Dell Wyse Management Suite
Version 2.1 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.
Kapitel 1: Einführung in die Wyse Management Suite........................................................................... 8
Editionen von Wyse Management Suite......................................................................................................8
Wyse Management Suite-Funktionsmatrix.........................................................................................................9

Kapitel 2: Erste Schritte mit der Wyse Management Suite........................................................................ 11
Anmelden bei der Wyse Management Suite in einer Public Cloud.................................................................11
Voraussetzungen für Wyse Management Suite in einer Private Cloud..............................................................12
Funktionsbereiche der Management Console.......................................................................................................13
Konfigurieren und Verwalten von Thin Clients....................................................................................................13
Wyse-Geräte-Agent..................................................................................................................................................14

Kapitel 3: Installieren oder Aktualisieren von Wyse Geräte-Agent................................................................ 16
Manuelles Installieren von Wyse Geräte-Agenten auf einem Windows-eingebetteten Gerät.............................16
Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie.....................17
Installieren oder Aktualisieren von Wyse Geräte-Agenten auf ThinLinux- und Linux-Clients............................17

Kapitel 4: Registrieren und Konfigurieren eines neuen Geräts mithilfe von Wyse Management Suite......... 19
Registrieren und konfigurieren Sie ein neues Windows-eingebettetes Standard-Gerät mithilfe von Wyse Management Suite....................................................................................................................19
Registrieren und Konfigurieren eines neuen ThinOS-8.x-Geräts mithilfe von Wyse Management Suite..............20
Registrieren und Konfigurieren eines neuen Linux- oder ThinLinux-Geräts mithilfe von Wyse Management Suite.........................................................................................................................................................21
Registrieren und Konfigurieren eines neuen Wyse Software-Thin Clients mithilfe der Wyse Management Suite.........................................................................................................................................................22

Kapitel 5: Wyse Management Suite-Dashboard............................................................................................. 23
Anzeigen von Warnungen........................................................................................................................................24
Anzeigen der Ereignisliste.........................................................................................................................................24
Anzeigen des Gerätestatus.........................................................................................................................................24
Aktivieren der Anmeldungvalidierung.....................................................................................................................24
Ändern von Benutzereinstellungen........................................................................................................................25
Zugriff auf die Onlinehilfe.......................................................................................................................................25
Ändern Ihres Kennworts.........................................................................................................................................25
Abmelden von der Verwaltungskonsole..................................................................................................................26

Kapitel 6: Verwalten von Gruppen und Konfigurationen.................................................................................. 27
Bearbeiten einer nicht verwalteten Gruppe............................................................................................................28
Erstellen einer Standard-Geräterichtliniengruppe..................................................................................................29
Erstellen einer ThinOS-Auswahlgruppe...................................................................................................................29
Bearbeiten einer Standard-Geräterichtliniengruppe.............................................................................................30
Bearbeiten einer ThinOS-Auswahlgruppe................................................................................................................30
Entfernen einer ThinOS-Auswahlgruppe..................................................................................................................30
Konfigurieren von Richtlinien der Globalen Klasse............................................................................................31
Kapitel 7: Verwalten von Geräten

Methoden zum Registrieren Geräten bei Wyse Management Suite........................................................................................................... 43
  Registrieren von ThinOS-Geräten mit dem Wyse Geräte-Agenten................................................................. 43
  Registrieren von Windows Embedded Standard Thin Clients bei der Wyse Management Suite über Wyse Geräte-Agent................................................................................................................................. 44
  Registrieren des Wyse Software Thin Client bei der Wyse Management Suite über den Wyse Geräte-Agenten................................................................. 44
  Registrieren von ThinLinux Thin Clients über Wyse Geräte-Agent................................................................. 45
  Registrieren von ThinOS-Geräten mithilfe der FTP-INI-Methode................................................................. 45
  Registrieren von Geräten mit ThinLinux Version 2.0 mithilfe der FTP-INI-Methode........................................ 46
  Registrieren von Geräten mit ThinLinux Version 1.0 mithilfe der FTP-INI-Methode........................................ 47
  Registering devices by using DHCP option tags.......................................................................................... 47
  Geräte mit DNS-SRV-Eintrag registrieren...................................................................................................... 48
Suchen nach einem Gerät mithilfe von Filtern........................................................................................................... 50
Filter auf der Seite „Geräte“ speichern........................................................................................................... 50
Abfragen des Gerätestatus................................................................................................................................. 51
Sperren der Geräte.................................................................................................................................................. 51
Neustart der Geräte.................................................................................................................................................. 51
Registrierung eines Geräts aufheben.................................................................................................................. 51
Anmeldungsvorwahl.................................................................................................................................................. 52
  Validieren der Anmeldung eines Geräts........................................................................................................... 52
Gerät auf Werkseinstellungen zurücksetzen.......................................................................................................... 53
Ändern einer Gruppenzuweisung auf der Seite „Geräte“.................................................................................. 53
Senden von Meldungen an ein Gerät.................................................................................................................. 53
Aktivieren eines Geräts.................................................................................................................................................. 54
Anzeigen der Gerätedetails.................................................................................................................................................. 54
Verwalten der Gerätezusammenfassung.......................................................................................................................... 54
Anzeigen von Systeminformationen....................................................................................................................................... 55
Anzeigen von Geräteeignissen............................................................................................................................................. 55
Anzeigen installierter Anwendungen................................................................................................................................... 55
Umbenennen des Thin Client............................................................................................................................................... 56
Konfigurieren von Remote-Spiegelung-Verbindung........................................................................................................... 56
Herunterfahren von Geräten.................................................................................................................................................. 56
Hinzufügen eines Tags zu einem Gerät.................................................................................................................................. 57
Compliance-Status des Geräts................................................................................................................................................. 57
Pull für Windows Embedded Standard oder ThinLinux-Abbild ausführen....................................................................... 57
Anfordern einer Protokolldatei............................................................................................................................................. 58
Fehlerbehebung auf Ihrem Gerät.......................................................................................................................................... 59

Kapitel 8: Anwendungen und Daten................................................................................................................................. 60
Anwendungsrichtlinie.............................................................................................................................................................. 61
  Konfigurieren einer Thin-Client-Anwendungsbestandsaufnahme......................................................................................... 61
  Konfigurieren der Wyse Software Thin-Client-Anwendungsbestandsaufnahme............................................................. 62
Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Thin Clients................................................................. 62
Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf Thin Clients................................................................. 63
Einmaliges Anmelden für Citrix StoreFront mithilfe der Standard-Anwendungsrichtlinie aktivieren.................................. 64
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients.......................................................... 65
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie für Wyse Software-Thin Clients.................................... 66
Abbildrichtlinie........................................................................................................................................................................ 67
  Hinzufügen von ThinOS-Firmware zum Repository........................................................................................................ 68
  Hinzufügen von ThinOS-BIOS-Datei zum Repository.................................................................................................... 68
  Hinzufügen von ThinOS-Paketdatei zu Repository........................................................................................................... 69
  Hinzufügen von ThinOS-9.x-Firmware zum Repository................................................................................................ 69
  Hinzufügen von ThinOS-9.x-Paketdatei zu Repository.................................................................................................. 69
Erstellen von Windows-eingebetteten Standard- und ThinLinux-Abbildrichtlinien............................................................... 70
  Verwalten eines Datei-Repositories.................................................................................................................................... 70

Kapitel 9: Verwalten von Regeln.............................................................................................................................................. 72
Bearbeiten einer Registrierungsregel.................................................................................................................................... 73
Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte................................................................. 73
Bearbeitung der Regel für die automatische Zuweisung nicht verwalteter Geräte................................................................. 74
Deaktivieren und Löschen von Regeln für die automatische Zuweisung nicht verwalteter Geräte....................................... 74
Speichern der Regelreihenfolge............................................................................................................................................ 74
Hinzufügen einer Regel für Warnmeldungen.......................................................................................................................... 75
Bearbeiten einer Warnmeldungsrregel................................................................................................................................... 75

