

# Dell Wyse Management Suite

Version 1.4 Administratorhandbuch



## Anmerkungen, Vorsichtshinweise und Warnungen

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

<b>1 Einführung in die Wyse Management Suite.....</b>	<b>9</b>
Editionen.....	9
Was ist neu in dieser Version?.....	10
<b>2 Erste Schritte mit der Wyse Management Suite.....</b>	<b>11</b>
Anmeldung bei der Wyse Management Suite in einer öffentlichen Cloud.....	11
Ändern Ihres Kennworts.....	11
Abmelden.....	12
Voraussetzungen für Wyse Management Suite in einer privaten Cloud.....	12
Funktionsbereiche der Management Console.....	13
Konfigurieren und Verwalten von Thin Clients.....	13
<b>3 Wyse Management Suite-Dashboard.....</b>	<b>16</b>
Anzeigen von Warnungen.....	16
Anzeigen der Ereignisliste.....	17
Anzeigen des Gerätestatus.....	17
Ändern von Benutzereinstellungen.....	17
Zugriff auf die Onlinehilfe.....	17
Ändern Ihres Kennworts.....	18
Abmelden.....	18
<b>4 Verwalten von Gruppen und Konfigurationen.....</b>	<b>19</b>
Hinzufügen einer Gruppe.....	20
Bearbeiten einer Gruppe.....	21
Entfernen einer Gruppe.....	21
Bearbeiten einer nicht verwalteten Gruppe.....	21
Konfigurieren von Richtlinien der Globalen Klasse.....	22
Konfigurieren von Richtlinien auf Gruppenebene.....	22
Konfigurieren von Richtlinien der Geräteklasse.....	22
Gruppenrichtlinien exportieren.....	22
Gruppenrichtlinien importieren.....	23
Bearbeiten der Einstellungen für ThinOS-Richtlinien.....	24
ThinOS – Assistentenmodus.....	24
ThinOS – Erweiterter Modus.....	30
Bearbeiten von Windows Embedded Standard-Richtlinieneinstellungen.....	74
Konfigurieren der Systempersonalisierung.....	75
Desktop-Erfahrung konfigurieren.....	77
Konfigurieren der Netzwerkeinstellungen.....	78
Konfigurieren der Sicherheits- und Sperrmoduseinstellungen.....	78
Andere Einstellungen konfigurieren.....	78
Konfigurieren von Remote-Verbindungseinstellungen – Citrix.....	80
Konfigurieren von Remote-Verbindungseinstellungen – VMware.....	83
Konfigurieren von Remote-Verbindungseinstellungen – RDP.....	85

Konfigurieren von Remote-Verbindungseinstellungen – Browser.....	87
Konfigurieren der BIOS-Einstellungen für mobilen Latitude Thin Client.....	89
Wyse 7040 Thin Client BIOS-Einstellungen konfigurieren.....	91
Geräteinformationen konfigurieren.....	92
Konfigurieren von Wyse Easy Setup-Einstellungen.....	93
Konfigurieren der VNC-Einstellungen.....	95
Konfigurieren von Domäneneinstellungen.....	95
Konfiguration der BIOS-Einstellungen für Wyse 5070 Thin-Client mit Windows 10 IoT Enterprise.....	95
Konfiguration der BIOS-Einstellungen für Wyse 5470 All-in-One Thin-Client mit Windows 10 IoT Enterprise.....	98
Bearbeiten der Einstellungen für die Linux-Richtlinie.....	100
Konfigurieren der Systempersonalisierung.....	101
Desktop-Erfahrung konfigurieren.....	102
Konfigurieren von Anmeldeerlebnis-Einstellungen.....	103
Konfigurieren der Netzwerkeinstellungen.....	104
Konfigurieren der Sicherheitseinstellungen.....	104
Konfigurieren von zentralen Konfigurationseinstellungen.....	105
Andere Einstellungen konfigurieren.....	106
Konfigurieren von globalen VDI-Einstellungen.....	106
Konfigurieren von Remote-Verbindungseinstellungen – Citrix.....	108
Konfigurieren von Remote-Verbindungseinstellungen – VMware.....	110
Konfigurieren von Remote-Verbindungseinstellungen – RDP.....	112
Konfigurieren von Remote-Verbindungseinstellungen – Browser.....	114
Erweiterte Einstellungen konfigurieren.....	114
Bearbeiten der Einstellungen für die ThinLinux-Richtlinie.....	114
Konfigurieren der Systempersonalisierung.....	115
Desktop-Erfahrung konfigurieren.....	116
Konfigurieren des Anmeldeerlebnisses.....	117
Konfigurieren der Netzwerkeinstellungen.....	118
Konfigurieren der Sicherheitseinstellungen.....	118
Konfigurieren von zentralen Konfigurationseinstellungen.....	120
Andere Einstellungen konfigurieren.....	120
Konfigurieren von globalen VDI-Einstellungen.....	121
Konfigurieren von Remote-Verbindungseinstellungen – Citrix.....	123
Konfigurieren von Remote-Verbindungseinstellungen – VMware.....	125
Konfigurieren von Remote-Verbindungseinstellungen – RDP.....	128
Konfigurieren von Remote-Verbindungseinstellungen – Browser.....	130
Erweiterte Einstellungen konfigurieren.....	131
Geräteinformationen konfigurieren.....	131
Wyse 3040 Thin Client BIOS-Einstellungen konfigurieren.....	131
Konfiguration der BIOS-Einstellungen für Wyse 5070 Thin-Client mit ThinLinux.....	134
Konfigurieren der globalen Browsereinstellungen.....	137
Konfigurieren von Proxy-Einstellungen.....	138
Bearbeiten von Teradici-Richtlinieneinstellungen.....	138
Konfigurieren von Zeitzoneneinstellungen.....	139
Konfigurieren von Spracheinstellungen.....	139
Konfigurieren von Firmenlogo-Einstellungen.....	140

Konfigurieren von Videoeinstellungen.....	140
Konfigurieren der Energieeinstellungen.....	141
Konfigurieren der Sicherheitseinstellungen.....	141
Upgrade der Firmware-Einstellungen.....	142
Konfigurieren von Remote-Verbindungseinstellungen.....	143
Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen.....	145
Konfigurieren der Systempersonalisierung.....	146
Desktop-Erfahrung konfigurieren.....	149
Konfigurieren der Netzwerkeinstellungen.....	150
Konfigurieren der Sicherheits- und Sperrmoduseinstellungen.....	150
Andere Einstellungen konfigurieren.....	150
Konfigurieren von Remote-Verbindungseinstellungen – Citrix.....	152
Konfigurieren von Remote-Verbindungseinstellungen – VMware.....	155
Konfigurieren von Remote-Verbindungseinstellungen – RDP.....	156
Konfigurieren von Remote-Verbindungseinstellungen – Browser.....	160
Geräteinformationen konfigurieren.....	161
Konfigurieren von Wyse Easy Setup-Versionseinstellungen.....	161
Konfigurieren der VNC-Einstellungen.....	163
Konfigurieren von Domäneneinstellungen.....	164
<b>5 Verwalten von Geräten.....</b>	<b>165</b>
Methoden zum Registrieren Geräten bei Wyse Management Suite.....	166
Registrieren von ThinOS Geräten mit dem Wyse Geräte-Agenten.....	166
Registrieren des Wyse Software Thin Client bei der Wyse Management Suite über den Wyse Geräte-Agenten.....	167
Registrieren von Linux Thin Clients über Wyse Geräte-Agent.....	167
Registrieren von Wyse Embedded Standard Thin Clients bei der Wyse Management Suite über Wyse Geräte-Agent.....	168
Registrieren von Geräten mit ThinLinux Version 2.0 mithilfe der FTP-INI-Methode.....	168
Registrieren von Geräten mit ThinLinux Version 1.0 mithilfe der FTP-INI-Methode.....	169
Registrieren von ThinOS-Geräten mithilfe der FTP-INI-Methode.....	169
Registrieren von ThinLinux Thin Clients über Wyse Geräte-Agent.....	170
Registering devices by using DHCP option tags.....	170
Geräte mit DNS-SRV-Eintrag registrieren.....	171
Suche nach einem Gerät unter Verwendung von Filtern.....	172
Aktuellen Filter speichern.....	173
Abfragen des Gerätestatus.....	173
Sperren der Geräte.....	174
Neustart der Geräte.....	174
Deregistrierung der Geräte.....	174
Wiederherstellen der Standardeinstellungen.....	174
Ändern einer Gruppenzuweisung.....	175
Senden von Nachrichten an Geräte.....	175
Aktivieren der Geräte.....	175
Anzeigen von Gerätedetails.....	175
Gerätezusammenfassung verwalten.....	176
Anzeigen von Systeminformationen.....	176

Anzeigen von Geräteereignissen.....	176
Anzeigen installierter Anwendungen.....	177
Umbenennen des Thin Client.....	177
Konfigurieren von Remote Shadowing-Verbindung.....	178
Herunterfahren von Geräten.....	179
Tagging von Geräten.....	179
Compliance-Status des Geräts.....	180
Pull für Windows Embedded Standard oder ThinLinux-Abbild ausführen.....	180
Aktualisieren von ThinLinux 1.x auf 2.1 und neuere Versionen.....	181
Vorbereiten des ThinLinux 2.x-Abbilds.....	181
ThinLinux 1.x auf 2.x aktualisieren.....	182
Anfordern einer Protokolldatei.....	183
Beheben von Störungen auf Ihrem Gerät.....	183
<b>6 Anwendungen und Daten.....</b>	<b>185</b>
Anwendungsrichtlinie.....	185
Konfigurieren einer Thin-Client-Anwendungsbestandsaufnahme.....	186
Konfigurieren der Wyse Software Thin-Client-Anwendungsbestandsaufnahme.....	186
Erstellen und Bereitstellen von Standardanwendungsrichtlinie für Thin Clients.....	187
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients.....	188
Erstellen und Bereitstellen einer Standardanwendungsrichtlinie für Wyse Software Thin Clients.....	189
Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie für Wyse Software Thin Clients.....	190
Einmaliges Anmelden für Citrix StoreFront mithilfe der Standard-Anwendungsrichtlinie aktivieren.....	192
Abbildrichtlinie.....	192
Hinzufügen von Windows Embedded Standard-Betriebssystem- und ThinLinux-Abbildern zum Bestand..	192
Hinzufügen von ThinOS-Firmware zum Repository.....	193
Hinzufügen von ThinOS-Paketdatei zu Repository.....	193
Hinzufügen von ThinOS-BIOS-Datei zu Repository.....	193
Hinzufügen von Teradici-Firmware zum Repository.....	194
Erstellen von Windows Embedded Standard- und ThinLinux-Abbildrichtlinien.....	194
Datei-Repository verwalten.....	195
Ändern des Hintergrundbilds für alle Geräte, die einer Marketinggruppe angehören.....	195
<b>7 Verwalten von Regeln.....</b>	<b>197</b>
Bearbeiten einer Registrierungsregel.....	197
Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte.....	197
Bearbeitung der Regel für die automatische Zuweisung nicht verwalteter Geräte.....	198
Deaktivieren und Löschen einer Regel.....	198
Speichern der Regelreihenfolge.....	198
Hinzufügen einer Regel für Warnmeldungen.....	198
Bearbeiten einer Warnmeldungsregel.....	199
<b>8 Aufträge verwalten.....</b>	<b>200</b>
BIOS-Administratorkennwort synchronisieren.....	201
Suchen eines geplanten Jobs mithilfe von Filtern.....	201
Planen der Abbildrichtlinie.....	202
Planen einer Anwendungsrichtlinie.....	202

Planen des Gerätebefehlsjobs.....	203
<b>9 Verwalten von Ereignissen.....</b>	<b>204</b>
Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern.....	204
Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern.....	205
Anzeigen einer Zusammenfassung der Ereignisse.....	205
Überwachungsprotokoll anzeigen.....	206
<b>10 Verwalten von Benutzern.....</b>	<b>207</b>
Hinzufügen eines neuen Administratorprofils.....	208
Bearbeiten eines Administratorprofils.....	209
Deaktivieren eines Administratorprofils.....	209
Löschen eines Administratorprofils.....	210
Bearbeiten eines Benutzerprofils.....	210
Importieren der CSV-Datei.....	210
<b>11 Portalverwaltung.....</b>	<b>211</b>
Hinzufügen der Active Directory-Serverinformationen.....	212
Funktion "Active Directory-Verbunddienste" in einer öffentlichen Cloud konfigurieren.....	213
Importieren von Benutzern in die öffentliche Cloud über Active Directory.....	214
Warnungsklassifizierungen.....	214
Erstellen eines API-Kontos (Application Programming Interface).....	214
Zugriff auf Datei-Repository.....	214
Andere Einstellungen konfigurieren.....	215
Verwalten von Teradici-Konfigurationen.....	216
Aktivieren der Zweifaktor-Authentifizierung.....	216
Generieren von Berichten.....	216
Aktivieren von Multi-Tenant Konten.....	217
Aktivieren von benutzerdefiniertem Branding.....	218
Verwalten des Lizenzabonnements.....	218
Importieren von Lizenzen von der öffentlichen Cloud-Konsole der Wyse Management Suite.....	219
Exportieren von Lizenzen in die privaten Cloud-Konsole der Wyse Management Suite.....	219
Thin Client-Lizenzzuweisung.....	219
Lizenzbestellungen.....	220
Verwalten des System-Setup.....	220
<b>12 Konfigurieren von Wyse Easy Setup mithilfe der Wyse Management Suite.....</b>	<b>222</b>
Installieren von Wyse Easy Setup.....	222
Implementieren einer Wyse Easy Setup-Konfiguration.....	222
<b>13 Konfigurieren von Wyse Converter for PCs mithilfe der Wyse Management Suite.....</b>	<b>224</b>
Registrieren des Wyse Software Thin Clients bei der Wyse Management Suite.....	224
Registrieren des Wyse Software Thin Client bei der Wyse Management Suite über den Wyse Geräte-Agenten.....	224
Registrieren von Geräten durch die Verwendung von DHCP-Option-Tags bei der Wyse Management Suite..	225
Registrieren von Wyse Software Thin Clients mithilfe des DNS-SRV-Eintrags bei Wyse Management Suite..	225
Konfigurieren des Wyse Software Thin Clients mithilfe der Wyse Management Suite.....	226

<b>14 Teradici-Geräteverwaltung.....</b>	<b>228</b>
Ermittlung von Teradici-Geräten.....	228
Sicherheitsstufe.....	228
Manuelle Ermittlung über den Client.....	229
Hinzufügen der PCoIP-Endpunkt-Anbieterklasse zum DHCP-Server.....	229
Konfigurieren von DHCP-OptionenErstellen des DNS-SRV-Eintrags.....	230
Hinzufügen eines DNS-TXT-Eintrags.....	231
Erstellen eines SHA-256-Fingerabdrucks.....	231
CIFS-Anwendungsszenarien.....	231
<b>15 Wyse-Geräte-Agent.....</b>	<b>233</b>
<b>16 Beheben von Fehlern in der Wyse Management Suite.....</b>	<b>234</b>
<b>Anhang A: Installieren oder Aktualisieren von Wyse Geräte-Agent.....</b>	<b>239</b>
Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie.....	239
Manuelles Installieren von Wyse Geräte-Agent.....	240
Installieren oder Aktualisieren von Wyse Geräte-Agenten auf ThinLinux- und Linux-Clients.....	240
<b>Anhang B: Wyse Management Suite-Funktionsmatrix.....</b>	<b>241</b>
<b>Anhang C: Unterstützte Thin Clients auf der Wyse Management Suite.....</b>	<b>243</b>
<b>Anhang D: Funknetzwerkprofil-Kennworteditor.....</b>	<b>246</b>
Konfigurieren des Windows Wireless-Profiles.....	246
Konfigurieren des Funknetzwerkprofil-Kennworteditors.....	246
Einschränkungen des Funknetzwerkprofil-Kennworteditors.....	247
<b>Anhang E: Erstellen und Konfigurieren von DHCP-Options-Tags.....</b>	<b>248</b>
<b>Anhang F: Erstellen und Konfigurieren von DNS-SRV-Einträgen.....</b>	<b>254</b>
<b>Anhang G: Schritte zum Ändern des Hostnamens zur IP-Adresse.....</b>	<b>261</b>

# Einführung in die Wyse Management Suite

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

**ANMERKUNG:** Die Wyse Management Suite ist die überarbeitete Neufassung des Dell Cloud Client Manager (CCM) und stellt neue Merkmale und Funktionen mit erheblichen Verbesserungen auf Produktebene gegenüber dem CCM R14 zur Verfügung. Weitere Informationen finden Sie in den Versionshinweisen von Wyse Management Suite, die unter [www.dell.com/support/manuals](http://www.dell.com/support/manuals) Verfügbar sind. Bestehende Kunden können ihre Thin Clients weiterhin wie bisher verwalten und die neuen Funktionen nutzen, die in dieser Version eingeführt werden.

## Editionen

Wyse Management Suite ist in den folgenden Editionen erhältlich:

- **Standard (kostenlos)** – Die Standard-Edition der Wyse Management Suite ist nur für die Bereitstellung vor Ort verfügbar. Sie benötigen keinen Lizenzschlüssel, um die Standard Edition zu verwenden. Die Standard Edition eignet sich für kleine und mittelständische Unternehmen.
- **Pro (kostenpflichtig)** – Die Pro Edition der Wyse Management Suite steht sowohl für die Bereitstellung vor Ort als auch in der Cloud zur Verfügung. Sie benötigen einen Lizenzschlüssel zur Verwendung der Pro Edition. Die Lizenzierung ist abonnementbasiert möglich. Mit dem Pro-Lösung können Unternehmen ein Hybridmodell und bewegliche Lizenzen zum Wechsel zwischen der Bereitstellung vor Ort und in der Cloud nutzen. Die Pro Edition für die Bereitstellung vor Ort eignet sich für kleine, mittelständische und große Unternehmen. Für eine Cloud Bereitstellung kann die Pro Edition in Nicht-Firmennetzwerken verwaltet werden (Home Office, Drittanbieter, Partner, mobile Thin Clients, usw.). Die Pro Edition der Wyse Management Suite bietet außerdem:
  - Eine mobile App, zum Anzeigen von kritischen Warnungen sowie Benachrichtigungen und dem Senden von Befehlen in Echtzeit.
  - Verbesserte Sicherheit durch Zwei-Faktor-Identifizierung und Active Directory-Authentifizierung für rollenbasierte Verwaltung.
  - Erweiterte App-Richtlinie und -Berichterstellung

**ANMERKUNG:**

- Cloud-Dienste werden in den USA und Deutschland gehostet. Kunden in Ländern mit Beschränkungen bezüglich zulässiger Datenspeicherorte können u. U. den Cloud-basierten Dienst nicht nutzen.
- Lizenzen können ganz einfach zwischen Cloud- und vor-Ort-Installation gewechselt werden.

