob** abgeschlossen ist.
4. Aktivieren Sie die CA-Validierung im lokalen Repository der privaten Cloud oder im Remote-Repository der öffentlichen Cloud.
5. Erstellen Sie eine Abbildrichtlinie und planen Sie die Gruppe.