Kapitel 10: Aufträge verwalten............................................................................................................................................... 76
BIOS-Administratorkennwort synchronisieren................................................................................................................... 77
Suchen eines geplanten Jobs mithilfe von Filtern.................................................................................................................. 78
Planen des Gerätebefehljobs.................................................................................................................................................. 79
Planen der Abbildrichtlinie..................................................................................................................................................... 79
Planen einer Anwendungsrichtlinie....................................................................................................................................... 80
ThinLinux 1.x auf 2.x aktualisieren.............................................................................................................................. 109
Aktualisieren von ThinOS 8.x auf 9.0............................................................................................................................... 110
Hinzufügen von ThinOS-Firmware zum Repository....................................................................................................... 110
Upgrade von ThinOS 8.6 auf ThinOS 9.x..................................................................................................................... 111
Aktualisieren von ThinOS 9.x auf spätere Versionen mit der Wyse Management Suite........................................ 111

Kapitel 17: Remote-Repository................................................................................................................................. 113
Verwalten des Wyse Management Suite Repository-Dienstes..................................................................................... 119

Kapitel 18: Fehlerbehebung auf Ihrem Gerät........................................................................................................ 120
Anfordern einer Protokolldatei mithilfe von Wyse Management Suite........................................................................ 120
Anzeigen von Prüfprotokollen mithilfe von Wyse Management Suite......................................................................... 121
Gerät kann nicht bei Wyse Management Suite registriert werden, wenn der WinHTTP-Proxy konfiguriert ist........... 121
RemoteFX USB-Umleitungsrichtlinie wird für USB-Massenspeichergeräte nicht angewendet............................ 121

Kapitel 19: Häufig gestellte Fragen.................................................................................................................. 123
Was hat Vorrang zwischen Wyse Management Suite und der ThinOS-Benutzeroberfläche, wenn in Konflikt stehende Einstellungen durchgesetzt werden?................................................................. 123
Wie verwende ich das Wyse Management Suite Datei-Repository?........................................................................ 123
Wie kann ich Benutzer aus einer .csv-Datei importieren?......................................................................................... 124
Wie prüfe ich die Version von Wyse Management Suite.......................................................................................... 124
Wie Sie DHCP-Options-Tags erstellen und konfigurieren............................................................................................. 125
Wie Sie DNS-SRV-Einträge erstellen und konfigurieren............................................................................................... 126
Schritte zum Ändern des Hostnamens zur IP-Adresse................................................................................................. 127
Wie kann ich das Gerät mit einem selbstsignierten Remote-Repository abbilden?................................................. 127
Einführung in die Wyse Management Suite


Themen:

- Editionen von Wyse Management Suite
- Wyse Management Suite-Funktionsmatrix

Editionen von Wyse Management Suite

Wyse Management Suite ist in den folgenden Editionen erhältlich:


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

Die Pro Edition der Wyse Management Suite bietet außerdem:

- Erweiterte App-Richtlinie und -Berichterstellung

**ANMERKUNG:** Cloud-Dienste werden gehostet in den USA und Deutschland. Kunden in Ländern mit Beschränkungen bezüglich zulässiger Datenspeicheroorte 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**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hochgradig skalierbare Lösung zur Verwaltung von Thin Clients</td>
<td>Bis zu 10.000 Geräte freimachen</td>
<td>50.000 Geräte und mehr</td>
<td>1 Million Geräte und mehr</td>
</tr>
<tr>
<td>Lizenzschlüssel</td>
<td>Nicht erforderlich</td>
<td>Erforderlich</td>
<td>Erforderlich</td>
</tr>
<tr>
<td>Gruppenbasierte Verwaltung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Gruppen mit mehreren Ebenen und Vererbung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Konfigurationsrichtlinienverwaltung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Betriebssystempatch und Abbildverwaltung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Effektive Konfiguration auf Geräteebene nach Vererbung anzeigen</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Anwendungsrichtlinienverwaltung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Anlagen-, Bestands- und Systemverwaltung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Automatische Geräteermittlung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Echtzeit-Befehle</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Smart planen</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Warnungs-, Ereignis- und Überwachungsprotokolle</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Sichere Kommunikation (HTTPS)</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Verwalten von Geräten hinter einer Firewall</td>
<td>Eingeschränkt*</td>
<td>Eingeschränkt*</td>
<td>√</td>
</tr>
<tr>
<td>Mobile Anwendung</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Warnungen unter Verwendung von E-Mail und mobilen Anwendungen</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Scripting-Support für benutzerspezifische Anwendunginstallation</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Bundle-Anwendungen zur Vereinfachung der Bereitstellung und zum Minimieren von Neustarts</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Delegierte Verwaltung</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Dynamische Gruppenerstellung und - Zuweisung basierend auf Geräte-Attributen</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Zweifaktor-Authentifizierung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Active Directory-Authentifizierung für rollenbasierte Verwaltung</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Multi-Tenancy</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Berichterstellung der Unternehmensklasse</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Mehrere Repositorys</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Aktivieren/Deaktivieren von Hardware-Ports auf unterstützten Plattformen</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>BIOS-Konfiguration auf unterstützten Plattformen</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Konfiguration der Export- und Importrichtlinien</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Repository-Zuweisung zu einer Anwendungsrichtlinie</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Befehle zum Herunterfahren für Thin Clients</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Zeitüberschreitung der Wyse Management Suite-Konsole</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Richtlinien-Reihenfolge</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Auswahl der Anwendung gemäß dem Betriebssystem optimiert</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Option zum Konfigurieren eines Alias</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Subnetz-Zuordnung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Batch-Upload</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Konfiguration eines dynamischen Schemas</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Anmeldungsvalidierung</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Auswahlgruppe für ThinOS</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Wyse Management Suite-Repository</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

**ANMERKUNG:** *Das Sternchen zeigt an, dass Sie Geräte mit der Wyse Management Suite nur in einer sicheren Firewall-Umgebung verwalten können. Sie können Thin Clients nicht über den Anwendungsbereich der Firewall-Einstellungen hinaus verwalten.*
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 Management Console
- Konfigurieren und Verwalten von Thin Clients
- Wyse-Geräte-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
   - EU-Rechenzentrum – eu1.wysemanagementsuite.com/ccm-web
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

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.


Ändern Ihres Kennworts

So ändern Sie Ihr Anmeldekennwort:

2. Klicken Sie auf Kennwort ändern.

Abmelden

So melden Sie sich bei der Managementkonsole ab:

2. Klicken Sie auf Abmelden.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>GUID-4C9EFBA1-783A-4B54-A183-08D9C00B3D70</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2</td>
</tr>
<tr>
<td>Status</td>
<td>Translation in review</td>
</tr>
</tbody>
</table>

Voraussetzungen für Wyse Management Suite in einer Private Cloud

Tabelle 2. Vorbedingungen

<table>
<thead>
<tr>
<th>Beschreibung</th>
<th>10 000 Geräte oder weniger</th>
<th>50 000 Geräte oder weniger</th>
<th>120 000 Geräte oder weniger</th>
<th>Wyse Management Suite – Software-Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unterrichtete Sprachpakete: Englisch, Französisch, Italienisch, Deutsch, Spanisch, Japanisch und Chinesisch (Vorschau-Version)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mindest-Festplattenspeicherplatz</td>
<td>40 GB</td>
<td>120 GB</td>
<td>200 GB</td>
<td>120 GB</td>
</tr>
<tr>
<td>Mindest-Arbeitsspeicher (RAM)</td>
<td>8 GB</td>
<td>16 GB</td>
<td>32 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>Minimale CPU-Anforderungen</td>
<td>4</td>
<td>4</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>• TCP 443 – HTTPS-Kommunikation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TCP 1883 – MQTT-Kommunikation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TCP 3306 – MariaDB (optional, wenn Remote)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TCP 27017 – MongoDB (optional, wenn Remote)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TCP 11211 – Memcache</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TCP 5172, 49159 – End-User Management Software Development Kit (EMSDK) – optional und nur für Teradici Geräte erforderlich</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Die Standardschnittstellen, die vom Installationsprogramm verwendet werden, können im Rahmen der Installation zu einem alternativen Port geändert werden.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unterstützte Browser</td>
<td>Internet Explorer Version 11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google Chrome, Version 58.0 und höher</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox, Version 52.0 und höher</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edge-Browser unter Windows – nur in englischer Sprache</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