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

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

# Was ist neu in dieser Version?

- Wyse 5470 Thin Client und Wyse 5470 All-in-One Thin Client werden unterstützt.
- Komponenten der Wyse Management Suite wie Open JDK und Tomcat-Dienste sind aktualisiert.
- Öffentliche Cloud-Speicherung von ThinOS-Paketen wird unterstützt.
- Einheitlicher Workflow für ThinOS-Firmware und -Paket wurde integriert.
- Option zum Hinzufügen von Paketen aus **Apps & Daten** wurde integriert.
- Teradici EMSDK-Komponente wurde zur Unterstützung von Open JDK 11 aktualisiert.
- Option zum Exportieren oder Importieren einer Richtlinienkonfiguration wurde integriert.
- Option zum Beibehalten der Konfigurationen auf Geräteebene, wenn das Gerät in eine andere Gruppe verschoben wird, wurde integriert.
- Option für die Aktualisierung von Hostdateien integriert.
- Bereitstellung von Multi-Monitor-Setup-Konfigurationen auf Thin Clients mit ThinOS-Betriebssystem wird unterstützt.
- Option zum Konfigurieren der Zeitüberschreitung der Wyse Management Suite-Konsole wurde integriert.
- Option zum Ausschalten des Thin Client wurde integriert.
- Wyse Easy Setup Version 2.0 wird unterstützt.
- Overlay Optimizer Version 1.0 wird unterstützt.
- Dell Secure Client Version 1.0 wird unterstützt.
- Upgrade von ThinLinux 1.x auf 2.2 wird auf Wyse 3040 Thin Client und Wyse 5070 Thin Client unterstützt.
- Sperrmodus-Einstellungen für das ThinLinux-Betriebssystem werden unterstützt.
- Option zum Konfigurieren der Zeitüberschreitungseinstellungen pro Anwendung für Standard- und erweiterte Richtlinie wird unterstützt.
- Option zum Sortieren der Geräte nach Filterstatus wird unterstützt.
- Option zur Optimierung der Anwendungsliste auf Basis des Betriebssystems wird unterstützt.
- Option zum Konfigurieren von Alias-Daten wird unterstützt.
- Konfigurationen, die auf Thin Clients mit den Betriebssystemen ThinOS, ThinLinux und Windows Embedded Standard bereitgestellt werden können, wurden aktualisiert.
- Wyse Geräte-Agent wurde auf Version 14.4.x aktualisiert.

# 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:

- Anmeldung bei der Wyse Management Suite in einer öffentlichen Cloud
- Voraussetzungen für Wyse Management Suite in einer privaten Cloud
- Funktionsbereiche der Management Console
- Konfigurieren und Verwalten von Thin Clients

## Anmeldung bei der Wyse Management Suite in einer öffentlichen Cloud

Zum Anmelden bei der Wyse Management Suite-Konsole benötigen Sie einen unterstützten Webbrowser, der auf dem System installiert ist. Eine Liste der unterstützten Webbrowser finden Sie unter [Unterstützte Web-Browser](#). So melden Sie sich an der Wyse Management Suite-Konsole an:

1 Greifen Sie auf die öffentliche Cloud (SaaS) Edition der Wyse Management Suite mithilfe einer der folgenden Links zu:

- **US-Rechenzentrum** – [us1.wysemanagementsuite.com/ccm-web](https://us1.wysemanagementsuite.com/ccm-web)
- **EU-Rechenzentrum** – [eu1.wysemanagementsuite.com/ccm-web](https://eu1.wysemanagementsuite.com/ccm-web)

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

2 Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

3 Klicken Sie auf **Anmelden**.

### **ANMERKUNG:**

- Sie erhalten Ihre Anmeldeinformationen bei der Anmeldung für die Testversion der Wyse Management Suite auf [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com) oder beim Kauf Ihres Abonnements. Sie können das Wyse Management Suite-Abonnement vom Dell Vertrieb oder von Ihrem lokalen Dell Partner erwerben. Weitere Informationen finden Sie auf [www.wysemanagementsuite.com](https://www.wysemanagementsuite.com).
- Dell empfiehlt Ihnen, Ihr Kennwort nach der ersten Anmeldung zu ändern.
- Die Standardbenutzernamen und Kennwörter für zusätzliche Administratoren werden von dem Wyse Management Suite-Kontobesitzer erstellt.
- Ein extern zugängliches Repository muss auf einem Server mit einer DMZ während der Verwendung der Pro Edition von Wyse Management Suite in der öffentlichen Cloud installiert werden. Zudem muss der vollständig qualifizierte Domainname (FQDN) des Servers im öffentlichen DNS registriert werden.

## Ändern Ihres Kennworts

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

# Abmelden

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

## Voraussetzungen für Wyse Management Suite in einer privaten Cloud

Tabelle 1. Vorbedingungen

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

## ANMERKUNG:

- **WMS.exe** und **WMS\_Repo.exe** müssen auf zwei verschiedenen Servern installiert werden. Sie müssen das Wyse Management Suite Remote-Repository für die öffentliche Cloud installieren. Für eine private Cloud müssen Sie zunächst das Wyse Management Suite Remote-Repository und das lokale Repository herunterladen. Weitere Informationen finden Sie unter [Zugriff auf das Datei-Repository](#).
- Die Software kann auf einer physischen oder einer virtuellen Maschine installiert werden.
- Es ist nicht notwendig, dass der Software-Repository- und der Wyse Management Suite-Server das gleiche Betriebssystem aufweisen.
- Die Installationsskripte für den Overlay Optimizer Version 1.0 werden mit dem Wyse Management Suite-Installationsprogramm mitgeliefert. Der Administrator muss die Skripte ausführen, damit der Overlay Optimizer in der Wyse Management Suite verfügbar gemacht werden kann.
- Die Installationsskripte für den Dell Secure Client Version 1.0 werden mit dem Wyse Management Suite-Installationsprogramm mitgeliefert. Der Administrator muss die Skripte ausführen, damit der Dell Secure Client in der Wyse Management Suite verfügbar gemacht werden kann.

# 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 **Gruppen und Konfigurationen** nutzt eine hierarchische Gruppenrichtlinienverwaltung zur Gerätekonfiguration. Optional können Untergruppen der globalen Gruppenrichtlinien erstellt werden, um Geräte entsprechend den Unternehmensstandards zu kategorisieren. Beispielsweise können Geräte nach Stellenfunktion, Gerätetyp und so weiter untergliedert werden.
- Die Seite **Benutzer** ermöglicht es, lokalen und aus dem Active Directory importierten Benutzern, die Rollen globaler Administrator, Gruppenadministrator und Viewer zuzuweisen und sich bei der Wyse Management Suite anzumelden. Benutzer erhalten Berechtigungen zum Ausführen von Vorgängen auf Basis der ihnen zugewiesenen Rollen.
- Die Seite **Geräte** ermöglicht das Anzeigen und Verwalten von Geräten, Gerätetypen, und gerätespezifischen Konfigurationen.
- Die Seite **Apps & Daten** ermöglicht die Verwaltung von Geräteanwendungen, Betriebssystemabbildern, Richtlinien, Zertifikatdateien, Logos und Hintergrundbildern.
- Die Seite **Regeln** ermöglicht Ihnen das Hinzufügen, Bearbeiten und Aktivieren oder Deaktivieren von Regeln wie z. B. automatische Gruppierung und Warnmeldung.
- Die Seite **Jobs** ermöglicht Ihnen die Erstellung von Jobs für Aufgaben wie z. B. Neustart, WOL und Anwendungs- oder Abbildrichtlinien, die auf registrierten Geräten bereitgestellt werden sollen.
- Die Seite **Ereignisse** ermöglicht das Anzeigen und Überprüfen von Systemereignissen und Warnungen.
- Die Seite **Portalverwaltung** ermöglicht Ihnen die Konfiguration verschiedener Systemeinstellungen, wie die Konfiguration des lokalen Repositories, Lizenzabonnements, Active Directory-Konfiguration und Zwei-Faktor-Authentifizierung.

# Konfigurieren und Verwalten von Thin Clients

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

## ANMERKUNG:

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

Sie können auch Folgendes konfigurieren:

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

Beispiel:

- Konfigurieren Sie die Richtlinien für die Standardrichtliniengruppe (übergeordnete Gruppe). Nach der Konfiguration der Richtlinien überprüfen Sie die Richtlinien der benutzerdefinierten Gruppe (untergeordnete Gruppe). Derselbe Satz von Richtlinien wird auf die untergeordnete Gruppe angewendet. Eine Konfiguration der Einstellungen der Standardrichtliniengruppe ist der globale Parametersatz, den alle Gruppen und Untergruppen von der übergeordneten Gruppe übernehmen.
- Konfigurieren Sie die verschiedenen Einstellungen für die benutzerdefinierte Gruppe. Die benutzerdefinierte Gruppe empfängt beide Nutzlasten, aber Geräte in der Standardrichtliniengruppe empfangen nicht die Nutzlast, die für die benutzerdefinierte Richtliniengruppe konfiguriert ist.
- Konfigurieren Sie die verschiedenen Einstellungen für die benutzerdefinierte Gruppe. Die für Gruppen auf einer niedrigeren Ebene konfigurierten Einstellungen haben Vorrang vor den Einstellungen, die für übergeordnete Gruppen konfiguriert wurden.
- Einstellungen, die spezifisch für ein bestimmtes Gerät gelten, können auf der Seite **Gerätedetails** konfiguriert werden. Diese Einstellungen haben wie auch bei untergeordneten Gruppen Vorrang vor den in übergeordneten Gruppen konfigurierten Einstellungen.

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

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

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

**Bereitstellung der Anwendung und des Betriebssystemabbilds** – Aktualisierungen an Anwendungen und dem Betriebssystemabbild können über die Registerkarte **Apps & Daten** bereitgestellt werden. Anwendungen werden basierend auf den Richtliniengruppen bereitgestellt.

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

Die Wyse Management Suite unterstützt die Anwendungsrichtlinien "Standard" und "Erweitert". Eine Standardanwendungsrichtlinie ermöglicht die Installation eines einzigen Anwendungspakets. Das Gerät wird während der Installation einer Anwendung neu gestartet. Sie müssen das Gerät vor und nach jeder Anwendungsinstallation neu starten. Bei einer erweiterten Anwendungsrichtlinie, können mehrere Anwendungspakete mit nur zwei Neustarts installiert werden. Diese Funktion ist nur in der Pro-Edition verfügbar. Erweiterte Anwendungsrichtlinien unterstützen auch die Ausführung von Installationskripten vor und nach der Betriebssysteminstallation, die Sie möglicherweise zur Installation einer bestimmten Anwendung benötigen.

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

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

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

Zum Navigieren zur Seite **Gerätedetails** für dieses Gerät klicken Sie auf den auf dieser Seite aufgelisteten Geräteeintrag. Alle Einzelheiten für das Gerät werden angezeigt.

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

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

**Berichte** – Sie können vordefinierte Berichte auf der Grundlage der voreingestellten Filter generieren und anzeigen. Zum Erzeugen vordefinierter Berichte klicken Sie auf die Registerkarte **Berichte** auf der Seite **Portaladministrator**.

**Mobile-Anwendung** – Sie können mithilfe der mobilen App **Dell Mobile Agent** Warnbenachrichtigungen erhalten und Geräte verwalten. Sie ist für Android-Geräte verfügbar. Zum Herunterladen der mobilen App und des **Dell Mobile Agent Handbuchs zum Einstieg** klicken Sie auf die Registerkarte **Warnungen und Klassifizierung** auf der Seite **Portaladministrator**.

# Wyse Management Suite-Dashboard

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

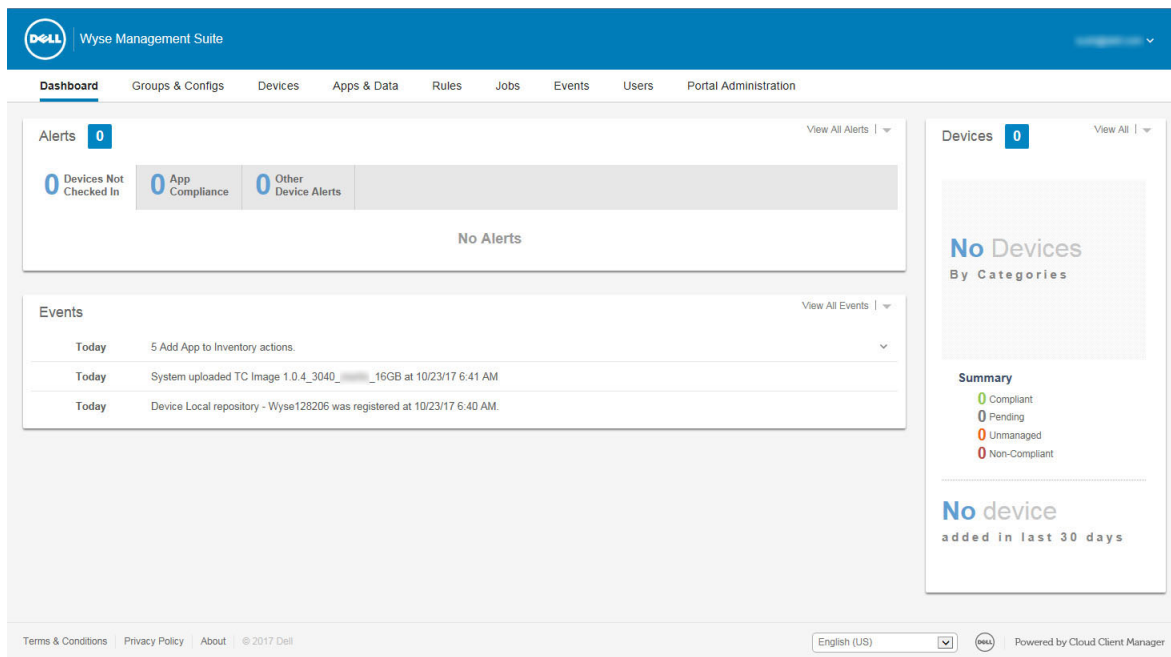


Abbildung 1. Dashboard

Themen:

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

## Anzeigen von Warnungen

Im Bereich **Warnungen** wird die Zusammenfassung aller Warnungen angezeigt. Dieser Abschnitt hat die folgenden Attribute:

- **Gerät nicht eingecheckt**
- **App-Konformität**
- **Andere Gerätewarnungen**

So zeigen Sie die detaillierte Liste aller Warnungen an:

- 1 Klicken Sie auf **Dashboard**.

Die Warnungsübersicht wird angezeigt.

- 2 Klicken Sie auf **Alle Warnungen anzeigen**.

Die Seite **Ereignisse** wird angezeigt. Sie enthält eine Liste mit allen Warnungen.

## Anzeigen der Ereignisliste

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

So zeigen Sie die detaillierte Liste aller Ereignisse an:

- 1 Klicken Sie auf **Dashboard**.

Die Ereignisübersicht wird angezeigt.

- 2 Klicken Sie auf **Alle Ereignisse anzeigen**.

Die Seite **Ereignisse** wird angezeigt. Sie enthält eine Liste mit allen Ereignissen.

## Anzeigen des Gerätestatus

Der Abschnitt **Anzeige** enthält die Zusammenfassung der Gerätestatus. Der Abschnitt **Zusammenfassung** zeigt die Geräteanzahl auf Basis der folgenden Gerätestatuskategorie an:

- **Konform**
- **Ausstehend**
- **Nicht verwaltet**
- **Nicht konform**

So zeigen Sie die detaillierte Liste aller Geräte an:

- 1 Klicken Sie auf **Dashboard**.

Es wird eine Geräteübersicht angezeigt.

- 2 Klicken Sie auf **Alle anzeigen**.

Die Seite **Geräte** wird angezeigt. Sie enthält eine Liste mit allen registrierten Geräten.

## Ändern von Benutzereinstellungen

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

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

## Zugriff auf die Onlinehilfe

So greifen Sie auf die Handbücher der Wyse Management Suite zu:

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

# Ändern Ihres Kennworts

So ändern Sie Ihr Kennwort:

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

# Abmelden

So melden Sie sich bei der Verwaltungskonsole ab:

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

# Verwalten von Gruppen und Konfigurationen

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

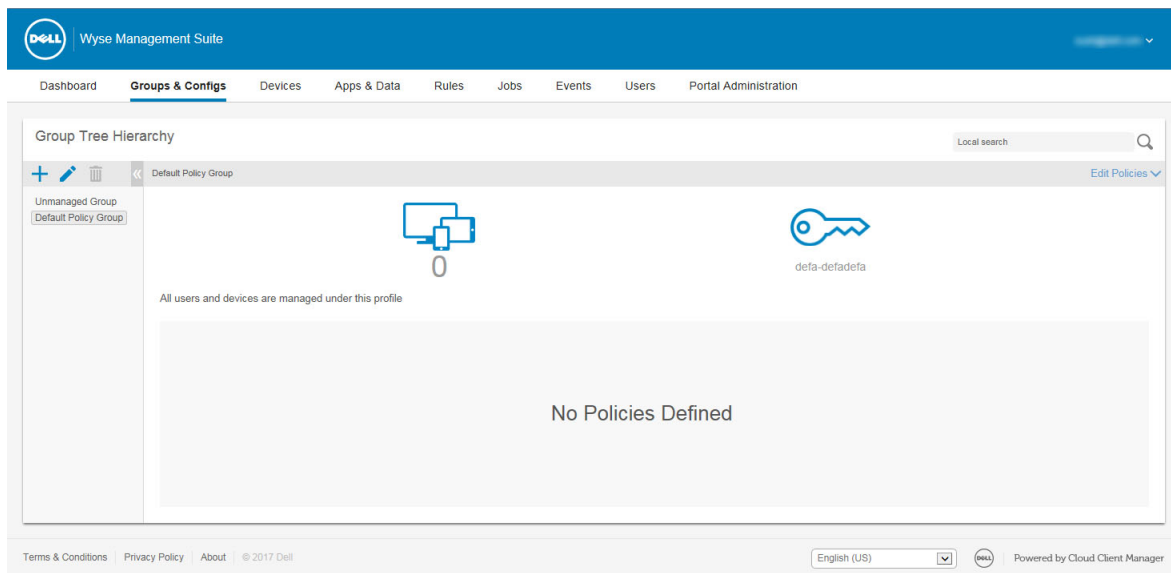


Abbildung 2. Gruppen und Konfiguration

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

- **ThinOS**
- **WES**
- **Linux**
- **ThinLinux**
- **Teradici**
- **Wyse Software Thin Client**

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

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

Die Konfiguration für eine bestimmte Ressource mit Einzelheiten dazu, wo Konfigurationen festgelegt werden (global, auf Gruppen- oder Geräteebene), werden auf der Seite angezeigt. Die Option zum Erstellen von Ausnahmen ist auf der Seite verfügbar. Die **Ausnahme**-Einstellungen gelten nur für die ausgewählten Geräte. Weitere Informationen finden Sie unter [Konfigurieren von Richtlinien der Geräteklasse](#).