### Funktionsbereiche der Management Console

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 **Apps & Daten** ermöglicht die Verwaltung von Geräteeinstellungen, Betriebssystemabbildern, Richtlinien, Zertifikateabbildern, Logos und Hintergrundbildern.
- Die Seite **Regeln** ermöglicht die Erstellung von Geräteeinstellungen, Betriebssystemabbildern, Richtlinien, Zertifikateabbildern, Logos und Hintergrundbildern.
- Die Seite **Jobs** ermöglicht die Verwaltung von Geräteeinstellungen, Betriebssystemabbildern, Richtlinien, Zertifikateabbildern, Logos und Hintergrundbildern.
- Die Seite **Ereignisse** ermöglicht das Anzeigen und Überprüfen von Systemereignissen und Warnungen.
- Die Seite **Portalverwaltung** ermöglicht die Konfiguration verschiedener Systemeinstellungen, wie die Konfiguration des lokalen Repositories, Lizenzabonnements, Active Directory-Konfiguration und Zwei-Faktor-Authentifizierung.

### Konfigurieren und Verwalten von Thin Clients


**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 Gerätattributen wie z. B. Subnetz, Zeitzone und Standort. Sie können auch Folgendes konfigurieren:

Beispiel:
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:

- Gerätbestand
- Berichte
- Mobile-Anwendung


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.


Die Seite Gerätedetails enthält außerdem die 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.


Einzelheiten für das Gerät werden angezeigt.

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.


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:

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.


• **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.
Installieren oder Aktualisieren von Wyse Geräte-Agent


- Manuelles Installieren von Wyse Geräte-Agent
- Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie


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:** Sie können auch den Wyse Geräte-Agent manuell aktualisieren, indem Sie auf die neueste Version der Wyse Geräte-Agent-.exe-Datei doppelklicken.

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

Voraussetzungen

Schritte


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


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


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 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.
   - ANMERKUNG: Sie können die Geräte auch mit einer der folgenden Methoden registrieren:
4. Konfigurieren Sie den Thin Client mit einer der folgenden Optionen:
Registrieren und Konfigurieren eines neuen ThinOS-8.x-Geräts mithilfe von Wyse Management Suite

Schritte

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.
   Um die CA-Validierungsoption in der Private Cloud zuaktivieren, 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.
7. Klicken Sie auf OK.

Das Gerät wird in der Wyse Management Suite registriert.

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

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.


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.


Es wird ein Benachrichtigungsfenster angezeigt.

7. Klicken Sie auf OK.

8. Klicken Sie im Fenster Zentrale Konfiguration auf OK.

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

- Ein Benutzer der Wyse Management Suite kann über das Backend-Portal die Geräte manuell verwalten.

Das Gerät wird in der Wyse Management Suite registriert.


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


Identifer | GUID-C2E18382-6533-4C7D-8F3E-FCB9FFD98E70
Version | 1
Status | Translation approved

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.


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

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

Schrifte
1. Installieren Sie den Wyse Geräte-Agent auf Ihrem Thin Client – siehe Installieren oder Aktualisieren des Wyse Geräte-Agent.

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

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

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

**Abbildung 1. Dashboard**

**Themen:**

- Anzeigen von Warnungen
- Anzeigen der Ereignisliste
- Anzeigen des Gerätestatus
- Aktivieren der Anmeldungsvalidierung
- 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

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


Anzeigen des Gerätestatus

Der Abschnitt Anzeige enthält die Zusammenfassung der Gerätestatus.

Schritte

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 Anmeldungsvalidierung

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 Anmeldungsvvalidierung. Sie werden auf der Seite Portalverwaltung auf die Option Andere Einstellungen umgeleitet.
3. Aktivieren oder Deaktivieren der Option Anmeldungsvvalidierung.

Identifier GUID-33F6F7DA-92D4-44C6-BF29-688C0310654A
Version 1
Status Translation approved

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.
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.

Identifier GUID-AA80F2E8-9CC5-48FE-8468-D141E799E6F
Version 1
Status Translation approved

Zugriff auf die Onlinehilfe

Schritte
1. In der rechten oberen Ecke der Seite Dashboard klicken Sie auf die Anmeldungs-Dropdownliste.

Identifier GUID-B47AF88F-2EED-4997-B0E6-48183ADC921B
Version 1
Status Translation approved

Ändern Ihres Kennworts

Schritte
1. In der rechten oberen Ecke der Seite Dashboard klicken Sie auf die Anmeldungs-Dropdownliste.
3. Geben Sie das aktuelle Kennwort ein.
4. Neues Kennwort eingeben.
5. Geben Sie das neue Kennwort zur Bestätigung erneut ein.
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


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

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


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 Standardrichtlinien der Gruppe unterscheiden.


**ANMERKUNG:**


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.

**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:

- Global
- Gruppe
- Gerät
Abbildung 2. Gruppen und Konfigurationen

Themen:
- Bearbeiten einer nicht verwalteten Gruppe
- Erstellen einer Standard-Geräterichtliniengruppe
- Entfernen einer ThinOS-Auswahlgruppe
- Konfigurieren von Richtlinien der Globalen Klasse
- Erstellen einer Nutzerrichtliniengruppe
- Bearbeiten der Nutzerrichtliniengruppe
- Importieren einer Nutzerrichtliniengruppe
- Importieren einer Nutzerrichtliniengruppe aus dem Active Directory
- 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 einer nicht verwalteten Gruppe

Geräte, die der nicht verwalteten Gruppe angehören, verwenden keine Lizenzen oder empfangen Konfigurationen oder anwendungsbasierter Richtlinien. Zum Hinzufügen von Geräten zu einer nicht verwalteten Gruppe verwenden Sie den Geräteregistrierungsschlüssel 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.
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.

Identifier: GUID-FFC489B7-6F43-4A6D-B722-5A1CAEE9F021
Version: 2
Status: Translation approved
Erstellen einer Standard-Geräterichtliniengruppe

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

Schritte
2. Klicken Sie auf .
3. Im Dialogfeld Neue Gruppe hinzufügen geben Sie Gruppenname, Beschreibung, Domain und AD-Attributname ein.
   - **ANMERKUNG:** Wählen Sie die Option Dies ist eine übergeordnete ThinOS-Auswahlgruppe aus, um eine übergeordnete Auswahlgruppe für ThinOS-Geräte zu erstellen. Weitere Informationen finden Sie unter Erstellen einer ThinOS-Auswahlgruppe.
4. Aktivieren Sie auf der Registerkarte Registrierung das Kontrollkästchen Aktiviert unter Gruppentoken.
5. Geben Sie das Gruppentoken ein.
   - **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
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.
   - **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**.
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 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.
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.

Erstellen einer Nutzerrichtliniengruppe

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

**Schritte**
2. Klicken Sie auf .
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.
   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.
   **ANMERKUNG:** 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 .
Importieren einer Nutzerrichtliniengruppe

**Schritte**

1. Klicken Sie auf der Seite **Gruppen und Konfigurationen** auf die Option **Standard-Nutzerrichtliniengruppe**.
2. Klicken Sie auf .
3. Navigieren Sie im Dialogfeld **Massenimport** zu der .csv-Datei.
   Die .csv-Datei muss die Details in der folgenden Reihenfolge enthalten:
   - Gruppenname
   - Beschreibung
   - Domain
   - AD-Attribut
   - AD-Attributname
4. Klicken Sie auf Importieren.

Importieren einer Nutzerrichtliniengruppe aus dem Active Directory

**Schritte**

1. Melden Sie an der Private Cloud der Wyse Management Suite an.
2. Gehen Sie zu **Portaladministrator > Konsoleinstellungen > Active Directory**.
3. Klicken Sie auf die Registerkarte **AD-Informationen**.
4. Klicken Sie auf .
5. Wählen Sie **AD-Nutzergruppe** unter **AD-Authentifizierung und einmaliger Import** aus und klicken Sie auf **Gruppe importieren**.
   Sie können die Nutzerrichtliniengruppen sehen, die auf der Registerkarte **Standard-Nutzerrichtliniengruppe** auf der Seite **Gruppen und Konfigurationen** erstellt werden.