## **i ANMERKUNG:**

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

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

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

## **i ANMERKUNG: Gewisse Einstellungen, wie z. B. die BIOS-Konfiguration für Windows Embedded 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

Themen:

- [Hinzufügen einer Gruppe](#)
- [Bearbeiten einer Gruppe](#)
- [Entfernen einer Gruppe](#)
- [Bearbeiten einer nicht verwalteten Gruppe](#)
- [Konfigurieren von Richtlinien der Globalen Klasse](#)
- [Konfigurieren von Richtlinien auf Gruppenebene](#)
- [Konfigurieren von Richtlinien der Geräteklasse](#)
- [Gruppenrichtlinien exportieren](#)
- [Gruppenrichtlinien importieren](#)
- [Bearbeiten der Einstellungen für ThinOS-Richtlinien](#)
- [Bearbeiten von Windows Embedded Standard-Richtlinieneinstellungen](#)
- [Bearbeiten der Einstellungen für die Linux-Richtlinie](#)
- [Bearbeiten der Einstellungen für die ThinLinux-Richtlinie](#)
- [Bearbeiten von Teradici-Richtlinieneinstellungen](#)
- [Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen](#)

# Hinzufügen einer Gruppe

Zum Hinzufügen einer Gruppe gehen Sie wie folgt vor:

- 1 Klicken Sie auf der Seite **Gruppen und Konfigurationen** auf das Symbol .
- 2 Im Dialogfeld **Neue Gruppe(n) hinzufügen** geben Sie den **Gruppennamen** und eine **Beschreibung** ein.

## **i ANMERKUNG: Zum Ändern von Name und Beschreibung einer Gruppe verwenden Sie Active Directory.**


- 3 Aktivieren Sie auf der Registerkarte **Registrierung** das Kontrollkästchen **Aktiviert** unter Gruppentoken.
- 4 Geben Sie das Gruppentoken ein.

## **i ANMERKUNG: Die Geräte können durch Eingabe des Gruppentokens in einer Gruppe registriert werden, der auf dem Geräteregistrierungsbildschirm zu finden ist.**

- 5 Auf der Registerkarte **Verwaltung** können Sie den Namen der Gruppenadministratoren auswählen, die diese Gruppe verwalten sollten. Wählen Sie im Feld **Verfügbare Gruppenadministratoren** die betreffende Gruppe aus und klicken Sie dann auf den Rechtspfeil, um sie in das Feld **Zugewiesene Gruppenadministratoren** zu verschieben. Zum Verschieben einer Gruppe von **Zugewiesene Gruppenadministratoren** nach **Verfügbare Gruppenadministratoren**, gehen Sie umgekehrt vor.
- 6 Klicken Sie auf **Speichern**.  
Die Gruppe wird der Liste verfügbarer Gruppen auf der Seite **Gruppen und Konfigurationen** hinzugefügt.

## Bearbeiten einer Gruppe

Zum Bearbeiten einer Gruppe gehen Sie wie folgt vor:


- 1 Klicken Sie auf der Seite **Gruppen und Konfigurationen** auf das Symbol .
- 2 Bearbeiten Sie im Dialogfeld **Standardrichtliniengruppe bearbeiten** die Gruppeninformationen wie z. B. **Gruppenname** und **Beschreibung**.
- 3 Bearbeiten Sie unter der Registerkarte **Registrierung** das Gruppentoken.

**ANMERKUNG:** Die Geräte können durch Eingabe des Gruppentokens in einer Gruppe registriert werden, der auf dem Geräteregistrierungsbildschirm zu finden ist.

- 4 Klicken Sie auf **Speichern**.

## Entfernen einer Gruppe

Als Administrator können Sie eine Gruppe aus der Gruppenhierarchie entfernen. Zum Entfernen einer Gruppe gehen Sie wie folgt vor:

- 1 Klicken Sie auf der Seite **Gruppen und Konfigurationen** in der **Gruppenstruktur-Hierarchie** auf das Symbol .  
Eine Warnmeldung, die darauf hinweist, dass diese Maßnahme eine oder mehrere Gruppen aus der Gruppenstruktur-Hierarchie entfernt, wird angezeigt.
- 2 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.

## Bearbeiten einer nicht verwalteten Gruppe

Geräte, die der nicht verwalteten Gruppe angehören, verwenden keine Lizenzen oder empfangen Konfigurationen oder anwendungs-basierte Richtlinien. Zum Hinzufügen von Geräten zu einer nicht verwalteten Gruppe verwenden Sie den Geräteregistrierungsschlüssel für die nicht verwaltete Gruppe im Rahmen der automatischen Registrierung oder der manuellen Registrierung. Gehen Sie folgendermaßen vor, um eine nicht verwaltete Gruppe zu bearbeiten:

- 1 Klicken Sie auf **Gruppe bearbeiten**.  
Die Seite **Nicht verwaltete Gruppe bearbeiten** wird angezeigt. Der **Gruppenname** zeigt den Namen der Gruppe an.
- 2 Geben Sie folgende Informationen ein:
  - **Beschreibung** – Zeigt eine kurze Beschreibung der Gruppe an.
  - **Gruppentoken** – Wählen Sie diese Option aus, um das Gruppentoken zu aktivieren.
- 3 Klicken Sie auf **Speichern**.

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

# Konfigurieren von Richtlinien der Globalen Klasse

Zur Konfiguration von Richtlinien der Globalen Klasse, gehen Sie wie folgt vor:

- 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 auf die Richtlinieneinstellung aus, die Sie konfigurieren möchten, und klicken Sie dann auf **Dieses Element konfigurieren**.
- 3 Klicken Sie auf **Speichern und Veröffentlichen**.

## Konfigurieren von Richtlinien auf Gruppenebene

Zum Konfigurieren von Richtlinien auf Gruppenebene oder mehrstufigen Gruppenrichtlinien, gehen Sie wie folgt vor:

- 1 Gehen Sie auf der Seite **Gruppen und Konfigurationen** zu der Gruppe, in der Sie die Richtlinie konfigurieren möchten, und klicken Sie auf **Richtlinien bearbeiten**.
- 2 Wählen Sie aus dem Dropdownmenü den Gerätetyp aus, den Sie konfigurieren möchten. Die Richtlinieneinstellungen des Gerätetyps werden angezeigt.
- 3 Wählen Sie eine Richtlinieneinstellung aus und klicken Sie dann auf **Dieses Element konfigurieren**.
- 4 Klicken Sie auf **Speichern und Veröffentlichen**.

## Konfigurieren von Richtlinien der Geräteklasse

Zur Konfiguration von Richtlinien der Geräteklasse gehen Sie wie folgt vor:

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

## Gruppenrichtlinien exportieren

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

- 1 Wählen Sie auf der Seite **Gruppen und Konfigurationen** die Gruppe aus, aus der Sie Richtlinien exportieren möchten. Für die Gruppe müssen Richtlinien konfiguriert sein.
- 2 Klicken Sie auf **Richtlinien exportieren**. Der Bildschirm **Richtlinien exportieren** wird angezeigt.
- 3 Wählen Sie die zu exportierenden Gerätetypen aus. Die folgenden Optionen stehen zur Verfügung:
  - Alle Gerätetypen: Alle Gerätetyp-Richtlinien werden exportiert.
  - Spezifische Gerätetypen: Wählen Sie einen oder mehrere Gerätetypen aus der Dropdown-Liste aus. Nur die ausgewählten Gerätetypen werden exportiert.
- 4 Klicken Sie auf die Schaltfläche "Ja", um die ausgewählten Gerätetypen zu exportieren. Übergeordnete Gruppenrichtlinien werden nicht exportiert. Es werden nur Richtlinien exportiert, die auf der ausgewählten oder Zielgruppen-Ebene konfiguriert sind.
- 5 Klicken Sie auf den Download-Link oder mit der rechten Maustaste auf die Datei und anschließend auf **Speichern unter**, um die JSON-Datei zu speichern. Die Kennwörter werden in der exportierten Datei verschlüsselt. Der Dateiname wird im Format `[Group Name]-[ALL]-[Exported Date & Time]UTC.json` erstellt.

# Gruppenrichtlinien importieren

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

Um die Gruppenrichtlinien von der Seite **Gruppen und Konfigurationen** zu importieren, gehen Sie wie folgt vor:

- 1 Wählen Sie auf der Seite **Gruppen und Konfigurationen** die gewünschte Gruppe aus.  
Wenn die Zielgruppe Richtlinien des gleichen Gerätetyps wie die importierten enthält, werden sie entfernt und neue hinzugefügt.
- 2 Klicken Sie auf **Richtlinien importieren**.  
Daraufhin wird der Bildschirm **Assistent zum Import von Richtlinien** angezeigt.
- 3 Wählen Sie den Modus zum Importieren der Gruppenrichtlinien aus der ausgewählten Gruppe.  
Die folgenden Optionen stehen zur Verfügung:
  - Aus einer vorhandenen Gruppe: Wählen Sie eine Gruppe aus der Dropdown-Liste aus. Richtlinien aus dieser Gruppe werden in die aktuelle Gruppe kopiert.
  - Aus einer exportierten Datei: Suchen Sie die Datei `.json`. Richtlinien aus dieser Datei werden in die aktuelle Gruppe kopiert.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie die zu importierenden Gerätetypkonfigurationen aus.  
Die folgenden Optionen stehen zur Verfügung:
  - Alle Gerätetyprichtlinien: Alle konfigurierten Gerätetyprichtlinien werden in die aktuelle Gruppe importiert.
  - Spezifische Gerätetyprichtlinien: Wählen Sie einen oder mehrere Gerätetypen aus der Dropdown-Liste aus. Nur die ausgewählten Gerätetyprichtlinien werden in die aktuelle Gruppe importiert.
- 6 Klicken Sie auf **Weiter**.  
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 Bestandsaufnahme-dateien 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 Bestandsaufnahme-dateien enthält.
- 7 Klicken Sie auf **Importieren**.

## ANMERKUNG:

- Nur die ausgewählten Gerätetypkonfigurationen können importiert werden.
- Richtlinien, die in der Zielgruppe für den ausgewählten Gerätetyp definiert sind, werden entfernt, bevor die neuen Richtlinien des gleichen Gerätetyps angewendet werden.
- Wenn Sie eine Richtlinie aus einer Datei importieren und Verweise oder ungültige Abhängigkeiten existieren, schlägt der Import fehl und es wird eine Fehlermeldung angezeigt.

Um die Gruppenrichtlinien von der Seite **Richtlinien bearbeiten** zu importieren, gehen Sie wie folgt vor:

- 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 bearbeiten** und wählen Sie die gewünschte Option.
- 3 Klicken Sie auf **Importieren**.  
Daraufhin wird der Bildschirm **Assistent zum Import von Richtlinien** angezeigt.
- 4 Wählen Sie den Modus zum Importieren der Gruppenrichtlinien aus der ausgewählten Gruppe.  
Die folgenden Optionen stehen zur Verfügung:
  - Aus einer vorhandenen Gruppe: Wählen Sie eine Gruppe aus der Dropdown-Liste aus. Richtlinien aus dieser Gruppe werden in die aktuelle Gruppe kopiert.

- Aus einer exportierten Datei: Suchen Sie die Datei `.JSON`. Richtlinien aus dieser Datei werden in die aktuelle Gruppe kopiert.
- 5 Klicken Sie auf **Weiter**. Die Zusammenfassung des Importvorgangs wird angezeigt. Die folgenden Arten von Warnungen können angezeigt werden:
    - *Importierte <Gerätetyp>-Richtlinien werden auf die Gruppe <Gruppenname> angewendet:* 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 Bestandsaufnahme-dateien 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 Bestandsaufnahme-dateien enthält.
  - 6 Klicken Sie auf **Importieren**.

## Bearbeiten der Einstellungen für ThinOS-Richtlinien

Gehen Sie folgendermaßen vor, um die ThinOS-Richtlinieneinstellungen zu bearbeiten:

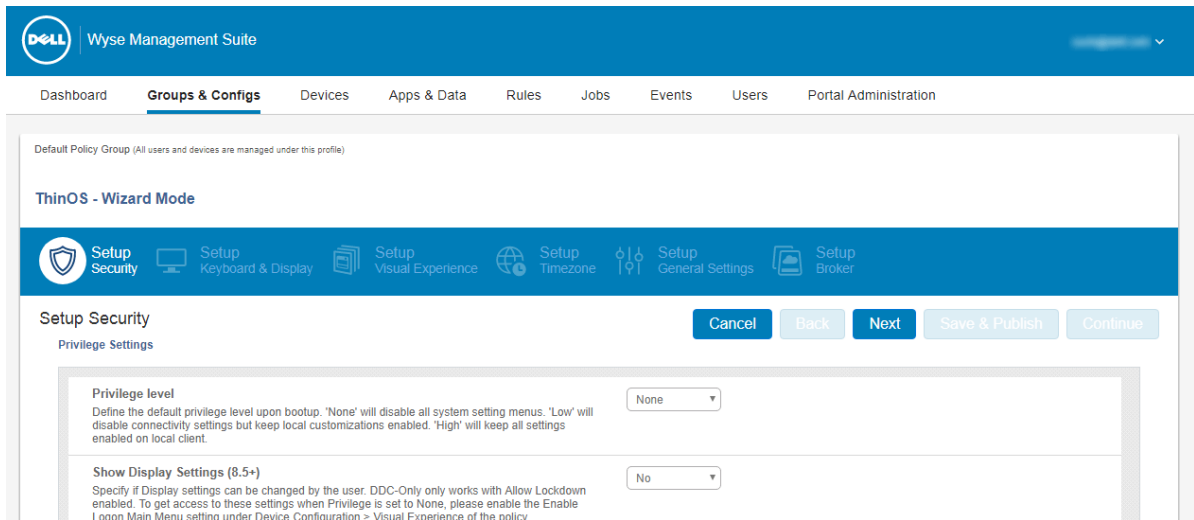
- 1 Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
  - 2 Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
  - 3 Klicken Sie auf **ThinOS**.  
Es wird das Fenster **ThinOS-Konfigurationsmodus auswählen** angezeigt.
  - 4 Wählen 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.
- 5 Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

- ANMERKUNG:** Der Thin Client wird neu gestartet, wenn Sie Änderungen an den folgenden Einstellungen vornehmen:
- BIOS-Einstellung
  - DP-Audio
  - Popup – Buchse
  - 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. Gehen Sie folgendermaßen vor, um die Richtlinieneinstellungen zu konfigurieren:

- 1 Wählen Sie **Assistent** als Modus der Konfiguration.
- 2 Im Folgenden finden Sie die verfügbaren Richtlinieneinstellungen auf der Seite **ThinOS – Assistentenmodus**.



**Abbildung 3. ThinOS – Assistentenmodus**

- Setup für Sicherheitseinstellungen
  - Setup für Tastatur und Bildschirm
  - Setup für visuelles Erlebnis
  - Zeitzone festlegen
  - Setup für allgemeine Einstellungen
  - Broker einrichten
- Klicken Sie auf **Weiter** und gehen Sie zu Richtlinieneinstellungen.
  - Klicken Sie auf **Zurück** zum Anzeigen der vorherigen Richtlinieneinstellungen.
  - Klicken Sie auf **Abbrechen**, um zur Seite **Gruppen und Konfigurationen** zurückzukehren.
  - Klicken Sie zum Speichern der Änderungen auf **Speichern und veröffentlichen**.
  - Klicken Sie auf **Weiter**, um zum erweiterten ThinOS-Konfigurationsmodus zu gehen.

## Konfigurieren der Setup-Sicherheitseinstellungen

Verwenden Sie diese Seite zum Konfigurieren der Thin Client-Sicherheitseinstellungen, wie z. B. Benutzerberechtigungen und Zertifikatinstallation.

### **ANMERKUNG:**

- Die Zertifikatszuweisung kann auf globaler Ebene, Gruppenebene oder Geräte-Ebene verwaltet werden. Wenn Sie die Option **Zertifikate automatisch installieren** wählen, wird die Liste der Benutzerzertifikate auf die Seite **Datei-Repository-Bestand** hochgeladen.
- Für automatisierte Zertifikatbereitstellungen wählen Sie die Zertifikate, die automatisch auf Thin Clients installiert werden sollen.

**Tabelle 2. Konfigurieren von Berechtigungseinstellungen**

Option	Beschreibung
<b>Berechtigungsebene</b>	Wählen Sie diese Option zum Definieren der Standard-Berechtigungsstufe während des Systemstarts. Wählen Sie im Dropdownmenü eine beliebige der folgenden Stufen aus: <ul style="list-style-type: none"> <li>• Keine – Deaktiviert alle Systemeinstellungsoptionen.</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>· Hoch – Deaktiviert alle Verbindungseinstellungen außer lokalen Anpassungen.</li> <li>· Niedrig – Alle Einstellungen auf dem lokalen Client sind aktiviert.</li> </ul>
<b>Anzeigeeinstellungen einblenden (8.5+)</b>	Wählen Sie diese Option zum Konfigurieren der Anzeigeeinstellungen. Wählen Sie aus dem Dropdownmenü die Gruppe zum Einstellen des Konfigurationszugriffs.
<b>Sperrung zulassen</b>	Wählen Sie diese Option zum Speichern der Berechtigungsebene für das Gerät, sodass die Berechtigungsebene auch verwendet wird, wenn keine Netzwerkverbindung vorhanden ist oder wenn die Konfiguration auf dem Server nicht abgerufen werden konnte. Dies gilt, wenn die Berechtigungsebene hoch ist.
<b>Tastatur- und Mauseinstellungen aktivieren (8.5+)</b>	Wählen Sie diese Option zum Konfigurieren der Tastatur- und Mauseinstellungen.
<b>Administratormodus aktivieren</b>	Wählen Sie diese Option aus, um auf den Administratormodus durch Eingabe von <b>Administratorbenutzername</b> und <b>Administratorkennwort</b> zuzugreifen. Diese Option kann nur aktiviert werden, wenn die Berechtigungsebene auf "niedrig" oder "keine" eingestellt ist.
<b>Verschlüsselte Anmeldeinformationen (8.5+)</b>	Wählen Sie diese Option aus, um die Anmeldeinformationen zu verschlüsseln.
<b>Schaltfläche "Administratormodus" anzeigen (8.5+)</b>	Wählen Sie diese Option, um die Schaltfläche „Lokaler Administratormodus“ im Anmeldefenster anzuzeigen.
<b>Zertifikate automatisch installieren</b>	Wählen Sie diese Option aus, um Zertifikate automatisch zu installieren. Sobald Sie diese Option auswählen, wird die Liste der Zertifikate in der Repository-Datei angezeigt. Wählen Sie das gewünschte Zertifikat aus.
<b>VNC aktivieren</b>	Wählen Sie diese Option zur Aktivierung von VNC-Shadowing (Virtual Network Computing). VNC-Shadowing ist der Prozess, der es Ihnen ermöglicht, im Remote-Zugriff auf die gleiche Sitzung als Benutzer zuzugreifen, zu sehen, was der Benutzer sieht, und Hilfestellung bei spezifischen Problemen mit Anwendungen oder der Sitzung zu geben.
<b>VNC-Kennwort</b>	Ermöglicht die Einrichtung des VNC-Kennworts. Das Kennwort darf aus maximal 16 Zeichen bestehen.
<b>Kennwort verschlüsseln (8.5+)</b>	Wählen Sie diese Option aus, um das Kennwort zu verschlüsseln.

## Konfigurieren von Tastatur- und Anzeigeeinstellungen

Auf dieser Seite können Sie die Anzeigeeinstellungen für den Thin Client-Monitor konfigurieren.

**Tabelle 3. Konfigurieren von Tastatureinstellungen – ThinOS 8.5+**

Option	Beschreibung
<b>Tastaturlayout</b>	Wählen Sie das Layout und die Sprache der Tastatur aus der Dropdownliste aus.

**Tabelle 4. Konfigurieren der Monitor-Anzeigeeinstellungen**

Option	Beschreibung
<b>Monitore</b>	Wählen Sie im Dropdown-Menü <b>Monitore</b> die Anzahl der Anzeigen, die Sie einrichten möchten.
<b>Monitor-Modus</b>	Wählen Sie den Monitor-Modus aus dem Dropdown-Menü <b>Monitor-Modus</b> . Sie können entweder den <b>Spiegelungsmodus</b> oder den <b>Span-Modus</b> wählen.
<b>Monitore automatisch erkennen (8.5+)</b>	<p>Aktivieren Sie das Kontrollkästchen, um die Gesamtzahl der Monitore zu ermitteln, die mit dem System verbunden sind.</p> <p><b>ANMERKUNG:</b> Wenn Sie sowohl die Optionen <b>automatische Monitoreerkennung (8,5 +)</b> als auch <b>Dualmonitor</b> aktivieren ausgewählt haben, bleiben die Konfigurationseinstellungen sowohl für das Einrichten eines einzelnen als auch für zwei Monitore gleich.</p>

## Konfigurieren des visuellen Erlebnisses

Verwenden Sie diese Seite zum Konfigurieren der Einstellungen für das visuelle Erlebnis mit dem Thin Client, wie z. B. Desktopanzeige (Classic oder Zero Launchpad) und Sitzungsfunktionen.

**Tabelle 5. Konfigurieren der Desktopdarstellung**

Option	Beschreibung
<b>Desktophintergrund</b>	Zeigt nur die Bilder an, die in das Datei-Repository hochgeladen wurden. Wenn Sie dieses Kontrollkästchen auswählen, werden das Dropdownmenü für die Hintergrundbild-Datei und das Hintergrundbild-Layout angezeigt.
<b>Unternehmenslogo</b>	Zeigt das Logo auf dem Geräte-Anmeldebildschirm an. Wählen Sie dieses Kontrollkästchen aus, um das <b>Logodatei</b> -Dropdownmenü anzuzeigen. Laden Sie die Logodatei aus dem Datei-Repository-Bestand hoch.

**Tabelle 6. Konfigurieren des visuellen Erlebnisses**

Option	Beschreibung
<b>Klassischer Desktop im Vergleich zu Zero Launchpad</b>	<p>Wählen Sie diese Option zum Definieren des Desktoperlebnisses aus.</p> <p><b>ANMERKUNG:</b> Zero Launchpad wird für ThinOS Lite/ Xenith-Geräte und für Vollbildsitzungen empfohlen. Der klassische Desktop wird für Seamless-Anwendungen empfohlen.</p>
<b>Anmelde-Hauptmenü aktivieren (8.5+)</b>	Wählen Sie diese Option aus, um das Anmelde-Hauptmenü zu aktivieren.
<b>Aktion nach Beenden aller Sitzungen</b>	<p>Wählen Sie diese Option aus, um die Aktion nach dem Schließen der letzten aktiven Sitzung zu definieren. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>Kein</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>· Automatisch abmelden</li> <li>· Das System automatisch herunterfahren</li> <li>· Das System automatisch neu starten</li> </ul>
<b>Zähler für das Herunterfahren/Neustarten</b>	Geben Sie die Sekunden ein, die vor dem Neustart des Systems verstreichen sollen. Die gültigen Werte liegen zwischen 0 und 60.

## Konfigurieren der Zeitzone

Verwenden Sie diese Seite zum Konfigurieren der Thin Client Einstellungen, wie z. B. Zeitserver und Zeitzone.

**Tabelle 7. Zeitzone**

Option	Beschreibung
<b>Zeitzone manuell festlegen</b>	Wählen Sie diese Option aus, um die Einstellungen im Systempräferenzenmenü des Geräts mit der Zeitzone zu überschreiben.
<b>Datumsformat (8.5+)</b>	Wählen Sie das erforderliche Datumsformat aus.
<b>Zeitformat (8.5+)</b>	Wählen Sie das erforderlichen Uhrzeitformat aus.
<b>Zeitserver</b>	Geben Sie die Liste der Zeitserver zum Synchronisieren der Ortszeit getrennt durch Semikolon ein.

## Konfigurieren der allgemeinen Einstellungen

Verwenden Sie diese Seite zum Konfigurieren der Upgradeeinstellungen für die Thin Client-Firmware, wie z. B. Live Upgrade, Logik der Firmware-Aktualisierung und Plattform-Firmware-Zuweisungen.

### ANMERKUNG:

- Remote-Firmware-Abbilderstellung aus der Cloud wird ab der ThinOS Firmware Version 8.0\_037 unterstützt.

**Tabelle 8. Konfigurieren von Anmeldeinstellungen**

Option	Beschreibung
<b>Domänenliste (8.5+)</b>	Geben Sie die Liste der Domains zur Anmeldung beim Broker-Server ein. Trennen Sie die Namen durch ein Semikolon.

**Tabelle 9. Firmware-Upgrade**

Option	Beschreibung
<b>Live-Upgrade deaktivieren</b>	Mit Live Upgrade wird der Thin Client unmittelbar nach dem Herunterladen aktiviert und die neue Firmware basierend auf definierten Richtlinien angewendet. Wenn Sie es vorziehen, dass der Thin Client nur bei jedem Systemstart neue Firmware suchen sollte, deaktivieren Sie die Funktion Live Upgrade.
<b>Definieren der gewünschten Plattform- oder Firmware-Zuordnungen</b>	Diese Option ordnet eine bestimmte Firmware-Version einem anderen Plattformtyp zu. Zum Zuordnen eines Plattformtyps zu einer bestimmten Firmware-Version führen Sie die folgenden Schritte aus:

Option	Beschreibung
	<ol style="list-style-type: none"> <li>1 Wählen Sie eine Plattform aus der Dropdownliste <b>Plattformtyp</b> aus.</li> <li>2 Wählen Sie aus dem Dropdownmenü <b>Automatische Firmware-Bereitstellung</b> eine Firmware-Version aus.</li> </ol> <p>Die Liste der Plattformtypen und die Nummer der Firmware-Version, die derzeit auf der Seite <b>Datei-Repository-Bestand</b> hochgeladen sind, werden angezeigt.</p>

Tabelle 10. Lokale Ressourcen konfigurieren

Option	Beschreibung
<b>Smartcards zuordnen</b>	Wählen Sie diese Option aus, um die Smartcards an die Remotesitzung umzuleiten.
<b>USB-Umleitung aktivieren</b>	Wählen Sie diese Option aus, um die USB-Umleitung auf den Geräten zu aktivieren. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>Festplattengeräte ausschließen</b>	Wählen Sie diese Option zum Ausschließen der Festplattengeräte.
<b>Audiogeräte ausschließen</b>	Wählen Sie diese Option zum Ausschließen der Audiogeräte.
<b>Druckergeräte ausschließen</b>	Wählen Sie diese Option zum Ausschließen der Druckergeräte.
<b>Videogeräte ausschließen</b>	Wählen Sie diese Option zum Ausschließen der Videogeräte.

## Konfigurieren der Broker-Einstellungen

Verwenden Sie diese Seite zum Konfigurieren der Thin Client Remote-Verbindungs- und Broker-Einstellungen, wie z. B. Adressen und Anmeldeinformationen für Broker wie Citrix, Microsoft, VMware und vWorkspace.

Tabelle 11. Konfiguration des Broker-Servers

Option	Beschreibung
<b>Verwendeten Broker auswählen</b>	<p>Wählen Sie diese Option zum Herstellen einer Broker-Verbindung für einen veröffentlichten Desktop. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Citrix</li> <li>• Microsoft</li> <li>• vWorkspace</li> <li>• VMware</li> </ul>
<b>Broker-Server</b>	Geben Sie den Broker-Serverhostnamen oder die IP-Adresse an.
<b>Benutzerdefinierter Citrix-Speichernamen</b>	Geben Sie den Citrix-Speichernamen für die Citrix StoreFront-Verbindung ein. Diese Option gilt nur für Citrix.
<b>Sitzungen, mit denen automatisch eine Verbindung hergestellt werden soll</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu der Sitzung herzustellen.

Option	Beschreibung
	<p><b>ANMERKUNG:</b> Beim Namen des Desktops oder der Anwendung wird zwischen Groß- und Kleinschreibung unterschieden. Verwenden Sie ein Semikolon zum Trennen mehrerer Sitzungen, die automatisch initialisiert werden müssen.</p>
<b>Bei Anmeldung erneut verbinden</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Es ist die erneute Verbindungsherstellung bei aktiven und getrennten Sitzungen möglich. Diese Option gilt nur für Citrix.
<b>Sicherheitsmodus</b>	Wählen Sie diese Option aus, um einen Sicherheitsmodus festzulegen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Diese Option gilt nur für VMware.
<b>Protokoll</b>	Wählen Sie diese Option zur Auswahl eines Protokolls. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Diese Option gilt nur für VMware.
<b>vWorkspace-Gateway aktivieren</b>	Wählen Sie diese Option aus, um die Verwendung der vWorkspace-Gateway-Funktionalität zu aktivieren. Diese Option gilt nur für vWorkspace.

## ThinOS – Erweiterter Modus

Verwenden Sie diese Seite zum Konfigurieren erweiterter Einstellungen für ThinOS-Geräte. Gehen Sie folgendermaßen vor, um die erweiterten Richtlinieneinstellungen zu konfigurieren:

- 1 Wählen Sie **Erweiterte Konfiguration** als Modus der Konfiguration.
- 2 Im Folgenden finden Sie die verfügbaren Richtlinieneinstellungen auf der Seite **ThinOS**.

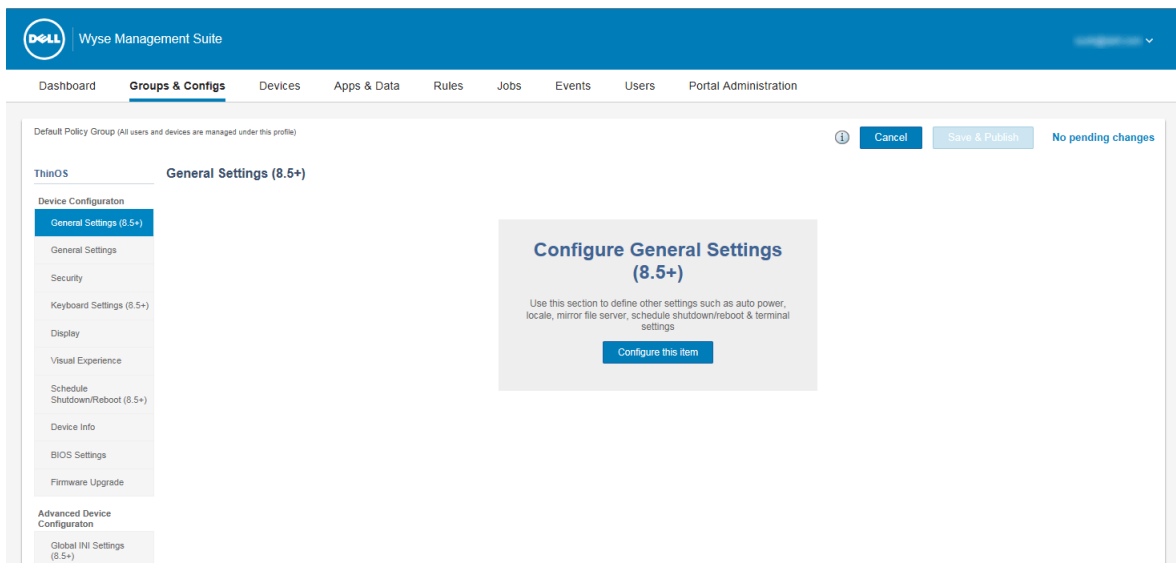


Abbildung 4. ThinOS – Erweiterter Modus

- **Gerätekonfiguration**
- **Erweiterte Gerätekonfiguration**

- Remoteverbindung (alt)
  - Remoteverbindung (8.5+)
  - Drucker (8.5+)
  - Netzwerkeinstellungen (8.5+)
- 3 Klicken Sie zum Speichern der Änderungen auf **Speichern und veröffentlichen**.
  - 4 Klicken Sie auf **Richtlinie entfernen** um zurück zur Seite **ThinOS** zu gelangen.
  - 5 Klicken Sie auf **Abbrechen**, um zur Seite **Gruppen und Konfigurationen** zurückzukehren.

## Konfigurieren der allgemeinen Einstellungen

Verwenden Sie die Seite **Allgemeine Einstellungen** zum Konfigurieren der allgemeinen Einstellungen für den Thin Client, wie z. B. Einstellungen für automatisches Hochfahren, lokale Einstellungen, Spiegeldateiservereinstellungen und Terminaleinstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 12. Konfigurieren der allgemeinen Einstellungen**

Option	Beschreibung
<b>Automatisches Hochfahren</b>	Das Kontrollkästchen <b>Automatisches Hochfahren</b> gibt an, wie das System beim erstmaligen Einschalten gestartet werden soll.

**Tabelle 13. Konfigurieren von Tastaturoptionen**

Option	Beschreibung
<b>Sprachdatei laden</b>	Wählen Sie diese Option zur Installation der Sprachdateien auf ThinOS-Geräten.
<b>Systemsprache</b>	Wählen Sie diese Option zum Einstellen der Sprache für das System aus. Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
<b>Name der Gebietsschemadatei</b>	Aktivieren Sie diese Option, um die Zertifikate auf den Geräten zu installieren. Wählen Sie aus der Dropdownliste die Zertifikate aus, die dem Datei-Repository hinzugefügt wurden.
<b>Name der Schriftartdatei</b>	Aktivieren Sie diese Option, um die Schriftdatei auf den Geräten zu installieren. Wählen Sie aus der Dropdownliste die Schriftdateien aus, die dem Datei-Repository hinzugefügt wurden.

**Tabelle 14. Konfigurieren des Spiegeldateiservers**

Option	Beschreibung
<b>Spiegeldateiserver</b>	Wenn der <b>Dateiserver</b> offline ist, können Sie mit dieser Einstellung eine lokale Kopie der Konfiguration im Cache speichern.

**Tabelle 15. Konfigurieren von Terminal Gateway-Einstellungen**

Option	Beschreibung
<b>Terminalname</b>	Geben Sie den Terminalnamen ein. Sie können auch die Systemvariablen zum automatischen Umbenennen von mehreren Geräten verwenden.

Option	Beschreibung
	<p><b>ANMERKUNG:</b> Wenn Sie Änderungen an diesen Einstellungen vornehmen, wird der Thin Client neu gestartet. Ab ThinOS 8.5_020 können Sie den Neustart verzögern, indem Sie in den Allgemeinen Einstellungen die Option An Neustart erinnern aktivieren.</p>
<b>Neustart des Terminals</b>	Wenn diese Einstellung aktiviert ist, wird das System gezwungen, neu zu starten, sobald der Terminalname geändert wurde. Starten Sie das System neu, um die Änderungen anzuzeigen.
<b>Inaktiv</b>	Wählen Sie diese Option aus, um das System neu zu starten oder herunterzufahren, je nachdem, welche Option Sie aus der Dropdownliste <b>Aktion nach Beendigung aller Sitzungen</b> in der Richtlinieneinstellung <b>Visuelles Erlebnis</b> für die ThinOS-Geräte ausgewählt haben. Geben Sie den Zeitwert in Minuten ein. Der Bereich der inaktiven Zeit beträgt 0 bis 480 Sekunden.
<b>Keine Sitzungszeit</b>	Wählen Sie diese Option aus, um das System neu zu starten oder herunterzufahren, je nachdem, welche Option Sie aus der Dropdownliste <b>Aktion nach Beendigung aller Sitzungen</b> in der Richtlinieneinstellung <b>Visuelles Erlebnis</b> für die ThinOS-Geräte ausgewählt haben. Geben Sie den Zeitwert in Minuten ein. Der Bereich der inaktiven Zeit beträgt 0 bis 480.  <p><b>ANMERKUNG:</b> Die Einstellung ist nur relevant, wenn der Wert Inaktiv auf 0 gesetzt ist.</p>

**Tabelle 16. Konfigurieren der Einstellungen für den Wyse Management Suite-Agenten**

Option	Beschreibung
<b>Erinnerung aktivieren</b>	Wenn diese Einstellung aktiviert ist, wird auf dem Thin Client ein Warndialogfeld angezeigt, wenn nach einer Richtlinienänderung ein Neustart erforderlich ist.