   **ANMERKUNG:** Sie müssen die Benutzeroberfläche des Remote-Repositories verwenden, um Nutzerrichtliniengruppen aus Active Directory in der Public Cloud zu 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 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 der gelöschten Gruppe angehörten, in eine ausgewählte Gruppe verschoben.

Konfigurieren von Richtlinien der Geräteklasse

Schritte
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.
3. Wählen Sie die zu exportierenden Gerätetyprichtlinien aus. Die folgenden Optionen stehen zur Verfügung:
   - Alle Gerätetyprichtlinien: Alle Gerätetyp-Richtlinien werden exportiert.
4. Klicken Sie auf die Schaltfläche Ja, um die ausgewählten Gerätetyprichtlinien 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.

Importieren von Gruppenrichtlinien

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 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.

   Eine Vorschau der Richtlinien in der ausgewählten Gruppe wird angezeigt.

   Die Zusammenfassung des Importvorgangs wird angezeigt. Die folgenden Arten von Warnungen können angezeigt werden:
   - Importierte <Betriebssystemtyp>-Richtlinien werden auf die Gruppe <Gruppenname> angewendet: 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: wenn Sie neue Betriebssystemtypkonfigurationen in eine Gruppe importieren, die die Betriebssystemtypkonfigurationen enthält.
   - Das Importieren von Richtlinien aus einer Datei, die Abhängigkeiten enthält, in Bestandsaufnahmedateien schlägt fehl. Um diesen Import zu ermöglichen, verwenden Sie die Importoption aus dem Fenster "Richtlinien bearbeiten": wenn Sie die Gerätetypkonfigurationen aus einer Datei importieren, die Verweise auf Bestandsaufnahmedateien enthält.

8. Klicken Sie auf Importieren.

Anmerkung: Nur die ausgewählten Gerätetypkonfigurationen können importiert werden und Richtlinien, die in der Zielgruppe für den ausgewählten Gerätetyp definiert sind, werden entfernt, bevor Sie die neuen Richtlinien desselben Gerätetyps anwenden.

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

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.
   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 exportierten Datei – suchen Sie die Datei .JSON. 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.
   - Importierte <Gerätetyp>-Richtlinien werden auf die Gruppe <Gruppenname> angewendet: 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 – wenn Sie die Gerätetypkonfigurationen in eine Gruppe importieren, die die Gerätetypkonfigurationen enthält.
   - Das Importieren von Richtlinien aus einer Datei, die Abhängigkeiten enthält, in Bestandsaufnahmedateien schlägt fehl. Um diesen Import zu ermöglichen, verwenden Sie die Importoption aus dem Fenster "Richtlinien bearbeiten": wenn Sie die Gerätetypkonfigurationen aus einer Datei importieren, die Verweise auf Bestandsaufnahmedateien enthält.
7. Klicken Sie auf Importieren.

**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 exportierende Datei über eine Referenz oder eine Abhängigkeitsdatei verfügt, gehen Sie zu der Seite Richtlinie bearbeiten des jeweiligen Gerätetyps und importieren Sie dann die Gruppenrichtlinien.

**Ergebnisse**

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

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

**Identifier** GUID-BF1868D8-7F12-4544-9654-ED94F29A6F1D
**Version** 1
**Status** Translation approved

#### 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
   **ANMERKUNG:** Zum Einstellen der Erweiterten ThinOS-Konfiguration als Standardmodus, wählen Sie das Kontrollkästchen aus.
   **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.

3. Klicken Sie auf die Option Erweitert.

Abbildung 3. Erweiterte Option

4. Wählen Sie die Optionen aus, die Sie konfigurieren wollen.

   ANMERKUNG: Die Unterstützung der BIOS-Einstellungen wurde der Wyse Management Suite 2.1 hinzugefügt.

5. Klicken Sie in den entsprechenden Feldern auf die Option, die Sie konfigurieren möchten.

6. Konfigurieren Sie die Optionen nach Bedarf.


   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


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

Schritte


2. Klicken Sie im Dropdownmenü Richtlinien bearbeiten auf ThinOS 9.x.


4. Klicken Sie im Feld BIOS auf Plattform auswählen, um die Plattform auszuwählen, auf der Sie die BIOS-Einstellungen konfigurieren möchten.
Hochladen und Pushen von OS-Paketen

Voraussetzungen

- Registrieren des Thin Clients bei der Wyse Management Suite

Schritte

1. Navigieren Sie zur Seite Gruppen & Konfigurationen und wählen Sie eine Gruppe aus.
4. Wählen Sie im Feld Firmware die Option OS-Firmware-Updates aus.

Hochladen und Pushen von BIOS-Paketen

Voraussetzungen

- Registrieren des Thin Clients bei der Wyse Management Suite

Schritte

1. Navigieren Sie zur Seite Gruppen und Konfigurationen und wählen Sie eine Gruppe aus.
4. Wählen Sie im Feld Firmware die Option BIOS-Firmware-Updates aus.
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 hinzufügen, 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 der Wyse Management Suite

Voraussetzungen
- 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.
4. Klicken Sie im Feld Firmware auf Anwendungspaket-Updates.
5. Wählen Sie das Paket aus dem Dropdownmenü zur Bereitstellung von ThinOS-Paket (s) auswählen aus.
   **ANMERKUNG:** Sie können mehrere Firmware-Pakete aus dem Remote-Repository, dem Mandanten-Cloud-Repository oder dem Operator-Cloud-Repository hochladen und bereitstellen.
   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.

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.
Bearbeiten der Einstellungen für die ThinLinux-Richtlinie

Schritte
2. Klicken Sie auf die Dropdownliste Richtlinien bearbeiten.

Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen

Schritte
2. Klicken Sie auf die Dropdownliste Richtlinien bearbeiten.

Bearbeiten der Einstellungen für die Cloud Connect-Richtlinieneinstellungen

Schritte
2. Klicken Sie auf die Dropdownliste Richtlinien bearbeiten.
Verwalten von Geräten


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


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 4. 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 Gerätestatus
- Sperren der Geräte
- Neustart der Geräte
- Registrierung eines Geräts aufheben
- Anmeldungsvollständigkeit
- Gerät auf Werkseinstellungen zurücksetzen
- Ändern einer Gruppenzuweisung auf der Seite „Geräte“
- Senden von Meldungen an ein Gerät
- Aktivieren eines Geräts
- Anzeigen der Gerätedetails
- Verwalten der Gerätezusammenfassung
- Anzeigen von Systeminformationen
- Anzeigen von Geräteereignissen
- Anzeigen installierter Anwendungen
- Umbenennen des Thin Client
- Konfigurieren von Remote-Spiegelung-Verbindung
- Herunterfahren von Geräten
- Hinzufügen eines Tags zu einem Gerät
- Compliance-Status des Geräts
- Pull für Windows Embedded Standard oder ThinLinux-Aufbau ausführen
- Anfordern einer Protokolldatei
- Fehlerbehebung auf Ihrem Gerät
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 von ThinOS-Geräten mit dem Wyse Geräte-Agenten

So registrieren Sie ThinOS Geräte manuell:

**Schritte**

2. Klicken Sie auf die Registerkarte WDA. Der WDA-Dienst wird automatisch ausgeführt, sobald der Client-Startprozess abgeschlossen ist. WMS ist standardmäßig ausgewählt.
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.

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.
  - CCM-Server – eu1.wysemanagementsuite.com
  - MQTT-Server – eu1-pns.wysemanagementsuite.com:1883
Eine Warnmeldung wird angezeigt, wenn die Serveradresse „http“ enthält. Sie müssen zum Bestätigen auf OK klicken.


**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.


**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.


---

### 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.

---

44 Verwalten von Geräten
2. Geben Sie die Geräteregistrierungsinformationen ein.
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.