**Tabelle 17. Konfigurieren der Audioeinstellungen für ThinOS 8.6 und höher**

Option	Beschreibung
<b>Audioeinstellungen konfigurieren</b>	Wählen Sie diese Option aus, um die Audioeinstellungen zu konfigurieren.
<b>Popup für analoge Audiobuchse</b>	Durch Auswahl dieser Option wird die Audioauswahlmeldung beim Plug-in des analogen Headsets angezeigt.
<b>Stumm</b>	Wählen Sie diese Option zum Aktivieren oder Deaktivieren der Stummschaltung. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Keine Stummschaltung</li> <li>• Audio stummschalten</li> <li>• Audio und Signaltöne stummschalten</li> <li>• Signaltöne stummschalten</li> </ul>
<b>Mikrofonlautstärke</b>	Wählen Sie diese Option zum Einstellen der Mikrofonlautstärke. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Hoch</li> <li>• Mittel</li> <li>• Niedrig</li> </ul>

Option	Beschreibung
<b>Mikrofon stumm schalten</b>	Wählen Sie diese Option aus, um das Mikrofon stummzuschalten.
<b>Audio über Displayport deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der Audiofunktion über den Displayport.
<b>Mikrofonverstärkung</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Die verfügbaren Optionen sind: <ul style="list-style-type: none"> <li>• Ja: aktiviert die integrierte Mikrofonverstärkung.</li> <li>• Nein: deaktiviert die integrierte Mikrofonverstärkung.</li> <li>• 1, 2, 3, 4: erhöht die Dezibelwert des Mikrofons.</li> </ul>
<b>Pufferungs-Cache wiedergeben</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Diese Option ermöglicht das Konfigurieren der minimalen Pufferung der ThinOS-Audiowiedergabe in Einheiten von zehn Millisekunden. Diese Option kann verwendet werden, wenn die Netzwerkbandbreite nicht groß genug für die reibungslose Wiedergabe von Audio ist. Die verfügbaren Optionen sind: <ul style="list-style-type: none"> <li>• 1: ThinOS puffert mindestens 10 ms an Audiodaten beim Abspielen von Audio.</li> <li>• 50: ThinOS puffert mindestens 500 ms (0,5 s) an Audiodaten beim Abspielen von Audio.</li> </ul>
<b>Lautsprecher aktivieren</b>	Wählen Sie diese Option aus, um den internen Lautsprecher zu aktivieren.
<b>Wiedergabegerät</b>	Geben Sie den Namen des Wiedergabegeräts ein.
<b>Aufnahmegerät</b>	Geben Sie den Namen des Aufnahmegeräts ein.
<b>Mikrofonverstärkungsgerät</b>	Geben Sie den Gerätenamen ein, auf dem die Mikrofonverstärkung stattfinden soll.
<b>Mikrofonverstärkungsgrad</b>	Verbessert die Mikrofonverstärkung um die Anzahl des angegebenen Werts.
<b>Volume</b>	Wählen Sie aus der Dropdownliste die Lautstärke aus:



**Tabelle 18. Konfigurieren der Mauseinstellungen für ThinOS 8.6 und höher**

Option	Beschreibung
<b>Mauseinstellungen konfigurieren</b>	Wählen Sie diese Option aus, um die Mauseinstellungen zu konfigurieren.
<b>Mausgeschwindigkeit</b>	Wählen Sie aus der Dropdownliste die Mausgeschwindigkeit aus.
<b>Maustasten vertauschen</b>	Wählen Sie diese Option aus, um die Maustasten zu vertauschen.
<b>Touchscreen-Ziehen</b>	Wählen Sie diese Option zur Aktivierung der Option zum Ziehen auf dem Touchscreen aus.
<b>Mausrad umkehren</b>	Wählen Sie diese Option aus, um das Mausrad umzukehren.
<b>Großer Cursor</b>	Wählen Sie diese Option aus, um die Größe der lokalen Maus zu verdoppeln.
<b>Deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren des Mauszeigers auf dem Bildschirm aus.

## Konfigurieren der allgemeinen Einstellungen

Verwenden Sie die Seite **Allgemeine Einstellungen** zum Konfigurieren der ThinOS Thin Client Einstellungen, wie z. B. Anmeldeeinstellungen und Zeitzone.

**Tabelle 19. Konfigurieren von Anmeldeeinstellungen**

Option	Beschreibung
<b>Standardbenutzername</b>	Geben Sie den Standardbenutzernamen für die lokale Anmeldung am Bildschirm ein.
<b>Standardkennwort</b>	Geben Sie das Standardkennwort für die lokale Anmeldung am Bildschirm ein.
<b>Domainname</b>	Geben Sie den Standard-Domänennamen für die lokale Anmeldung am Bildschirm ein.   <b>ANMERKUNG: Sie können mehrere Domainnamen durch Komma getrennt mit höchstens 31 Zeichen eingeben.</b>
<b>Letzten Benutzernamen bei der Abmeldung merken</b>	Wählen Sie diese Option zum Speichern des Benutzernamens, wenn Sie sich vom System abmelden. Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.   <b>ANMERKUNG: Der Benutzername wird nicht gespeichert, wenn das System neu gestartet oder ausgeschaltet wird.</b>
<b>Domänenfeld deaktivieren (8.5+)</b>	Wählen Sie das Kontrollkästchen zum Deaktivieren der Option Domänenfeld im Anmeldefenster.
<b>Domänenliste (8.5+)</b>	Geben Sie die Liste der genannten Domains im Anmeldefenster ein. Verwenden Sie durch Semikolon getrennte Domainnamen.
<b>Letzten Benutzernamen und/oder Domain beim Neustart/Herunterfahren merken</b>	Wählen Sie diese Option zum Speichern von Benutzername oder Domain, wenn das System neu gestartet oder ausgeschaltet wird.

**Tabelle 20. Konfigurieren von Zeitzoneneinstellungen**

Option	Beschreibung
<b>Zeitzone manuell festlegen</b>	Wählen Sie das Kontrollkästchen aus, um die Einstellungen im Systempräferenzenmenü zu überschreiben. Wählen Sie aus den Dropdownmenüs <b>Zeitzone</b> und <b>Sommerzeit aktivieren</b> Ihre bevorzugte Option.
<b>Datumsformat (8.5+)</b>	Wählen Sie aus dem Dropdownmenü <b>Datumsformat (8.5+)</b> das gewünschte Format aus.
<b>Zeitformat (8.5+)</b>	Wählen Sie aus der Dropdownmenü <b>Zeitformat (8.5+)</b> das gewünschte Format aus.
<b>Zeitserver</b>	Geben Sie die Liste der Zeitserver zum Synchronisieren der Ortszeit getrennt durch Semikolon ein.

## Konfigurieren der Sicherheitseinstellungen

Verwenden Sie die Seite **Sicherheitseinstellungen** zum Konfigurieren der ThinOS Thin Client Sicherheitseinstellungen, wie z. B. Anmeldeeinstellungen, Berechtigungseinstellungen, Zurücksetzen mit G-Taste usw.

**Tabelle 21. Konfigurieren von Anmeldeinstellungen**

Option	Beschreibung
<b>Domain-Anmeldung erforderlich machen</b>	Wählen Sie aus dem Dropdownmenü <b>Domain-Anmeldung erforderlich machen</b> die gewünschte Option.
<b>Gastbenutzer deaktivieren</b>	Aktivieren Sie das Kontrollkästchen, um das Konto von lokalem Gastbenutzer zu deaktivieren.
<b>Erneute Eingabe des Kennworts erforderlich machen</b>	Aktivieren Sie das Kontrollkästchen, um das erneute Eingeben des Kennworts bei der Anmeldung erforderlich zu machen.
<b>Smartcard erforderlich machen</b>	Wählen Sie aus dem Dropdownmenü <b>Smartcard erforderlich machen</b> die gewünschte Option aus.
<b>Symbolgruppenstil</b>	Wählen Sie im Dropdown-Menü <b>Symbolgruppenstil</b> die Art des Gruppierungsstils für Symbole auf dem Desktop aus. Wenn der Symbolgruppenstil als Ordner ausgewählt ist, werden die veröffentlichten Anwendungen in einem Ordner zusammengefasst.

**Tabelle 22. Konfigurieren von Berechtigungseinstellungen**

Option	Beschreibung
<b>Berechtigungsebene</b>	Wählen Sie diese Option zum Definieren der Standard-Berechtigungsstufe während des Systemstarts. Wählen Sie im Dropdownmenü eine beliebige der folgenden Stufen aus: <ul style="list-style-type: none"> <li>· Keine – Deaktiviert alle Systemeinstellungsmenüs.</li> <li>· Hoch – Deaktiviert die Verbindungseinstellungen, aber die lokale Anpassung ist aktiviert.</li> <li>· Niedrig – Alle Einstellungen auf dem lokalen Client sind aktiviert.</li> </ul>
<b>Anzeigeeinstellungen einblenden (8.5+)</b>	Wählen Sie diese Option zum Konfigurieren der Anzeigeeinstellungen. Wählen Sie aus dem Dropdownmenü die Gruppe zum Einstellen des Konfigurationszugriffs.
<b>Tastatur- und Mauseinstellungen aktivieren (8.5+)</b>	Wählen Sie diese Option zum Konfigurieren der Tastatur- und Mauseinstellungen.
<b>Datums- und Zeitangaben deaktivieren (8.5+)</b>	Wählen Sie diese Option zum Konfigurieren der Einstellungen für Datum und Uhrzeit.
<b>Netzwerkstandort für Upload (8.5+)</b>	Geben Sie den Speicherort zum Hochladen der Netzwerkverfolgung, Netzwerkaufnahme und Protokolldateien ein.

**Tabelle 23. Konfigurieren des Administratormodus**

Option	Beschreibung
<b>Administratormodus aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, um den Administratormodus zu aktivieren. Wenn die Berechtigungsstufe <b>niedrig</b> oder <b>keine</b> ist, können Sie den Zugriff auf den Administratormodus aktivieren, indem Sie den Benutzernamen und das Kennwort angeben.
<b>Verschlüsselte Anmeldeinformationen (8.5+)</b>	Wählen Sie das Kontrollkästchen zum Verschlüsseln der Anmeldeinformationen.

Option	Beschreibung
Schaltfläche "Administratormodus" anzeigen (8.5+)	Wählen Sie das Kontrollkästchen, um die Option "Administratormodus" im Anmeldefenster anzuzeigen.

Tabelle 24. Konfigurieren der allgemeinen Einstellungen


Option	Beschreibung
Zurücksetzen mit G-Taste aktivieren	Wählen Sie diese Option aus, um das Gerät auf Werkseinstellungen zurückzusetzen. Drücken Sie beim Neustart des Systems die G-Taste zum Zurücksetzen auf Werkseinstellungen.
Ablaufverfolgung aktivieren	Wählen Sie diese Option aus, um die Dateien zu verfolgen. Dieser Parameter aktiviert den ICA- oder RDP-Verfolgungsmodus und die Ablaufverfolgungsdatei wird in dem Verzeichnis erstellt.
Zertifikat entfernen (8.5+)	Wählen Sie diese Option zum Entfernen des Zertifikats.
Zertifikat löschen (8.5+)	Wählen Sie diese Option aus, um das Zertifikat zu löschen. Geben Sie den Namen des Zertifikats ein, das Sie löschen möchten.
Zertifikate automatisch installieren	Wählen Sie diese Option zur automatischen Installation des Zertifikats.
ThinPrint Dienst deaktivieren	Wählen Sie diese Option zum Deaktivieren des <b>ThinPrint</b> -Dienstes.
Lokalen Flash verschlüsseln	Wählen Sie diese Option zum Konfigurieren der lokalen Einstellungen sowie zur Eingabe der Benutzeranmeldeinformationen. Markieren Sie dieses Kontrollkästchen, wenn Sie den lokalen Flash verschlüsseln möchten.
VNC-Spiegelung deaktivieren	Wählen Sie diese Option zum Deaktivieren der VNC-Spiegelung.
Taste für schnelle Trennung	Wählen Sie diese Option aus, um die Taste für schnelle Trennung zu verwenden.   <b>ANMERKUNG: Drücken Sie die Taste &lt;F12&gt;, um sich von Citrix-Sitzungen abzumelden.</b>

Tabelle 25. Konfigurieren der Sicherheitsrichtlinie

Option	Beschreibung
Sicherheitsrichtlinie (8.5+)	Wählen Sie aus dem Dropdownmenü <b>Sicherheitsrichtlinie (8.5+)</b> den globalen Sicherheitsmodus für SSL-Verbindungen.
Gesichertes Netzwerkprotokoll (8.5+)	Wählen Sie diese Option aus, um das Netzwerkprotokoll zu sichern. Die unsicheren Netzwerkprotokolle werden deaktiviert.
TLS-Mindestversion (8.5+)	Wählen Sie diese Option aus, um die Mindestversion der SSL-Verbindung für die ThinOS Geräte zu wählen.
TLS-Maximalversion (8.5+)	Wählen Sie diese Option zur Auswahl der maximalen Version der SSL-Verbindung für die ThinOS Geräte.
DNS-Dateiserver Ermittlung (8.5+)	Wählen Sie diese Option zur Ermittlung des DNS-Dateiservers.

**Tabelle 26. Konfigurieren der VNC-Einstellungen**

Option	Beschreibung
<b>VNC aktivieren</b>	Wählen Sie diese Option zur Aktivierung von VNC-Shadowing.
<b>VNC-Kennwort</b>	Geben Sie das VNC-Kennwort mit bis zu 16 Zeichen ein.
<b>Kennwort verschlüsseln (8.5+)</b>	Wählen Sie diese Option aus, um das Kennwort zu verschlüsseln.
<b>Maximale Anzahl gleichzeitiger VNC-Verbindungen (8.5+)</b>	Wählen Sie aus dem Dropdownmenü die maximale Anzahl an gleichzeitigen VNC-Verbindungen.
<b>Zlib-Komprimierung (8.5+)</b>	Wählen Sie dieses Kontrollkästchen aus, um die Zlib-Komprimierung zu aktivieren.
<b>Benutzer beim Start auffordern</b>	Wählen Sie diese Option zum Durchführen des Shadowing-Vorgangs im Terminal.
<b>Zeitlimit für die Benutzerabfrage</b>	Geben Sie die maximale Zeitdauer in Sekunden ein, um die Shadowing-Sitzung anzunehmen oder abzulehnen. Der Bereich liegt zwischen 10 und 600 Sekunden.
<b>Benutzer am Ende auffordern</b>	Aktivieren Sie das Kontrollkästchen, um das Ende einer Remote-Shadowing-Sitzung zu melden.
<b>Nur Ansicht</b>	Wählen Sie das Kontrollkästchen zum Deaktivieren der Tastatur- oder Mausereignisse auf dem System während einer Shadowing-Sitzung.
<b>8-Bit erzwingen</b>	Wählen Sie diese Option zum Konfigurieren der Anzeigeeinstellungen. Wählen Sie das Kontrollkästchen zur Verwendung von 8-Bit pro Pixel aus.

**Tabelle 27. Konfigurieren von WDM-Diensten**

Option	Beschreibung
<b>WDM-Dienst deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren des WDM-Dienstes.
<b>Schnellmodus (8.5+)</b>	Wählen Sie diese Option zur Beschleunigung des Startens der ThinOS-Geräte.

## Konfigurieren der Tastatureinstellungen

Verwenden Sie die Seite **Tastatureinstellungen** zum Konfigurieren der Tastaturlayouts und der Funktionsweise der Tastenkombinationen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 28. Konfigurieren der Tastatureinstellungen**

Option	Beschreibung
<b>Zeichensatz</b>	Wählen Sie diese Option aus, um einen entsprechenden Zeichensatz einzustellen. Wählen Sie aus der Dropdownliste Ihren bevorzugten Zeichensatz.
<b>Tastaturlayout</b>	Wählen Sie diese Option aus, um ein entsprechendes Tastaturlayout einzustellen. Wählen Sie aus der Dropdownliste Ihr bevorzugtes Tastaturlayout.
<b>Tastatur-Wiederholverzögerung</b>	Wählen Sie diese Option aus, um die Zeit festzulegen, die eine Taste gedrückt bleiben kann, ohne dass der Buchstabe als Eingabe

Option	Beschreibung
	wiederholt wird. Wählen Sie in der Dropdownliste nach Bedarf eine der Optionen aus.
<b>Tastatur-Wiederholrate</b>	Wählen Sie diese Option aus, um die Wiederholrate Ihrer Tastatur einzustellen. Die Wiederholrate gibt die Geschwindigkeit an, mit der die Tasteneingabe beim Drücken und Halten der Taste auf der Tastatur wiederholt wird. Wählen Sie in der Dropdownliste nach Bedarf eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Langsam</li> <li>· Normal</li> <li>· Schnell</li> </ul>
<b>Schlüsselsequenz</b>	Aktivieren Sie das Kontrollkästchen, um die Schlüsselsequenz zu aktivieren.
<b>Strg-Alt-Entf</b>	Drücken Sie die Tasten <b>Strg-Alt-Entf</b> zum Sperren des Systems.
<b>Strg+Alt+Pfeil nach oben</b>	Drücken Sie die Tasten <b>Strg+Alt+Pfeil nach oben</b> zum Wechseln der Sitzung zwischen Vollbildschirm- und Fenstermodus.
<b>Strg+Alt+Pfeil nach unten</b>	Drücken Sie die Tasten <b>Strg+Alt+Pfeil nach unten</b> , um zwischen der Aufgabenauswahl umzuschalten.
<b>Strg+Alt+Nach-Links</b>	Drücken Sie die Tasten <b>Strg+Alt+Nach-Links</b> , um das System zu sperren.
<b>Strg+Alt-Nach-Rechts</b>	Drücken Sie die Tasten <b>Strg+Alt-Nach-Rechts</b> , um das System zu sperren.
<b>Win+L</b>	Drücken Sie die Tasten <b>Win+L</b> , um das System zu sperren.
<b>Alt-Tab</b>	Drücken Sie die Tasten <b>Alt+Tab</b> , um das System zu sperren.

## Konfigurieren der Anzeigeeinstellungen

Verwenden Sie die Seite **Anzeigeeinstellungen** zum Konfigurieren der ThinOS Thin Client Monitor-Anzeigeeinstellungen, wie z. B. Auflösung, Drehung und Farbtiefe.

**Tabelle 29. Konfigurieren der Monitor-Anzeigeeinstellungen**

Option	Beschreibung
<b>Monitore</b>	Wählen Sie im Dropdown-Menü <b>Monitore</b> die Anzahl der Anzeigen, die Sie einrichten möchten.
<b>Monitor-Modus</b>	Wählen Sie den Monitor-Modus aus dem Dropdown-Menü <b>Monitor-Modus</b> . Sie können entweder den <b>Spiegelungsmodus</b> oder den <b>Span-Modus</b> wählen.
<b>Unterstützung mehrerer Monitore</b>	Diese Option ist aktiviert, wenn Sie in der Dropdown-Liste <b>Monitore</b> die Option <b>Mehrere Monitore aktivieren</b> auswählen. Klicken Sie auf <b>+ Element hinzufügen</b> , um das Setup für mehrere Monitore zu konfigurieren.
<b>Hauptbildschirm</b>	Wählen Sie diese Option, um auf den Hauptbildschirm zuzugreifen. Wählen Sie aus dem Dropdown-Menü <b>Hauptbildschirm</b> Ihre bevorzugte Option. Für den Dual-Monitor-Modus müssen Sie entweder <b>Bildschirm 1</b> oder <b>Bildschirm 2</b> auswählen.

Option	Beschreibung
<b>Ausrichtung</b>	Wählen Sie diese Option aus, um den Bildschirm auszurichten. Wählen Sie aus dem Dropdownmenü <b>Ausrichtung</b> Ihre bevorzugte Option.
<b>Layout – ThinOS 8.5+</b>	Wählen Sie diese Option, um entweder <b>Querformat</b> oder <b>Hochformat</b> als Layout einzustellen.
<b>Taskleiste – ThinOS 8.5+</b>	Wählen Sie diese Option, um die Platzierung der Taskleiste auf dem Bildschirm festzulegen. Wählen Sie aus dem Dropdownmenü <b>Taskleiste (8.5+)</b> entweder <b>Hauptbildschirm</b> oder <b>Gesamter Bildschirm</b> .
<b>Monitore automatisch erkennen – ThinOS 8.5+</b>	Aktivieren Sie das Kontrollkästchen, um die Gesamtzahl der Monitore zu ermitteln, die mit dem System verbunden sind.  <b>ⓘ ANMERKUNG: Wenn Sie sowohl die Optionen automatische Monitoreerkennung (8,5 +) als auch Dualmonitor aktivieren ausgewählt haben, bleiben die Konfigurationseinstellungen sowohl für das Einrichten eines einzelnen als auch für zwei Monitore gleich.</b>
<b>Desktop-Farbtiefe</b>	Wählen Sie diese Option aus, um die Farbtiefe für Ihren Desktop festzulegen. Wählen Sie aus den Dropdownmenü <b>Desktop-Farbtiefe</b> entweder <b>16-Bit</b> oder <b>32-Bit</b> .  <b>ⓘ ANMERKUNG: Wenn Sie Änderungen an dieser Einstellung vornehmen, wird der Thin Client neu gestartet. Ab ThinOS 8.5_020 können Sie den Neustart verzögern, indem Sie in den Allgemeinen Einstellungen die Option An Neustart erinnern aktivieren.</b>

**Tabelle 30. Konfigurieren der primären Monitoreinstellungen**

Option	Beschreibung
<b>Monitorauflösung</b>	Wählen Sie diese Option aus, um die Auflösung Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Auflösung für Ihren Monitor aus.
<b>Monitordrehung</b>	Wählen Sie diese Option zum Definieren der Drehung aus. Wählen Sie aus dem Dropdownmenü die geeignete Drehung aus:
<b>Monitorwiederholfrequenz – ThinOS (8.5+)</b>	Wählen Sie diese Option aus, um die Aktualisierungsrate Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Aktualisierungsrate für Ihren Monitor aus.

**Tabelle 31. Konfigurieren der sekundären Monitoreinstellungen**

Option	Beschreibung
<b>Monitorauflösung (8.5+)</b>	Wählen Sie diese Option aus, um die Auflösung Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Auflösung für Ihren Monitor aus.
<b>Monitordrehung (8.5+)</b>	Wählen Sie diese Option aus, um die Richtung "Links", "Rechts" oder "Keine" zum Aktivieren der Drehung festzulegen. Wählen Sie aus dem Dropdownmenü die geeignete Drehung aus:

Option	Beschreibung
<b>Monitorwiederholfrequenz (8.5+)</b>	Wählen Sie diese Option aus, um die Aktualisierungsrate Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Aktualisierungsrate für Ihren Monitor aus.

**Tabelle 32. Konfigurieren von Multi-Touch-Einstellungen**

Option	Beschreibung
<b>Multi-Touch</b>	Wählen Sie diese Option, um Multi-Touch-Unterstützung auf Dell Touchscreen-Monitoren P2418HT und ELO zu aktivieren. Multi-Touch wird auf der lokalen ThinOS-Benutzeroberfläche nicht unterstützt und funktioniert nur mit RDP-Verbindungen.

**Tabelle 33. Konfigurieren von Bildschirmschonereinstellungen**

Option	Beschreibung
<b>Bildschirmschoner (8.5+)</b>	Geben Sie das Bildschirmschonerintervall in Minuten ein.
<b>Terminal sperren (8.5+)</b>	Wählen Sie diese Option, um das Terminal in den Sperrmodus zu versetzen, wenn der Bildschirmschoner aktiviert ist. Wählen Sie aus dem Dropdownmenü <b>Terminal sperren (8.5+)</b> eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• 0 – Deaktiviert</li> <li>• 1 – Entsperrn nur mit Kennwort und Hintergrundbild wird angezeigt</li> <li>• 2 – Entsperrn nur mit Kennwort und ein schwarzer Bildschirm wird angezeigt</li> <li>• 3 – Entsperrn mit Benutzername und Kennwort und ein schwarzer Bildschirm wird angezeigt</li> </ul>
<b>Bildschirmschonertyp (8.5+)</b>	Wählen Sie diese Option aus, um anzugeben, welchen Bildschirmschoner Sie verwenden möchten. Wählen Sie aus dem Dropdownmenü <b>Bildschirmschonertyp (8.5+)</b> die gewünschte Option.
<b>Ruhezustand (8.5+)</b>	Wählen Sie diese Option aus, um das Zeitintervall in Minuten anzugeben, nachdem der Bildschirmschoner gestoppt und der Monitor ausgeschaltet werden. Wählen Sie aus dem Dropdownmenü <b>Ruhezustand (8.5+)</b> die gewünschte Option aus.
<b>Stunden anstelle von Minuten verwenden (8.6 +)</b>	Wählen Sie diese Option, um die Zeit des Bildschirmschoners in Stunden zu ändern.

## Konfigurieren der Einstellungen für das visuelle Erlebnis

Auf der Seite **Visuelles Erlebnis** können Sie die Einstellungen zum visuellen Erlebnis mit dem ThinOS Thin Client konfigurieren, z. B. durch einen Desktophintergrund oder die Funktionsweise beim Beenden einer Sitzung.

**Tabelle 34. Konfigurieren der Desktopdarstellung**

Option	Beschreibung
<b>Desktopfarbe (8.6+)</b>	Geben Sie die Hintergrundfarbe des lokalen Desktops an.
<b>Desktophintergrund</b>	<p>Zeigt nur die Bilder an, die in das Datei-Repository hochgeladen wurden. Wenn Sie dieses Kontrollkästchen auswählen, werden die folgenden Optionen angezeigt:</p> <ul style="list-style-type: none"> <li>• Hintergrundbild deaktivieren</li> <li>• Hintergrundbild aktivieren</li> <li>• Dell Standard-Hintergrundbild (8.6+)</li> <li>• Wyse Standard-Hintergrundbild (8.6+)</li> </ul> <p><b>ANMERKUNG:</b> Wenn Sie die Option zum Aktivieren des Hintergrundbilds auswählen, werden die Hintergrundbild-Datei und das Hintergrundbild-Layout angezeigt.</p>
<b>Unternehmenslogo</b>	Zeigt das Logo auf dem Geräte-Anmeldebildschirm an. Wählen Sie dieses Kontrollkästchen aus, um das <b>Logodatei</b> -Dropdownmenü anzuzeigen. Laden Sie die Logodatei aus dem Datei-Repository-Bestand hoch.
<b>EULA bei Anmeldung</b>	Zeigt bei jeder Anmeldung die Endbenutzer-Lizenzvereinbarung an. Wählen Sie dieses Kontrollkästchen aus, um das Dropdownmenü <b>EULA-Datei</b> anzuzeigen. Mithilfe dieser Option können Sie eine unformatierte Textdatei hochladen.

**Tabelle 35. Konfigurieren des visuellen Erlebnisses**

Option	Beschreibung
<b>Klassischer Desktop im Vergleich zu Zero Launchpad</b>	<p>Wählen Sie diese Option zum Definieren des Desktoperlebnisses aus.</p> <p><b>ANMERKUNG:</b> Zero Launchpad wird für ThinOS Lite oder Xenith-Geräte und für Vollbildsitzungen empfohlen. Der klassische Desktop wird für Seamless-Anwendungen empfohlen.</p>
<b>Schließen der Symbolleiste verhindern, wenn sich der Mauszeiger nicht bewegt</b>	Markieren Sie dieses Kontrollkästchen, wenn Sie das Schließen der Symbolleiste verhindern möchten, es sei denn, der Mausfokus wird von ihr weg verschoben.
<b>Startsymbol deaktivieren</b>	Wählen Sie diese Option aus, um das Startsymbol zu deaktivieren.
<b>Anmelde-Hauptmenü aktivieren (8.5+)</b>	Wählen Sie das Kontrollkästchen zum Aktivieren des Hauptmenü-Dialogs auf dem Desktop, wenn Sie sich beim System anmelden.
<b>Aktivierung der Zero Taskleiste am rechten Rand aktivieren</b>	<p>Wählen Sie diese Option, um eine beliebige der folgenden Optionen zur Aktivierung der Zero Taskleiste auszuwählen:</p> <ul style="list-style-type: none"> <li>• Nein</li> <li>• Wenn der Mauszeiger über etwas bewegt wird nach den angegebenen Sekunden</li> <li>• Nur nach Klicken</li> </ul>
<b>Taskleiste Maus deaktivieren</b>	Wählen Sie das Kontrollkästchen zum Deaktivieren der Mausfunktionalität, wenn die Zero-Taskleiste aktiviert ist.

Option	Beschreibung
<b>Taskleisten-Klick (8.5+)</b>	Wählen Sie das Kontrollkästchen zum Aktivieren der Taskleisten-Klick-Option wenn die Zero-Taskleisten-Option aktiviert ist.
<b>Anzahl der Sekunden, bevor die Taskleiste aktiviert wird</b>	Wählen Sie diese Option aus, um die Zeit (in Sekunden) festzulegen, bevor die Taskleiste aktiviert wird. Wählen Sie basierend auf Ihren Präferenzen einen der folgenden Zeitwerte: <ul style="list-style-type: none"> <li>· 0,5 Sekunden</li> <li>· 1 Sekunde</li> <li>· 1,5 Sekunden</li> <li>· 2 Sekunden</li> </ul>
<b>Aktion nach Beenden aller Sitzungen</b>	Wählen Sie diese Option aus, um die Aktion nach dem Schließen der letzten aktiven Sitzung zu definieren. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Kein</li> <li>· Automatisch abmelden</li> <li>· Das System automatisch herunterfahren</li> <li>· Das System automatisch neu starten</li> </ul>

## Einstellungen für den Zeitplan für das Herunterfahren/Neustarten

Verwenden Sie die Seite **Zeitplan für das Herunterfahren/Neustarten (8.5+)** zum Konfigurieren eines Zeitplans für das Herunterfahren oder Neustarten für Geräte mit ThinOS 8.5 und höher.

**Tabelle 36. Zeitplan für das Herunterfahren oder Neustarten**

Option	Beschreibung
<b>Geplanter Neustart</b>	Aktivieren Sie das Kontrollkästchen, um Uhrzeit oder Tag für den Zeitplan für einen Systemneustart festzulegen.
<b>Geplantes Herunterfahren</b>	Aktivieren Sie das Kontrollkästchen, um Uhrzeit oder Tag für den Zeitplan für ein Herunterfahren des Systems festzulegen.
<b>Leerlaufzeit</b>	Geben Sie die Leerlaufzeit an. Das System wird in einer aktiven Sitzung neu gestartet, wenn der Wert der Leerlaufzeit auf 10 Minuten eingestellt ist.
<b>Neustart-/Abschaltungszeit</b>	Geben Sie die Zeit ein, zu der das System neu gestartet oder heruntergefahren werden muss. Stellen Sie die Uhrzeit im 24-Stunden-Format ein.
<b>Neustart-/Abschaltungsende</b>	Geben Sie die Zeit ein, zu der der Neustart oder das Herunterfahren des Systems gestoppt wird. Stellen Sie die Uhrzeit im 24-Stunden-Format ein.
<b>Tage</b>	Aktivieren Sie das Kontrollkästchen, um die Tage festzulegen, an denen Sie das System neu starten oder herunterfahren möchten.
<b>Woche</b>	Wählen Sie aus dem Dropdown-Menü die Anzahl der Wochen, nach denen der Thin Client neu gestartet werden muss.

## Geräteinformationen konfigurieren

Verwenden Sie die Seite **Geräteinfo**, um die ThinOS-Gerätedetails anzuzeigen.

**Tabelle 37. Geräteinformationen konfigurieren**

Option	Beschreibung
<b>Standort</b>	Geben Sie den Gerätestandort ein.
<b>Kontakt</b>	Geben Sie die Kontaktdaten des Geräts ein.
<b>Benutzerdefiniert 1 bis 3</b>	Geben Sie benutzerdefinierte Werte ein.

## Konfigurieren der BIOS-Einstellungen

Verwenden Sie Seite **BIOS-Einstellungen** für die Konfiguration der BIOS-Einstellungen von ThinOS Thin Clients.

**Tabelle 38. Systemkonfiguration**

Option	Beschreibung
<b>Audio aktivieren</b>	Markieren Sie dieses Kontrollkästchen, um das Audiogerät zu aktivieren.
<b>OSD aktivieren</b>	Aktivieren Sie dieses Kontrollkästchen, um die OSD-Benutzeroberfläche (Object Storage Device) zu aktivieren. Diese Option steht nur auf dem Wyse 5470 All-in-One Thin Client zur Verfügung.
<b>MAC-Passthrough konfigurieren</b>	<p>Wählen Sie in der Dropdown-Liste die Option aus, mit der der Computer die MAC-Passthrough-Funktion aktivieren oder deaktivieren kann. Die verfügbaren Optionen sind:</p> <ul style="list-style-type: none"><li>• Deaktivieren</li><li>• Passthrough-MAC-Adresse</li><li>• Integrierte NIC-MAC-Adresse</li></ul> <p>Diese Option steht nur auf dem Wyse 5470 All-in-One Thin Client zur Verfügung.</p>

**Tabelle 39. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
<b>Setupsperre durch Administrator</b>	Wählen Sie diese Option, um Benutzer vom Aufrufen des Setups abzuhalten, wenn ein Administratorenkennwort festgelegt worden ist.



**Tabelle 40. Konfigurieren der Administratorkennworteinstellungen**

Option	Beschreibung
<b>Administratorkennwort aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, um das BIOS-Administratorkennwort zu aktivieren.
<b>Administratorkennwort</b>	Geben Sie ein neues BIOS-Administratorkennwort ein. Diese Option ist nur verfügbar, wenn Sie das Kontrollkästchen <b>Administratorkennwort aktivieren</b> auswählen.

**Tabelle 41. Konfigurieren der Einstellungen für das automatische Einschalten**

Option	Beschreibung
Auto On Time	Wählen Sie aus der Dropdownliste die Tageszeit aus, zu der das System automatisch eingeschaltet werden soll.

**Tabelle 42. Konfigurieren von USB**

Option	Beschreibung
Dual-USB-2.0-Anschlüsse hinten links aktivieren	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät an diesem Port aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, ist das Gerät für das Betriebssystem verfügbar. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System das dort angeschlossene Gerät nicht erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>
Vordere USB-Anschlüsse aktivieren	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät an diesem Port aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, ist das Gerät für das Betriebssystem verfügbar. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System das dort angeschlossene Gerät nicht erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>
USB-Start-Unterstützung aktivieren	Wählen Sie dieses Kontrollkästchen aus, um das USB-Startsetup zu aktivieren. Diese Option ermöglicht das Starten von jedem USB-Massenspeichergerätetyp.

**Tabelle 43. Konfigurieren der Energieverwaltungseinstellungen**

Option	Beschreibung
AC-Wiederherstellung	Wählen Sie aus der Dropdownliste eine Option aus, um anzugeben, wie das System reagieren muss, wenn der Netzstrom wiederhergestellt wurde.
Wake On LAN	Wählen Sie aus der Dropdownliste eine Option aus, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird. Sie können einen Thin Client dazu bringen, aus dem ausgeschalteten Zustand über ein LAN-Signal hochgefahren zu werden.
Wake-on-USB	Wählen Sie diese Option aus, damit USB-Geräte das System einschalten oder aus dem Ruhezustand aufwecken können.

**Tabelle 44. Neustart-Zeitplan**

Option	Beschreibung
Neustartoption	Einige BIOS-Einstellungen machen einen Systemneustart erforderlich. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Sofort neu starten: Das System startet sofort neu.</li> <li>• Später neu starten: Wählen Sie <b>Neustart-Stunde</b> und <b>Neustart-Minute</b> aus, um den Zeitpunkt für den Systemneustart festzulegen,</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>Keinen Neustart durchführen: Das System wird nicht neu gestartet.</li> </ul>

## Firmware-Upgrade konfigurieren

Verwenden Sie die Seite **Firmware-Upgrade** zum Konfigurieren der Upgradeeinstellungen für die ThinOS Thin Client-Firmware, wie z. B. Live Upgrade, Logik der Firmware-Aktualisierung, lokale Firmware Überprüfungseinstellungen und Plattform-Firmware-Zuweisungen.

**Tabelle 45. Firmware-Upgrade konfigurieren**

Option	Beschreibung
<b>Live-Upgrade deaktivieren</b>	Dieser Parameter installiert automatisch die neue Firmware auf dem Thin Client basierend auf den festgelegten Richtlinien sofort nach dem Neustart des Thin Client. Um bei jedem Neustart zu prüfen, ob neue Firmware verfügbar ist, deaktivieren Sie diese Option.
<b>Logik der Firmware-Aktualisierung</b>	<p>Dieser Parameter legt fest, wie der Thin Client sich verhält, wenn die neue Firmware von der Verwaltungskonsole aus veröffentlicht wird. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>Nicht aktualisieren – Der Thin Client ignoriert die Firmware-Versionen, die den Verwaltungsrichtlinien zugewiesen wurden.</li> <li>Nur neue Firmware – Der Thin Client aktualisiert die Firmware nur, wenn eine neuere Version der Verwaltungsrichtlinie zugewiesen wurde.</li> <li>Jede andere Firmware – Der Thin Client aktualisiert die Firmware auf die durch die Verwaltungsrichtlinie zugewiesene Version, auch wenn die Version niedriger ist als das aktuelle Abbild auf dem Gerät.</li> </ul>
<b>Lokale Firmware-Überprüfung überspringen</b>	<p>Wählen Sie diese Option aus, damit der Thin Client die Überprüfung des lokalen Dateiservers auf Aktualisierungen der Firmware umgeht.</p> <p><b>i ANMERKUNG: Dell empfiehlt, dass Sie diese Option aktivieren, wenn Sie eine Firmware über die Verwaltungskonsole festlegen. Es führt zu einem endlosen Neustart, während der Thin Client unterschiedliche Abbilder anwendet, wenn Sie Firmwarerichtlinien in der Verwaltungskonsole und auf einem lokalen Dateiserver haben.</b></p>
<b>Signatur überprüfen</b>	Wählen Sie das Kontrollkästchen, um die Signatur zu überprüfen.
<b>BIOS-Upgrade aktivieren</b>	Wählen Sie diese Option aus, um den BIOS-Upgrade-Vorgang zu aktivieren.
<b>BIOS-Datei auswählen</b>	Wählen Sie diese Option aus, um die BIOS-Datei auszuwählen, die in das Datei-Repository hochgeladen wird. Wählen Sie aus dem Dropdown-Menü die BIOS-Datei aus.
<b>Paket-Upgrade aktivieren</b>	Wählen Sie diese Option aus, um den Paket-Upgrade-Vorgang zu aktivieren. Diese Option steht für Thin Clients mit ThinOS 8.6_017 höher zur Verfügung. Um das Paket hochzuladen, navigieren Sie zu <b>Apps &amp; Daten &gt; OS-Abbild-Repository &gt; ThinOS &gt; Paketdatei hinzufügen</b> . Weitere Informationen finden Sie unter <a href="#">ThinOS Paketdatei zu Repository hinzufügen</a> .
<b>Verfügbare Pakete</b>	Wählen Sie die Paketdateien aus, die auf dem Thin Client bereitgestellt werden sollen.