Nachdem die Registrierung abgeschlossen ist, wird die Meldung An Wyse Management Suite registriert angezeigt.

Identifikator: GUID-7649FF26-0BA4-4037-8637-92808E7611CA
Version: 1
Status: Translation approved

**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.
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.

Identifikator: GUID-16BFD811-8B57-45C2-991C-D901E5E22266
Version: 1
Status: Translation approved

**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 NMS 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-Validierungssoption die folgenden INI-Parameter ein:
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:
   
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Werte</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMSEnable</td>
<td>yes/n</td>
</tr>
<tr>
<td>WMSServer</td>
<td><a href="https://FQDN">https://FQDN</a> of the WMS Server:Port &lt;By default 443 is used&gt;</td>
</tr>
<tr>
<td>GroupRegistrationKey</td>
<td>GroupToken present in WMS Server</td>
</tr>
<tr>
<td>CAValidation</td>
<td>True/False</td>
</tr>
</tbody>
</table>

   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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Werte</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMSEnable</td>
<td>yes/n</td>
</tr>
<tr>
<td>WMSServer</td>
<td><a href="https://ServerFQDN.domain.com:443">https://ServerFQDN.domain.com:443</a></td>
</tr>
<tr>
<td>GroupRegistrationKey</td>
<td>defa-defadefa</td>
</tr>
<tr>
<td>CAValidation</td>
<td>True</td>
</tr>
</tbody>
</table>

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.

   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
   - 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 aktiver 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.
   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.

Registering devices by using DHCP option tags
Sie können Geräte mithilfe der folgenden DHCP-Options-Tags registrieren:

Tabelle 3. Registrieren von Geräten mithilfe von DHCP-Options-Tags

<table>
<thead>
<tr>
<th>Options-Tag</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datentyp – Zeichenfolge</td>
<td></td>
</tr>
<tr>
<td>Code – 165</td>
<td></td>
</tr>
<tr>
<td>Beschreibung – WMS-Server-FQDN</td>
<td></td>
</tr>
<tr>
<td>Name – MQTT</td>
<td>Dieses Tag leitet das Gerät zum Wyse Management Suite-Pushbenachrichtigungsserver (PNS) weiter. Bei einer Installation in einer privaten</td>
</tr>
<tr>
<td>Datentyp – Zeichenfolge</td>
<td></td>
</tr>
<tr>
<td>Code – 166</td>
<td></td>
</tr>
</tbody>
</table>
### Tabelle 3. Registrieren von Geräten mithilfe von DHCP-Options-Tags (fortgesetzt)

<table>
<thead>
<tr>
<th>Options-Tag</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Datentyp – Zeichenfolge</strong></td>
<td><strong>Code</strong> – 167</td>
</tr>
<tr>
<td><strong>Beschreibung – Zertifizierungsstellenprüfung</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Datentyp – Zeichenfolge</strong></td>
<td><strong>Code</strong> – 199</td>
</tr>
<tr>
<td><strong>Beschreibung – Gruppentoken</strong></td>
<td></td>
</tr>
</tbody>
</table>

**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 Geräte-Registrierung 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 4. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags

<table>
<thead>
<tr>
<th>URL/Tag</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Eintrags-FQDN</strong></td>
<td><strong>– _WMS_MGMT</strong></td>
</tr>
<tr>
<td><strong>– <em>WMS_MGMT</em>.tcp.&lt;Domänenname&gt;</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Eintragstyp</strong></td>
<td><strong>– SRV</strong></td>
</tr>
</tbody>
</table>
### Tabelle 4. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags (fortgesetzt)

<table>
<thead>
<tr>
<th>URL/Tag</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Eintrags-FQDN</strong> – _WMS_MQTT._tcp.&lt;Domänenname&gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Eintragstyp</strong> – SRV</td>
<td></td>
</tr>
<tr>
<td><strong>ANMERKUNG:</strong> Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird.</td>
<td></td>
</tr>
</tbody>
</table>

| **Eintragsname** – _WMS_GROUPTOKEN | Dieser Datensatz ist erforderlich, um ThinOS-Geräte in der Wyse Management Suite in einer öffentlichen oder privaten Cloud zu registrieren. |
| **Eintragstyp** – TEXT |                                                                                                                                             |
| **ANMERKUNG:** Das Gruppentoken ist optional für die neueste Version von Wyse Management Suite in einer privaten Cloud. |

| **Eintragstyp** – TEXT | Geben Sie **Falsch** ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server nicht von einer bekannten Zertifizierungsstelle importiert haben. |
| **ANMERKUNG:** CA Validation ist bei der neuesten Version der Wyse Management Suite optional. |
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
     - Anmeldungvalidierung 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
4. Wählen Sie aus der Dropdownliste **OS-Subtyp** einen Subtyp für Ihr Betriebssystem aus.
5. Wählen Sie eine Plattform aus der Dropdownliste **Plattform** aus.
7. Wählen Sie aus der Dropdownliste **Agentversion** eine Agentversion.
8. Wählen Sie aus der Dropdownliste **Subnetz** 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.

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 **Namens** 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.

   
   Es wird ein Fenster mit einer Warnung angezeigt.

5. Klicken Sie auf Befehl senden zum Senden des Abfragebefehls.

Sperren der Geräte

Sie können einen Befehl senden, um das registrierte Gerät zu sperren.

**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.

   
   Es wird ein Fenster mit einer Warnung angezeigt.


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.

   
   Es wird ein Fenster mit einer Warnung angezeigt.


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 Geräte angezeigt.
2. Wenden Sie die Filter an, um das bevorzugte Gerät zu finden.
3. Aktivieren Sie das Kontrollkästchen für das Gerät.
   Es wird ein Fenster mit einer Warnung angezeigt.
5. Aktivieren Sie das Kontrollkästchen Aufhebung der Registrierung erzwingen.


**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.


**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 Geräte im Status Validierung 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 Anmeldung validieren 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.
Gerät auf Werkseinstellungen zurücksetzen

Sie können einen Befehl senden, um Ihr Gerät auf die werkseitigen Standard-einstellungen 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 **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 **Nachricht senden** aus.
   Der Bildschirm **Nachricht senden** wird angezeigt.
5. Geben Sie die Nachricht ein.
6. Klicken Sie auf **Senden**.
Aktivieren eines Geräts

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.
   Die Seite **Gerätedetails** wird angezeigt.

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 Geräterichtlinie 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.
   Die Seite Gerätedetails wird angezeigt.
   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.
   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.
   Die Seite Gerätedetails wird angezeigt.
4. Klicken Sie auf der 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


**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.

### Konfigurieren von Remote-Spiegelung-Verbindung


**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)


### Herunterfahren von Geräten


**Schritte**

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


**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.**
   Die Seite **Gerät** wird 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 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.

### Schritte
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-Repositorys:
     - 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]
   
   **ANMERKUNG**: Sie können durch Bearbeiten der vorhandenen oder Standardvorlagen benutzerdefinierte Vorlagen verwenden, die manuell erstellt wurden.


### 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:


  ![Anmerkung]
  
  **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

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

### Schritte
2. Klicken Sie auf die Registerkarte Geräteprotokoll.
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:** Linux oder ThinLinux lädt die Protokolldatei im `.tar`-Format hoch. Wenn Sie die Dateien auf Windows oder auf einem ThinOS-9.x-System extrahieren möchten, müssen Sie 7zip oder eine andere entsprechende Datei abrufen.

---

**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**.
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.

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.


In der Private Cloud werden jedoch alle Repositories als Mandanten-Repository angezeigt, bei dem es sich um das lokale Repository handelt.

Abbildung 5. Seite „Apps und Daten“

Themen:

- Anwendungsrichtlinie
- Abbildrichtlinie
**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 Benutzeraufgaben 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.


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

<table>
<thead>
<tr>
<th>Identifier</th>
<th>GUID-43CC8F3D-0E9D-4884-BD5F-F176903A173E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Status</td>
<td>Translation approved</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>GUID-BA9990EA-0CF1-4753-B6EA-A6D4D2D2864E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Status</td>
<td>Translation approved</td>
</tr>
</tbody>
</table>

**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 **Richtlinienname** 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.
10. 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.

62  Anwendungen und Daten
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 in eine ausgewählte Gruppe verschoben wird.
- Richtlinie beim Check-In-Vorgang auf Geräte anwenden – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet.

**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 Anwendungs-Installation gilt nur für Windows-eingebettete Standard-, Wyse Software Thin Clients-, Linux- und Thin Linux-Geräte.


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.
- 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.


**Erstellen und Bereitstellen von Standardanwendungsrichtlinie auf 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.


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.


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 in eine ausgewählte Gruppe verschoben wird.
- **Richtlinie beim Check-In-Vorgang auf Geräte anwenden** – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet.

**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.
- **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.


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

<table>
<thead>
<tr>
<th>Identifier</th>
<th>GUID-B517ED2A-D3AB-4E5D-9AC9-E815E6ED6373</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Status</td>
<td>Translation approved</td>
</tr>
</tbody>
</table>

**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:
  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`. 64 Anwendungen und Daten
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf 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 > Thin Client und überprüfen Sie, ob die Anwendung registriert ist.
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.

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 folgenden Dropdwnmenüs aktiviert:
   - Wählen Sie aus der Dropdownliste Max. Anzahl an Stunden pro Verzögerung die maximale Anzahl Stunden (1 bis 24 Stunden) aus, um die die Ausführung der Richtlinie 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 in eine ausgewählte Gruppe verschoben wird.
   - Richtlinie beim Check-In-Vorgang auf Geräte anwenden – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet.

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
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.
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 softwareTcApps im lokalen Repository oder dem Wyse Management Suite-Repository.
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.

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 Anwendungdateien 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 Stunden (1 bis 24 Stunden) aus, um die die Ausführung der Richtlinie 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 in eine ausgewählte Gruppe verschoben wird.
- Richtlinie beim Check-In-Vorgang auf Geräte anwenden – Die Richtlinie wird automatisch beim Check-in auf Geräte angewendet.


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: 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


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.
- 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.


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

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

Voraussetzungen

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**.


---

**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**.

Hinzufügen von ThinOS-Paketdatei zu Repository

Schritte
1. Klicken Sie in der Registerkarte Apps & Daten unter OS-Abbild-Repository auf ThinOS.
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.

Hinzufügen von ThinOS-9.x-Firmware zum Repository

Schritte
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.


Hinzufügen von ThinOS-9.x-Paketdatei zu Repository

Schritte
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

Schritte
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-Aufnahme 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.

Verwalten eines Datei-Repositorys


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.
3. Um eine Datei auszuwählen, klicken Sie auf Durchsuchen und wechseln Sie zum Speicherort, an dem sich die Datei befindet.
4. 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

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

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

**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.

6. Klicken Sie auf Hochladen.

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

**Schritte**

1. Navigieren Sie zur Registerkarte **Apps & Daten**.
2. In der Navigationsleiste wählen Sie im linken Fenster **Bestand**.
3. Klicken Sie auf die Schaltfläche **Datei hinzufügen**.
4. Navigieren Sie zum Bild, das Sie als Hintergrundbild verwenden möchten, und wählen Sie es aus.
5. Als Typ wählen Sie **Hintergrundbild**.
6. 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:

1. Navigieren Sie zur Seite **Gruppen & Konfiguration**.
2. Wählen Sie eine Richtliniengruppe aus.
3. Klicken Sie auf **Richtlinien bearbeiten** und wählen Sie WES.
4. Wählen Sie **Desktop-Erlebnis** und klicken Sie auf **Dieses Element konfigurieren**.
5. Wählen Sie **Desktop-Hintergrundbild** aus.
6. Wählen Sie aus der Dropdownliste die Hintergrundbild-Datei.
7. Klicken Sie auf **Speichern und Veröffentlichen**.

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 6. 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.
   Das Fenster Regel bearbeiten wird angezeigt.
   Sie können auch folgende Details anzeigen:
   - Regel
   - Beschreibung
   - Geräteziel
   - Gruppe
   **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.

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.
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.
   **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.

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) lösen.
   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 Verwaltungskonsole 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**
- **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 7. Seite „Jobs“

Themen:
• BIOS-Administratorkennwort synchronisieren
• Suchen eines geplanten Jobs mithilfe von Filtern
• Planen des Gerätebefehljobs
• Planen der Abbildrichtlinie
• Planen einer Anwendungsrichtlinie

BIOS-Administratorkennwort synchronisieren

Schritte
1. Klicken Sie auf Jobs.
2. Wählen Sie aus dem Dropdownmenü Weitere Maßnahmen die Option BIOS-Administratorkennwort synchronisieren.
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.
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.
Suchen eines geplanten Jobs mithilfe von Filtern

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

**Schritte**


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

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 Gerätebefehljobs

**Schrifte**

1. Klicken Sie auf der Seite Jobs auf **Gerätebefehljob planen**. Der Bildschirm **Gerätebefehljob** 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.
5. Wählen Sie aus der Dropdownliste den Gruppennamen aus.
7. Wählen Sie aus der Dropdownliste das Datum oder die Uhrzeit aus.
8. Geben 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.
10. Klicken Sie auf die nächste Seite auf die Option **Zeitplan festlegen** zum Einleiten des Jobs.

Planen der Abbildrichtlinie


**Schrifte**

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.
4. Wählen Sie aus der Dropdownliste das Datum oder die Uhrzeit aus.
5. Geben 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.
7. Klicken Sie auf die Option **Zeitplan festlegen** zum Initiieren des Jobs.
Planen einer Anwendungsrichtlinie


**Schritte**

2. Wählen Sie eine Richtlinie aus der Dropdownliste aus.
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.
Verwalten von Ereignissen

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


Abbildung 8. Seite „Ereignisse“

Themen:
- Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern
- Anzeigen einer Zusammenfassung der Ereignisse
- Anzeigen des Überwachungsprotokolls
Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern

Schritte
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
5. 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


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.

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

In diesem Abschnitt wird die Durchführung routinemäßiger Benutzerverwaltungsaufgaben in der Verwaltungskonsole beschrieben. Es gibt folgende zwei 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.

  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 bearbeiten
  - Benutzer aktivieren
  - Benutzer deaktivieren
  - Benutzer löschen

**ANMERKUNG:** Zum Importieren von Benutzern aus der .CSV-Datei klicken Sie auf Massenimport.
Abbildung 9. Seite „Benutzer“

Themen:

- Hinzufügen eines neuen Administratorprofils
- Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte
- Bearbeiten eines Administratorprofils
- Hinzufügen eines Endnutzers
- Bearbeiten eines Endnutzers
- Endnutzerausnahmen erstellen
- Massenimport von Endnutzern
- Endnutzer löschen
- Deaktivieren eines Administratorprofils
- Löschen eines Administratorprofils
- Bearbeiten eines Benutzerprofils
- Massenimport nicht zugewiesener Administratoren oder Cloud Connect-Nutzer

Identifikator: GUID-5777F5AD-C1B1-49D6-85AE-ACD5BD66ECA2
Version: 1
Status: Translation approved

Hinzufügen eines neuen Administratorprofils

Schritte

1. Klicken Sie auf Benutzer.
2. Klicken Sie auf Administrator(en).
   Das Fenster Neuer Administrator-Benutzer wird angezeigt.
5. Wählen Sie das Kontrollkästchen zur Verwendung des gleichen Benutzernamens, der in der E-Mail genannt wird.
6. Führen Sie eine der folgenden Aktionen aus:
Wenn Sie auf die Registerkarte **Persönliche Informationen** 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 Rollen die Option **Administratorrolle**.
   - Globaler Administrator
   - Gruppenadministrator
   - Viewer

   **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. Führen Sie im Abschnitt **Kennwort** die folgenden Schritte aus:
   i. Geben Sie das benutzerdefinierte Kennwort ein.
   ii. Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche **Zufälliges Kennwort generieren**.

7. 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**.


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.