Option	Beschreibung
<b>Definieren der gewünschten Plattform- oder Firmware-Zuordnungen</b>	<p>Diese Option ordnet eine bestimmte Firmware-Version einem anderen Plattformtyp zu.</p> <p>Zum Zuordnen eines Plattformtyps zu einer bestimmten Firmware-Version führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1 Wählen Sie eine Plattform aus der Dropdownliste <b>Plattformtyp</b> aus.</li> <li>2 Wählen Sie aus dem Dropdownmenü <b>Automatische Firmware-Bereitstellung</b> eine Firmware-Version aus.</li> </ol> <p>Die Liste der Plattformtypen und die Nummer der Firmware-Version, die auf der Seite <b>Datei-Repository-Bestand</b> hochgeladen sind, werden angezeigt.</p>

## Konfigurieren der Geräteeinstellungen

Verwenden Sie die Seite **Geräteeinstellungen (8.6+)** zum Konfigurieren der Maus-, Tastatur-, Monitor-, Zeitzone-, Drucker-, Audio- und Netzwerkeinstellungen für ThinOS 8.6 und höher.

**Tabelle 46. Bevorzugte Geräteeinstellungen**

Option	Beschreibung
<b>Verwaltung der Geräteeinstellungen</b>	<p>Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Die verfügbaren Optionen sind:</p> <ul style="list-style-type: none"> <li>• Manuelles Überschreiben deaktivieren: Wählen Sie diese Option zum Deaktivieren des manuellen Überschreibens aller Geräte mit Wyse Management Suite-Konfigurationen.</li> <li>• Manuelles Überschreiben bei allen Geräten aktivieren: Wählen Sie diese Option zum manuellen Überschreiben aller Geräte mit Client-Konfigurationen.</li> <li>• Manuelles Überschreiben ausgewählter Elemente aktivieren: Wählen Sie diese Option zum manuellen Überschreiben von ausgewählten Geräten mit bestimmten Client-Konfigurationen.</li> </ul>
<b>Überwachung</b>	<p>Wählen Sie diese Option aus, um die Monitoreinstellungen manuell zu überschreiben. Diese Option kann angewendet werden, wenn Sie die Option <b>Manuelles Überschreiben ausgewählter Elemente aktivieren</b> ausgewählt haben.</p>
<b>Maus</b>	<p>Wählen Sie diese Option aus, um die Mauseinstellungen manuell zu überschreiben. Diese Option kann angewendet werden, wenn Sie die Option <b>Manuelles Überschreiben ausgewählter Elemente aktivieren</b> ausgewählt haben.</p>
<b>Tastatur</b>	<p>Wählen Sie diese Option aus, um die Tastatureinstellungen manuell zu überschreiben. Diese Option kann angewendet werden, wenn Sie die Option <b>Manuelles Überschreiben ausgewählter Elemente aktivieren</b> ausgewählt haben.</p>
<b>Zeitzone</b>	<p>Wählen Sie diese Option aus, um die Zeitzoneneinstellungen manuell zu überschreiben. Diese Option kann angewendet werden, wenn Sie die Option <b>Manuelles Überschreiben ausgewählter Elemente aktivieren</b> ausgewählt haben.</p>
<b>Drucker</b>	<p>Wählen Sie diese Option aus, um die Druckereinstellungen manuell zu überschreiben. Diese Option kann angewendet werden, wenn</p>

Option	Beschreibung
	Sie die Option <b>Manuelles Überschreiben ausgewählter Elemente aktivieren</b> ausgewählt haben.
<b>Audio</b>	Wählen Sie diese Option aus, um die Audioeinstellungen manuell zu überschreiben. Diese Option kann angewendet werden, wenn Sie die Option <b>Manuelles Überschreiben ausgewählter Elemente aktivieren</b> ausgewählt haben.
<b>Netzwerk</b>	Wählen Sie diese Option aus, um die Netzwerkeinstellungen manuell zu überschreiben, wie beispielsweise WLAN oder statische IP-Adresse. Diese Option kann angewendet werden, wenn Sie die Option <b>Manuelles Überschreiben ausgewählter Elemente aktivieren</b> ausgewählt haben.

## Konfigurieren von globalen INI-Einstellungen

Verwenden Sie die Seite **Globale INI-Einstellungen** zur Konfiguration von globalen INI-Einstellungen für Geräte mit ThinOS 8.5 und höher.


**Tabelle 47. Konfigurieren von globalen INI-Einstellungen**

Option	Beschreibung
<b>Globale INI</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Die Datei <b>global.ini</b> enthält die globalen Parameter für alle Geräte. Die Parameter können in einer vorhandenen <b>wnos.ini</b> oder einer neu erstellten INI-Datei enthalten sein, die in das Datei-Repository hochgeladen wurde.

## Konfigurieren der Host-INI-Einstellungen

Verwenden Sie die Seite **Hosts (8.6 +)** zur Definition von Host-INI-Einstellungen.

**Tabelle 48. Konfigurieren der Host-INI-Einstellungen**

Option	Beschreibung
<b>Hosts</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Die in den Bestand hochgeladenen Hostdateien werden in der Dropdown-Liste angezeigt.   <b>ANMERKUNG: Die Größe hochgeladener Dateien muss geringer als 1 KB sein.</b>

## Konfigurieren von zentralen Konfigurationseinstellungen

Die Seite **Zentrale Konfiguration** dient zur Angabe eines Dateiservers, in dem der ThinOS Thin Client nach Konfigurations- und Abbildaktualisierungen sucht.

**Tabelle 49. Zentrale Konfiguration**

Option	Beschreibung
<b>Dateiserver/-pfad</b>	Geben Sie den vollständigen Pfad des Ordners an, in dem die Datei <b>wnos</b> liegt. Unterstützte Protokolle umfassen FTP, HTTP, und HTTPS. Das Standardprotokoll ist FTP.
<b>Benutzer</b>	Geben Sie den Benutzernamen für den Zugriff auf den Dateiserver ein.
<b>Kennwort</b>	Geben Sie das Kennwort für den Zugriff auf den Dateiserver ein.

## Erweiterte Einstellungen konfigurieren

Verwenden Sie die Seite **Erweiterte Einstellungen**, um zusätzliche Einstellungen in Form von für den ThinOS Thin Client spezifischen INI-Parametern zu konfigurieren oder die lokale INI-Überprüfung zu deaktivieren. Dell empfiehlt, dass Sie keine INI-Parameter für Richtlinien einschließen, die bereits in anderen Optionen konfiguriert sind. Kennwortkodierung und -Verschlüsselung werden nicht auf die Kennwortparameter angewendet.

**Tabelle 50. Erweiterte Einstellungen konfigurieren**

Option	Beschreibung
<b>Keine globale INI</b>	Wenn diese Option ausgewählt ist, werden die globalen INI-Parameter nicht vom Dateiserver geladen.  Geben Sie die INI-Parameter von Zeile 1 bis Zeile 20 für die Thin Clients ein.

## Konfigurieren von Remote-Verbindungen

Verwenden Sie die Seite **Remote-Verbindungen** zum Konfigurieren der ThinOS Thin Client Remote-Verbindungseinstellungen, wie z. B. Adressen und Anmeldeinformationen für Broker und direkte Verbindungen.

**Tabelle 51. Konfigurieren der Verbindungs-Broker-Einstellungen**

Option	Beschreibung
<b>Broker auswählen</b>	Wählen Sie diese Option zum Herstellen einer Broker-Verbindung für einen veröffentlichten Desktop. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Kein</li> <li>• Citrix</li> <li>• Microsoft</li> <li>• vWorkspace</li> <li>• VMware</li> </ul> <p><b>ANMERKUNG:</b> ThinOS Lite/Xenith Geräte unterstützen Citrix Brokerverbindungen.</p>
<b>Direkte RDP-Verbindungen manuell definieren</b>	Wählen Sie diese Option zum manuellen Definieren der RDP-Verbindungen. Wenn Sie diese Option auswählen, wird das Feld <b>direkte Verbindungen (RDP)</b> angezeigt.
<b>Broker-Server</b>	Geben Sie den Broker-Serverhostnamen oder die IP-Adresse an.

Option	Beschreibung
<b>Citrix StoreFront</b>	Wählen Sie diese Option aus, um das Citrix StoreFront-basierte Layout der veröffentlichten Anwendungen und Desktop-PCs auf dem Gerät zu aktivieren. Diese Option gilt nur für Citrix.
<b>Auf Desktop anzeigen</b>	Wählen Sie aus der Dropdownliste eine Option, die Sie auf dem Desktop anzeigen möchten. Diese Option gilt nur für Citrix.
<b>Automatisch mit Sitzungen verbinden</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu der Sitzung herzustellen. Diese Option gilt nur für Citrix, VMware und vWorkspace.
<b>Empfohlene Einstellungen für Sitzungen verwenden</b>	Wählen Sie diese Option aus, um die empfohlenen Einstellungen auszuwählen. Diese Option gilt nur für Citrix.
<b>Direkte RDP-Verbindungen manuell definieren</b>	Wählen Sie diese Option zum manuellen Definieren der RDP-Verbindungen. Wenn Sie diese Option auswählen, wird das Feld <b>direkte Verbindung</b> angezeigt.
<b>TS-Gateway konfigurieren</b>	Wählen Sie diese Option zum Konfigurieren des TS-Gateway. Wenn Sie diese Option auswählen, wird die Tabelle <b>TS-Gateway-Einstellungen</b> angezeigt. Diese Option gilt nur für Microsoft.
<b>Sicherheitsmodus</b>	Wählen Sie diese Option aus, um einen Sicherheitsmodus festzulegen. Diese Option gilt nur für VMware.
<b>Protokoll</b>	Wählen Sie diese Option zur Auswahl eines Protokolls. Diese Option gilt nur für VMware.

**Tabelle 52. Direkte Verbindungen (RDP) konfigurieren**

Option	Beschreibung
<b>Verbindungsname</b>	Geben Sie den Namen der Verbindung ein.
<b>Hostname oder IP-Adresse</b>	Geben Sie den Host-Namen oder die IP-Adresse der Verbindung ein.
<b>Automatischer Start</b>	Wählen Sie diese Option zum automatischen Neustart der Verbindung.
<b>Nach Trennung erneut verbinden</b>	Wählen Sie diese Option aus, um die Verbindung automatisch wiederherzustellen, nachdem sie getrennt wurde.
<b>Benutzername</b>	Geben Sie einen Benutzernamen für die Remote-Anmeldung ein.
<b>Kennwort</b>	Geben Sie das Kennwort für die Remote-Anmeldung ein.
<b>Domainname</b>	Geben Sie den RD-Domainnamen für die Remote-Anmeldung ein.
<b>Farbtiefe</b>	Wählen Sie diese Option aus, um die Farbtiefe festzulegen. Wählen Sie aus der Dropdownliste die Farbtiefe für die Remote-Anmeldung aus.
<b>Funktionsweise des Sitzungsfensters</b>	Wählen Sie diese Option aus, um die Funktionsweise des Sitzungsfensters festzulegen. Wählen Sie aus der Dropdownliste, ob die Remoteverbindung im Fenstermodus oder im Vollbildschirm-Modus gestartet werden soll.

Option	Beschreibung
	<p><b>ANMERKUNG:</b> Der Zero-Launchpad-Modus unterstützt nur Vollbildsitzungen und der Fenstermodus wird auf einem einzigen Bildschirm gestartet. Die Vollbildschirmdarstellung reicht über beide Monitore.</p>
<b>Audiowiedergabe</b>	<p>Diese Option hilft Ihnen dabei, die Audioeinstellungen in der Remote-Sitzung festzulegen. Wählen Sie im Dropdownmenü nach Bedarf eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Lokal wiedergeben</li> <li>• Auf Remote-Computer wiedergeben</li> <li>• Nicht wiedergeben</li> </ul>

**Tabelle 53. Standardeinstellungen für die Sitzungsfunktionsweise**

Option	Beschreibung
<b>Schriftartglättung</b>	Wählen Sie diese Option, um die Schriftglättung zu aktivieren. Die Schriftglättung ist eine Methode zum Erzielen schärferer Schriftarten bei Bildschirmen mit niedriger Auflösung.
<b>Erweiterte RDP-Protokollfunktionen</b>	Wählen Sie diese Option zum Konfigurieren des RDP-Protokolls.
<b>Standardfarbtiefe für Verbindungen</b>	Wählen Sie diese Option zum Einstellen der Farbtiefe für Ihre Verbindung. Wählen Sie aus der Dropdownliste die Farbtiefe für die Remote-Anmeldung aus.
<b>Funktionsweise des Sitzungsfensters</b>	<p>Wählen Sie diese Option aus, um die Funktionsweise des Sitzungsfensters festzulegen. Wählen Sie aus der Dropdownliste, ob die Remoteverbindung im Fenstermodus oder im Vollbildschirm-Modus gestartet werden soll. Diese Option gilt nur für Citrix.</p> <p><b>ANMERKUNG:</b> Der Zero-Launchpad-Modus unterstützt nur Vollbildsitzungen und der Fenstermodus wird auf einem einzigen Bildschirm gestartet. Die Vollbildschirmdarstellung reicht über zwei Monitore.</p>
<b>USB-Umleitungstechnologie</b>	Wählen Sie diese Option, um die USB-Umleitung zu aktivieren. Wählen Sie diese Option, um den Zugriff auf USB-Geräte zu ermöglichen, die eine Verbindung mit dem Thin Client von innerhalb eines Remotedesktops oder einer Anwendung herstellen. Diese Option gilt nur für Citrix.
<b>Audioqualität</b>	Wählen Sie diese Option aus, um die Audioqualität festzulegen. Diese Option gilt nur für Citrix.
<b>USB-Festplatten zuweisen zu</b>	Wählen Sie aus der Dropdownliste den Speicherplatz für die Zuweisung zum USB. Diese Option gilt nur für Citrix.
<b>Nahtlosmodus aktivieren</b>	Wählen Sie diese Option aus, um den Nahtlosmodus einzustellen. Eine <b>nahtlose</b> Schnittstelle ist die Verbindung von zwei Computerprogrammen, sodass sie ein Programm mit einer einzigen Benutzeroberfläche zu sein scheinen. Diese Option gilt nur für Citrix.
<b>Taskleiste im Nahtlosmodus ausblenden</b>	Wählen Sie diese Option zum Ausblenden der Taskleiste im Nahtlosmodus. Diese Option gilt nur für Citrix.

**Tabelle 54. Konfigurieren von HDX-Protokolleinstellungen**

Option	Beschreibung
<b>KB über hohe Latenz verbessern</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option zur Verbesserung der KB über hohe Latenz.
<b>Maus über hohe Latenz verbessern</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option zur Verbesserung der Maus über hohe Latenz.
<b>Automatisch verbinden</b>	Wählen Sie aus der Dropdownliste und aktivieren Sie die bevorzugte Option zum automatischen Herstellen der Remoteverbindung. <ul style="list-style-type: none"> <li>• Multimedia-Umleitung</li> <li>• Sitzungszuverlässigkeit aktivieren</li> <li>• Progressive Anzeige aktivieren</li> <li>• ICA-Ping aktivieren</li> <li>• Offscreen-Support</li> </ul>

**Tabelle 55. Konfigurieren der peripheren Funktionsweise**

Option	Beschreibung
<b>Ausgewählte lokale Ressourcen automatisch verbinden</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu den folgenden Peripheriegeräten herzustellen: <ul style="list-style-type: none"> <li>• Drucker</li> <li>• Serielle Schnittstellen</li> <li>• SmartCards</li> <li>• Ton</li> </ul>
<b>USB-Festplatten aktivieren</b>	Wählen Sie diese Option, um USB-Festplatten zu aktivieren. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Nein</li> <li>• Ja (Lesen oder Schreiben)</li> <li>• Ja (schreibgeschützt)</li> </ul>
<b>USB-Umleitung aktivieren</b>	Wählen Sie diese Option, um die USB-Umleitung zu aktivieren. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Nein</li> <li>• Ja, alle USB-Geräte umleiten</li> <li>• Ja, aber einige Geräte ausschließen</li> </ul> <p><b>ANMERKUNG:</b> Sie haben auch die Möglichkeit, Festplatte, Drucker, Audio- und Videogeräte auszuschließen.</p>
<b>Zeitgeber für Mauswarteschlange</b>	Wählen Sie diese Option aus, um den Zeitgeber für die Mauswarteschlange in einer ICA- oder RDP-Sitzung festzulegen. Der Bereich des Zeitgebers für die Mauswarteschlange ist 0 bis 99.