   
   **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 **Persönliche Informationen** 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. Führen Sie im Abschnitt **Kennwort** die folgenden Schritte aus:
        i. Geben Sie das benutzerdefinierte Kennwort ein.
        ii. Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche **Zufälliges Kennwort generieren**.

6. Klicken Sie auf **Speichern**.

### Hinzufügen eines Endnutzers

**Schritte**

1. Klicken Sie auf die Registerkarte **Benutzer**.
2. Klicken Sie auf **Endnutzer**.
3. Klicken Sie auf **Benutzer hinzufügen**.
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**.
5. Klicken Sie auf **Speichern**.

### Endnutzerausnahmen erstellen

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:** Diese Funktion wird nur für Thin Clients unterstützt, auf denen ThinOS 9.x als Betriebssystem ausgeführt wird. Die Anzahl der Endnutzer in der On-Premise-Umgebung ist unbegrenzt. Sie können 10.000 Nutzer in einer Public 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. Klicken Sie auf **Importieren**.

**ANMERKUNG:** Sie können der Wyse Management Suite bis zu 100 Endnutzer hinzufügen.

---

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**.

---

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**.

---

Verwalten von Benutzern
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).
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.

Bearbeiten eines Benutzerprofils

**Schritte**
1. Klicken Sie auf Benutzer.
2. Klicken Sie auf Nicht zugewiesene Administratoren.
   Das Fenster Administratorbenutzer bearbeiten wird angezeigt.
   **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 Persönliche Informationen klicken, geben Sie die folgenden Details ein:
     o Vorname
     o Nachname
     o Titel
     o 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. Führen Sie im Abschnitt Kennwort die folgenden Schritte aus:
       i. Geben Sie das benutzerdefinierte Kennwort ein.
       ii. Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche Zufälliges Kennwort generieren.
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**.
Dieser Abschnitt enthält eine kurze Übersicht über die Systemverwaltungsaufgaben, die erforderlich sind, um das System einzurichten und zu verwalten.

Abbildung 10. Portaladministrator

Themen:
- Hinzufügen der Active Directory-Serverinformationen
- Importieren von nicht zugewiesenen Nutzern oder Nutzergruppen in die Public Cloud über Active Directory
- 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
Hinzufügen der Active Directory-Serverinformationen

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

Schritte

1. Melden Sie sich an der Private Cloud der Wyse Management Suite an.
2. Gehen Sie zu Portaladministrator > Konsoleinstellungen > Active Directory (AD).
5. Klicken Sie auf Speichern.
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 enthalten verwenden. Sie können 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.

10. Im Feld Suche geben Sie den Gruppenamen ein, den Sie auswählen möchten.
11. Wählen Sie eine Gruppe aus.
    Die ausgewählte Gruppe wird in den rechten Fensterbereich auf der Seite verschoben.


    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:

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:

2. Klicken Sie auf dem Anmeldebildschirm auf den Link Mit Ihren Domain-Anmeldeinformationen anmelden.
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-Verwaltungssystem anmelden.

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

1. Importieren Sie das AD-Domänen-Server-Stammsertifikat 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).

   **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).

   **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:

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

   b. Geben Sie die Einzelheiten der Instanz-ID und des X.509-Signierungs zertifikat in die entsprechenden Felder ein.

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

5. Klicken Sie auf Speichern.

**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

**Ergebnisse**

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

<table>
<thead>
<tr>
<th>Identifier</th>
<th>GUID-DCB4B1F3-3D25-4228-863D-72D4E02D6F81</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>4</td>
</tr>
<tr>
<td>Status</td>
<td>Translation in review</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>GUID-13685E54-031A-4874-9890-F2C81F9DD734</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Status</td>
<td>Translation approved</td>
</tr>
</tbody>
</table>

**Warnungsklassifizierungen**

Die Warnungsseite kategorisiert die Warnungen als Krisch, 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. Krisch, Warnung oder Info für die folgenden Warnungen:
- Warnung über Gerätezustand
- Gerät nicht eingecheckt

<table>
<thead>
<tr>
<th>Identifier</th>
<th>GUID-0C6DFDD3-89CB-47E9-8A7C-58E5D602FA37</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2</td>
</tr>
<tr>
<td>Status</td>
<td>Translation approved</td>
</tr>
</tbody>
</table>

**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 Anwendungsdienstes 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:


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

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

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

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


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

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 Geräteinformationenbefehl an das Gerät zu senden.
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.


### Identifier
GUID-7D43A4A1-E157-42F4-8E89-8385ED37971

### 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.


### Konfigurieren der Subnetz-Zuordnung
**Schritte**

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

![Abbildung 11. Datei-Repository](image)

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.

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.
- **Taktintervall** – Geben Sie die Zeit ein. Das Gerät sendet alle 60 bis 360 Minuten ein Taktsignal.
- **Check-in-Intervall** – Geben Sie 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.

Verwalten von Teradici-Konfigurationen

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

**Schritte**

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.
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.


Aktivieren von Multi-Tenant Konten


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


Schritte

2. Klicken Sie auf die Option Bericht generieren.
   Das Fenster Bericht generieren wird angezeigt.
3. Wählen Sie aus der Dropdownliste Typ den Berichtstyp aus.
5. Wählen Sie das Trennzeichen aus.

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

2. Klicken Sie auf [Benutzerdefiniertes Branding aktivieren].

   Die maximale Größe des Kopfzeilenlogos beträgt 500 x 50 Pixel.

   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].

**Identifier** | GUID-FD506A7F-45B9-4EB5-B657-EFE39FD73139
---|---
**Version** | 5
**Status** | Translation in review

### 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.


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].
4. Geben Sie die folgenden Details im Bereich [SMTP für E-Mail-Warnungen aktualisieren] ein:
   - SMTP-Server
   - Von Adresse senden
   - Benutzername
   - Kennwort
   - Testadresse


5. Wählen Sie die folgenden Optionen aus und geben Sie die Einzelheiten ein:
6. Um die Details für externen MQTT zu aktualisieren, klicken Sie auf die Option [Externen MQTT ändern] und konfigurieren Sie die Informationen.

**Identifier** | GUID-FD506A7F-45B9-4EB5-B657-EFE39FD73139
---|---
**Version** | 5
**Status** | Translation in review
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**.
Teradici-Geräteverwaltung


Themen:
- Ermittlung von Teradici-Geräten
- CIFS-Anwendungsszenarien

Ermittlung von Teradici-Geräten

Vorbedingungen
- 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 vertrauenswürdiges 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 5. Zertifikatsanforderungen für Endpunkte

<table>
<thead>
<tr>
<th>Erkennungsmethode</th>
<th>Niedrige Sicherheit</th>
<th>Mittlere Sicherheit</th>
<th>Hohe Sicherheit</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP/DNS-Ermittlung ohne Bereitstellung eines EBM-Fingerabdrucks</td>
<td>Zertifikat erforderlich</td>
<td>Zertifikat erforderlich</td>
<td>Nicht zutreffend</td>
</tr>
<tr>
<td>DHCP/DNS-Ermittlung mit Bereitstellung eines EBM-Fingerabdrucks</td>
<td>Zertifikat nicht erforderlich</td>
<td>Zertifikat erforderlich</td>
<td>Nicht zutreffend</td>
</tr>
<tr>
<td>Ermittlung durch einen Endpunkt ausgelöst, der für eine</td>
<td>Nicht zutreffend</td>
<td>Nicht zutreffend</td>
<td>Zertifikat erforderlich</td>
</tr>
</tbody>
</table>
Tabelle 5. Zertifikatsanforderungen für Endpunkte (fortgesetzt)

<table>
<thead>
<tr>
<th>Erkennungsmethode</th>
<th>Niedrige Sicherheit</th>
<th>Mittlere Sicherheit</th>
<th>Hohe Sicherheit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hochsicherheitsumgebung konfiguriert ist</td>
<td>Zertifikat nicht erforderlich</td>
<td>Nicht zutreffend</td>
<td>Nicht zutreffend</td>
</tr>
<tr>
<td>Manuelle Ermittlung durch den MC initiiert</td>
<td>Zertifikat nicht erforderlich</td>
<td>Nicht zutreffend</td>
<td>Nicht zutreffend</td>
</tr>
</tbody>
</table>

**Manuelle Ermittlung über den Client**

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.
8. Klicken Sie auf Anwenden und dann auf Weiter.

**Hinzufügen der PCoIP-Endpunkt-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.
4. Klicken Sie auf Hinzufügen, um eine neue DHCP-Anbieterklasse hinzuzufügen.
5. Geben Sie den PCoIP-Endpunkt in das Feld Anzeigename 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-Endpunkt 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-Endpunkt aus.
9. Klicken Sie auf OK, um die Einstellungen zu speichern.
10. Wählen Sie PCoIP-Endpunkt als Klasse Option aus und klicken Sie auf Hinzufügen.
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.
17. Gehen Sie zum Webbrowser des Clients.
18. Gehen Sie zu **Konfiguration > Verwaltung** und legen Sie den **Manager-Erkennungsmodus** auf **Automatisch** fest.

**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.
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:
   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.

**Erstellen eines SHA-256-Fingerabdrucks**

1. Starten Sie Mozilla Firefox.
2. Navigieren Sie zur Registerkarte **Erweiterte Optionen**.
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.

  **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.
    ▪ 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 die Option CIFS-Benutzeranmeldeinformationen konfigurieren ausgewählt ist (standardmäßig)
  ▪ Wenn die Option CIFS-Benutzeranmeldeinformationen konfigurieren mit der Option Verwenden eines vorhandenen Benutzers ausgewählt ist.
    3. Aktualisieren Sie den Benutzer für die Anmeldung beim Dienst auf den ausgewählten Benutzer.
  ▪ Wenn die Option CIFS-Benutzeranmeldeinformationen konfigurieren mit der Option Einen neuen Benutzer erstellen ausgewählt ist.
    3. Aktualisieren Sie den Benutzer für die Anmeldung beim Dienst auf den neu erstellten Benutzer.
• 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 Verwaltungskonsole 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 (öffentlich 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 Suite 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:
   - Benutzername
   - Kennwort
   - Rechenzentrum
   - Anzahl an TC-Plätzen
   - Anzahl der Edge Gateway & Embedded PC Plätzen
   - Anzahl der Wyse Software Thin 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 Suite in die private Cloud-Konsole der Wyse Management Suite:

**Schritte**
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**.
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**
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.
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.
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 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**.
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.

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.
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_Commandsxml/uncompress_OS_Recovery_CommandsXml 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 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.
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 ().
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.
12. Kopieren Sie das heruntergeladene Abbild (Datei 2.2.0.00_3040_merlin_16GB.exe) nach Laufwerk C:/wms/localrepo/repository/osimages/zoomed/.


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

17. Aktualisieren Sie die anderen erforderlichen Felder nach Bedarf, und klicken Sie auf Speichern.

18. Planen Sie den Job.


---

### 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:

<table>
<thead>
<tr>
<th>Plattform</th>
<th>ThinOS-Firmware-Abbild</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wyse 3040 Thin Client</td>
<td>A10Q_wnos</td>
</tr>
<tr>
<td>Wyse 5070 Thin Client mit Celeron-Prozessor</td>
<td>X10_wnos</td>
</tr>
<tr>
<td>Wyse 5070 Thin Client mit Pentium-Prozessor</td>
<td>X10_wnos</td>
</tr>
<tr>
<td>Wyse 5070 Extended Thin Client mit Pentium-Prozessor</td>
<td>X10_wnos</td>
</tr>
<tr>
<td>Wyse 5470 Thin Client</td>
<td>X10_wnos</td>
</tr>
<tr>
<td>Wyse 5470 All-in-One Thin Client</td>
<td>X10_wnos</td>
</tr>
</tbody>
</table>

---

### Hinzufügen von ThinOS-Firmware zum Repository

**Schritte**


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


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:** Das Abbild im komprimierten Ordner wird in einen gültigen Ordner extrahiert. Der Extrahierungsvorgang kann 10–15 Minuten dauern.
Die hochgeladene Firmware kann nur für das Upgrade von ThinOS 8.6 auf ThinOS 9.0 verwendet werden.


**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.

**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 v9.0.1136 auf dem Thin Client installiert haben.
- 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 Konfigurationsteuerelement | ThinOS wird angezeigt.


4. Wählen Sie im Feld Firmware die Option OS-Firmware-Updates aus.

5. Klicken Sie auf Durchsuchen, um die Firmware zu durchsuchen und hochzuladen.


   Der Thin Client lädt die Firmware herunter und startet sie neu. Die Firmware-Version wird aktualisiert.

Voraussetzungen

Die Anforderungen an den Server zum Installieren von Wyse Management Suite Repository-Software sind:

- 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. Laden Sie die Datei WMS_Repo.exe vom Dell Digital Locker herunter.
2. Melden Sie sich als Administrator an und installieren Sie die Datei WMS_Repo.exe auf dem Repository-Server.
Abbildung 12. Registrierung – Details

5. Klicken Sie auf **Registrieren**, um die Registrierung zu starten. Wählen Sie **Im öffentlichen WMS Management Portal registrieren** für die Registrierung in der Public Cloud.
Abbildung 13. Registrieren in einer Public Cloud

6. Geben Sie die folgenden Details ein und wählen Sie **Registrieren**.
   a. Server-URL von Wyse Management Suite
   
   **ANMERKUNG**: Wenn Sie sich nicht für Wyse Management Suite v1.0 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. Passwort zum Anmelden des Administrators der Wyse Management Suite
   
   e. Repository-Pfadinformationen

7. Wenn die Registrierung erfolgreich ist, wird das **Registrierung** Fenster angezeigt.
Abbildung 14. Registrierung erfolgreich

8. Der folgende Bildschirm auf dem Wyse Management Suite Portal bestätigt die erfolgreiche Registrierung des Remote-Repositories:

Abbildung 15. Registrierung beim Portal erfolgreich

Abbildung 16. Zertifikat hochladen

10. Der Server wird neu gestartet und das hochgeladene Zertifikat wird angezeigt.
Abbildung 17. SSL-Zertifikat aktiviert


Abbildung 18. Truststore-Zertifikate


Themen:
- Verwalten des Wyse Management Suite Repository-Dienstes
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:
**Fehlerbehebung auf Ihrem Gerät**

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

**Schritte**

1. Klicken Sie auf der Seite **Gerätedetail** auf die Registerkarte **Fehlerbehebung**.
2. Klicken Sie auf **Screenshot anfordern**.
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.

**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.


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.
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-11D0-94F2-00A0C91EF8B8} for CD ROM : {53F56308-B6BF-11D0-94F2-00A0C91EF8B8}.

| ANMERKUNG | Geschweifte Klammern sind obligatorisch. |
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?

Schrifte

2. Nach dem Installationsprozess starten Sie die Anwendung.
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.


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 von Wyse Management Suite-Server nicht aktiviert ist, findet die Kommunikation zwischen Server und Client in einem sicheren Kanal ohne Validierung der Zertifikatssignatur statt.
   e. Fügen Sie einen Hinweis in dem angegebenen Feld hinzu.
   f. 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.
   - 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 Beispiel **WMSServerName.YourDomain.Com:443**.
   - 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
        - Beschreibung – CA-Validation
     b. Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
        - Zeichenfolge – WAHR/FALSCH
        Zum Beispiel **WMSServerName.YourDomain.Com**.
   - 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**.

Häufig gestellte Fragen
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.
5. Wählen Sie die Dienstidentifierung (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
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 \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: mongodb://127.0.0.1:27017/localhost
   • MongoDB-Serverversion: 3.4.10
5. Geben Sie Folgendes ein: `use stratus`
   Ausgabe: switched to db stratus
   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("5b97905e48b7b7e9ad22aa6"), "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?


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.
3. Übertragen Sie das Zertifikat mithilfe der Sicherheitsrichtlinie an die Zielclients oder Gruppen von Clients.
   Warten Sie, bis der Konfigurationsrichtlinienjob abgeschlossen ist.
5. Erstellen Sie eine Abbildrichtlinie und planen Sie die Gruppe.