**Tabelle 56. Konfigurieren von zusätzlichen Einstellungen**


Option	Beschreibung
<b>Maximaler Bitmap-Cache</b>	Für das Einstellen des maximalen Bitmap-Cache für Ihre RDP-Sitzung geben Sie eine Zahl von 128 bis 1024 ein.
<b>Ausgerichtete Sitzungsbreite von 4 Pixeln</b>	Wählen Sie diese Option aus, um die ausgerichtete Sitzungsbreite von 4 Pixeln zu aktivieren.
<b>Sitzungen bei Anmeldung automatisch erneut verbinden?</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung zur Sitzung bei der Anmeldung wiederherstellt. Diese Option gilt nur für Citrix.
<b>Automatisch über das Tastenmenü erneut verbinden?</b>	Wählen Sie diese Option aus, damit der Thin Client, automatisch wieder die Verbindung zu einer Sitzung aus dem Schaltflächen-Menü herstellt. Diese Option gilt nur für Citrix.
<b>Self-Service-Server des Kontos</b>	Geben Sie die Serverdetails ein.
<b>Auf Gateway-Authentifizierungsmethode zugreifen</b>	Wählen Sie aus der Dropdownliste die Methoden zum Zugriff auf die Gateway-Authentifizierung.
<b>HTTP zum Browsen verwenden</b>	Wählen Sie diese Option, um HTTP für Browser zu aktivieren. Diese Option gilt nur für Citrix.
<b>Adresse über Firewall ändern</b>	Wählen Sie diese Option für die Aktivierung einer alternativen Adresse durch die Firewall. Diese Option gilt nur für Citrix.
<b>Systemmenü</b>	Wählen Sie diese Option aus, um das Systemmenü einzustellen. Diese Option gilt nur für Citrix.
<b>Zurücksetzen der VM deaktivieren</b>	Wählen Sie diese Option aus, um den VM-Reset zu deaktivieren. Diese Option gilt nur für Citrix.
<b>32-Bit-Symbole für die ersten Verbindungen anzeigen</b>	Geben Sie die 32-Bit-Symbole für die ersten Verbindungen an. Diese Option gilt nur für Citrix.

## Konfigurieren von globalen Sitzungseinstellungen—ThinOS 8.5 und spätere Versionen

Verwenden Sie die Seite **Globale Sitzungseinstellungen** für die Konfiguration der globalen VDI-Einstellungen für Geräte mit ThinOS 8.5 und höher.


**Tabelle 57. Einstellungen für lokale Ressourcen konfigurieren**

Option	Beschreibung
<b>Drucker zuordnen</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu den lokalen Druckern herzustellen, wenn die Sitzung gestartet wird.
<b>Serielle Schnittstellen zuordnen</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu den lokalen seriellen Schnittstellen herzustellen, wenn die Sitzung gestartet wird.
<b>Smartcards zuordnen</b>	Wählen Sie diese Option aus, um die Smartcards an die Remotesitzung umzuleiten.
<b>Ton zuordnen</b>	Wählen Sie diese Option aus, um den Ton auf dem lokalen System zu aktivieren, wenn die Sitzung gestartet wird.

Option	Beschreibung
<b>Festplatten zuordnen</b>	Wählen Sie diese Option, um Festplatten zuzuordnen. Sie können USB-Laufwerke für ICA- und RDP-Verbindungen automatisch verbinden, wenn die Sitzung gestartet wird.
<b>Schreibgeschützte Festplatten</b>	Wählen Sie diese Option, um schreibgeschützte Festplatten zu aktivieren.
<b>USB-Umleitung aktivieren</b>	Wählen Sie diese Option aus, um die USB-Laufwerke an die Remotesitzung umzuleiten. Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Wenn die Option <b>Einige Geräte ausschließen</b> ausgewählt ist, können Sie die folgenden Geräte aus der Sitzung ausschließen: <ul style="list-style-type: none"> <li>• Festplattengeräte ausschließen</li> <li>• Audiogeräte ausschließen</li> <li>• Druckergeräte ausschließen</li> <li>• Videogeräte ausschließen</li> </ul>
<b>Auf Desktop anzeigen (8.6+)</b>	Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Alle</li> <li>• Kein</li> <li>• Desktops</li> <li>• Anwendungen</li> <li>• Andere</li> </ul>
<b>Whitelist aktivieren oder Blacklist deaktivieren</b>	Verwenden Sie diese Option, um die Whitelist zu aktivieren oder die Blacklist zu deaktivieren. Standardmäßig ist <b>Whitelist oder Blacklist nicht aktivieren</b> ausgewählt. <p> <b>ANMERKUNG: Das Gerät wird neu gestartet, wenn Sie diese Option aktivieren.</b></p> Die folgenden Optionen werden angezeigt, wenn Sie <b>Whitelist aktivieren</b> oder <b>Blacklist aktivieren</b> auswählen: <ul style="list-style-type: none"> <li>• Klasse</li> <li>• USB-Klasse</li> <li>• Anbieter-ID</li> </ul>

**Tabelle 58. Erweiterte Einstellungen konfigurieren**


Option	Beschreibung
<b>Nach Trennung erneut verbinden</b>	Wählen Sie diese Option aus, um die Verbindung automatisch wiederherzustellen, nachdem sie getrennt wurde.
<b>Multimonitor</b>	Wählen Sie diese Option aus, um die Multimonitor-Funktion zu aktivieren. Die Höhe und Breite des Sitzungsdesktops ist vergleichbar mit der Größe des lokalen virtuellen Desktops.
<b>Komprimierung deaktivieren</b>	Wählen Sie diese Option aus, um die Dateien zur Reduzierung der benötigten Download-Zeit zu komprimieren.
<b>Für langsame Linkgeschwindigkeit optimieren</b>	Aktivieren Sie das Kontrollkästchen, um die Sitzungseinstellungen für eine niedrige Linkgeschwindigkeit zu optimieren.

Option	Beschreibung
<b>Vollbildschirm-Modus</b>	Wählen Sie diese Option, um das Verbindungsfenster im Vollbildschirm-Modus auszuführen.
<b>Taste für schnelle Trennung</b>	Wählen Sie diese Option aus, um die Taste für schnelle Trennung zu verwenden.   <b>ANMERKUNG: Drücken Sie die Taste F12, um sich von Sitzungen abzumelden.</b>

## Konfigurieren von USB-Umleitungseinstellungen

Die USB-Umleitungstechnologie (Umleitung für universellen seriellen Bus) ist eine Technologie, die Ihnen den Anschluss eines externen Geräts an einen USB-Anschluss am Endpunkt sowie den Zugriff auf dieses Gerät mit einem Remote-Desktop oder einer Anwendung ermöglicht. Sie können die USB-Umleitung so konfigurieren, dass sie automatisch auf ein bestimmtes Gerät umleitet. Verwenden Sie die Seite **USB-Umleitungseinstellungen**, um die Umleitung von über USB angeschlossenen Geräten an die Remote-Sitzung für Geräte mit ThinOS 8.5 und höher zu erzwingen.

**Tabelle 59. USB-Umleitungseinstellungen**

Option	Beschreibung
<b>Umleitung erzwingen</b>	Geben Sie die Geräte-ID für das Erzwingen der Umleitung an.
<b>Lokale erzwingen</b>	Geben Sie die Geräte-ID für das lokale Erzwingen an.
<b>Umleitungstyp</b>	Wählen Sie in der Dropdownliste den Umleitungstyp aus.   <b>ANMERKUNG: Wenn als Verbindungstyp PCoIP oder Blast ausgewählt ist, wählen Sie keinen Wert.</b>
<b>Schnittstellenumleitung</b>	Wählen Sie diese Option, um die Option "Schnittstellenumleitung" zu aktivieren.

## Konfigurieren von Drittanbieter-Authentifizierungseinstellungen

Verwenden Sie die Seite mit den Einstellungen für die **Drittanbieter-Authentifizierung** zum Konfigurieren der Single Sign-On- (SSO-)Authentifizierungseinstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 60. Konfigurieren von Authentifizierungseinstellungen**

Option	Beschreibung
<b>Authentifizierungsmodus</b>	Wählen Sie diese Option aus, um den Authentifizierungsmodus anzugeben. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Imprivata</li> <li>• Caradialm</li> <li>• SecureMatrix</li> <li>• HealthCast</li> </ul>

**Tabelle 61. Konfigurieren von RF-ID-Einstellungen**

Option	Beschreibung
<b>RF-ID Signalton deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren des RFID Signaltons. Radio-Frequency Identification – RFID ist die Verwendung von Funkwellen für das Lesen und Erfassen von abgelegten Daten auf einem Tag, das an einem Objekt angebracht ist. Ein Tag kann aus bis zu mehreren Metern Entfernung gelesen werden und muss nicht in direktem Sichtkontakt des Lesegeräts sein. RFID-Authentifizierung ermöglicht einen schnellen Zugriff auf ein System zur Durchführung kurzer Aufgaben. Sie können schnelle Benutzeridentifizierung über RFID (Radio Frequency Identification) verwenden.
<b>Tastenkombination deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der Tastenkombinations-Funktionalität. Ein Tastaturanschlag ist ein einzelnes Drücken einer Taste auf der Tastatur. Jedes Drücken einer Taste ist ein Tastaturanschlag einer Tastenkombination. Die Tastatur wird als Eingabegerät für das Senden von Signalen verwendet.
<b>Kartentyp festlegen</b>	Wählen Sie diese Option zum Einstellen des Kartentyps. <b>RFID</b> -Karten enthalten eine integrierte Schaltung und eine Antenne, die verwendet werden, um Daten auf das RFID-Lesegerät zu übertragen.
<b>Initialisierung deaktivieren</b>	Mit dieser Option wird die allgemeine RFID-Authentifizierung deaktiviert.
<b>LED deaktivieren</b>	Wählen Sie diese Option aus, um die LED zu deaktivieren.

**Tabelle 62. Konfigurieren von Imprivata-Einstellungen**

Option	Beschreibung
<b>Imprivata OneSign-Server</b>	Geben Sie den Hostnamen oder die IP-Adresse mit optionaler TCP-Portnummer oder URLs des Imprivata OneSign-Servers an.
<b>Kioskmodus</b>	Wählen Sie diese Option aus, um den Kioskmodus zu aktivieren. Wenn diese Option aktiviert ist, dann können verschiedene OneSign-Benutzer den Client Desktop entsperren.
<b>Windows-Authentifizierung aktivieren</b>	Mit dieser Option wird die allgemeine Windows-Authentifizierung aktiviert. Falls diese Funktion aktiviert ist, schlägt die OneSign-Anmeldung fehl. Melden Sie sich im vordefinierten Broker mit Windows-Anmeldeinformationen an.
<b>Automatischer Zugriff</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>NetBIOS-Domänenname</b>	Wählen Sie diese Option aus, um die Option NetBIOS-Domännennamen zu aktivieren. Falls diese Funktion aktiviert ist, wird der NETBIOS-Domännennamen in der Imprivata-Domänenliste aufgelistet.
<b>Aktion aussetzen</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Wenn Sie 0 wählen, verriegeln Sie das Terminal, wenn Sie 1 wählen, melden Sie sich aus dem Terminal ab.
<b>Hotkey deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der Hotkey-Funktion.

Option	Beschreibung
<b>Aufforderung zur Registrierung deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der Aufforderung zur Registrierung. Wenn diese Option deaktiviert ist, bietet ThinOS System keine Aufforderung zum Registrieren der Sicherheitsantworten nach der OneSign-Anmeldung.
<b>Sicherheitsmodus</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Der Sicherheitsmodus legt die Richtlinie für die SSL-Zertifikatsprüfung fest.

**Tabelle 63. Konfigurieren von Caradigm-Einstellungen**

Option	Beschreibung
<b>SSO für CM-Server</b>	Geben Sie den Namen des SSO- (Einmaliges Anmelden) und CM- (Kontextmanagement)-Servers an. Sie können die Authentifizierung über "Einmaliges Anmelden" mit Web- oder Desktop-Anwendungen verwenden. Der Server authentifiziert die Benutzerinformationen.
<b>Standard-Gruppenname</b>	Geben Sie den Namen für den Standardgruppennamen ein.
<b>Abmeldung aktivieren</b>	Wählen Sie diese Option aus, um die Abmeldung zu aktivieren.
<b>Sicherheitsmodus für Cardigm</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Diese Option hilft Anbietern im Gesundheitswesen, sich schnell und sicher bei klinischen Anwendungen anzumelden.
<b>Protokollklasse für Cardigm</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. <b>Protokollklasse für Cardigm</b> ermöglicht die Trennung der Software, die Meldungen generiert, des Systems, das die Meldungen speichert, und der Software, die Berichte und Analysen der Meldungen erzeugt. Jede Meldung wird mit einem Raumcode versehen, der den Softwaretyp enthält, der die Meldung generiert hat, und eine zugewiesene Schweregradbeschriftung.
<b>Manuelle Anmeldung deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der manuellen Anmeldefunktion.

**Tabelle 64. Konfigurieren von SecureMatrix-Einstellungen**

Option	Beschreibung
<b>Secure Matrix-Server</b>	Geben Sie die Secure Matrix-Serverdetails ein. Sie können den Administratorzugriff verwalten, Kennwortrichtlinien durchsetzen und eine mehrstufige Authentifizierung für eine zusätzliche Sicherheitsebene hinzufügen.

**Tabelle 65. Konfigurieren von HealthCast-Einstellungen**

Option	Beschreibung
<b>HealthCast-Server</b>	Geben Sie den Namen des HealthCast-Servers ein. Sie können die Authentifizierung über "Einmaliges Anmelden" mit Web- oder

Option	Beschreibung
	Desktop-Anwendungen verwenden. Der Server authentifiziert die Benutzerinformationen.
<b>Sicherheitsmodus für HealthCast</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Die HealthCast-Lösung bietet sicheren Zugriff und unübertroffene Geschwindigkeit zu virtuellen Desktops und klinischen Desktops, bequeme, schnelle Benutzerumschaltung, automatisierte Workflows, einzigartige Näherungselementfunktionen, optionale PIN, Remote-Zugriff-Lösungen mit Zwei-Faktor-Authentifizierung und Roaming-Sitzungen mit unmittelbarem Zugriff auf die Arbeit von jedem Computer aus.
<b>Protokollklasse für HealthCast</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. <b>Protokollklasse für HealthCast</b> ermöglicht die Trennung der Software, die Meldungen generiert, des Systems, das die Meldungen speichert, und der Software, die Berichte und Analysen der Meldungen erzeugt. Jede Meldung wird mit einem Raumcode versehen, der den Softwaretyp enthält, der die Meldung generiert hat, und eine zugewiesene Schweregradbeschriftung.
<b>Client-Zertifikat</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Die Zertifikate werden in das Datei-Repository hochgeladen.

## Konfigurieren von Citrix Broker-Verbindungseinstellungen

Verwenden Sie die Seite mit den **Citrix Broker**-Verbindungseinstellungen zum Konfigurieren der Citrix Broker-Verbindungseinstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 66. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Broker-Server</b>	Geben Sie den Broker-Serverhostnamen oder die IP-Adresse an.
<b>Benutzerdefinierter Citrix-Speichernamen</b>	Geben Sie den benutzerdefinierten Speichernamen für die Citrix StoreFront-Verbindung ein.
<b>Self-Service-Server des Kontos</b>	Geben Sie die Serverdetails ein.
<b>Citrix StoreFront-Stil</b>	Wählen Sie diese Option aus, um das Citrix StoreFront-basierte Layout der veröffentlichten Anwendungen und Desktop-PCs auf dem Gerät zu aktivieren.
<b>Benachrichtigung bei Kennwortablauf</b>	Wählen Sie diese Option aus, um die Benachrichtigung bei Kennwortablauf zu aktivieren. Wenn das Kennwort läuft, wird eine Warnmeldung mit der Anzahl der verbleibenden Tage um das Kennwort zu ändern, angezeigt.
<b>Auf Desktop anzeigen</b>	Wählen Sie aus der Dropdownliste eine Option, die Sie auf dem Desktop anzeigen möchten.
<b>Empfohlene Einstellungen für Sitzungen verwenden</b>	Wählen Sie diese Option aus, um die empfohlenen Einstellungen zu konfigurieren. Um weitere Informationen zu erhalten, fahren Sie mit der Maus über das Symbol <b>Informationen (i)</b> .
<b>Automatisch über die Schaltfläche erneut verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client, automatisch wieder die Verbindung zu einer Sitzung aus dem Schaltflächen-Menü herstellt.

Option	Beschreibung
<b>Sitzungen, mit denen automatisch eine Verbindung hergestellt werden soll</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu der Sitzung herzustellen.
<b>RequestIconDataCount</b>	Geben Sie die Anzahl der Symbole an. Die Symbole werden in 32-Bit-Farbe dargestellt.
<b>Bei Anmeldung erneut verbinden</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Es ist die erneute Verbindungsherstellung bei aktiven und getrennten Sitzungen möglich.
<b>HTTPS-Benutzer-Agent (8.6+)</b>	Geben Sie den INI-Parameter ein, um die Kommunikation mit Ihrem Client über die NetScaler-Sitzungsrichtlinie zu ermöglichen.
<b>Zeitüberschreitung</b>	Wählen Sie in der Dropdown-Liste die Zeitdauer für die Verbindungsherstellung des Geräts aus. Wenn die Verbindung nach der angegebenen Zeitspanne nicht erfolgreich ist, meldet das Gerät, dass der Broker nicht erreichbar ist.

**Tabelle 67. Konfigurieren der NetScaler Gateway-Authentifizierung**

Option	Beschreibung
<b>NetScaler Gateway-Authentifizierung</b>	Wählen Sie diese Option aus, um die Verwendung der Funktion "NetScaler Gateway-Authentifizierung" zu aktivieren.
<b>Benutzername</b>	Geben Sie den Benutzernamen für die Authentifizierung ein.
<b>Kennwort</b>	Geben Sie das Kennwort für die Authentifizierung ein.
<b>Domain</b>	Geben Sie den Domänennamen für die Authentifizierung ein.
<b>CAG extern</b>	Wählen Sie diese Option, um den externen Netzwerkmodus direkt zu verwenden, ohne bestimmte Frames zu überprüfen, die von den Zugriffspunkten übertragen werden, um ihre Anwesenheit anzuzeigen.
<b>CAG-Benutzer als UPN</b>	Wählen Sie diese Option, um den Benutzernamen im UPN-Format an den Server zu senden.


**Tabelle 68. Konfigurieren von Einstellungen für Mehrfachanmeldung**

Option	Beschreibung
<b>Multi-Farm</b>	Wählen Sie diese Option zur Unterstützung von Servern aus, die Teil von verschiedenen Farmen sind.
<b>Multi-Domäne</b>	Wählen Sie diese Option aus, um die Funktion "Multi-Domäne" zu aktivieren.
<b>Mehrfachanmeldung</b>	Wählen Sie diese Option aus, um die Funktion "Mehrfachanmeldung" zu aktivieren.
<b>Sequenzielle Domäne</b>	Wählen Sie diese Option zur Auswahl der Domänen in sequenzieller Reihenfolge, die unter der Option DomainList aufgeführt werden.

# Konfigurieren von Citrix HDX-Verbindungseinstellungen

Verwenden Sie die Seite **Citrix HDX-Einstellungen** zur Definition der globalen VDI-Einstellungen für Citrix-Verbindungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 69. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Audioqualität</b>	Wählen Sie diese Option aus, um die Audioqualität festzulegen.
<b>Nahtlosmodus aktivieren</b>	Wählen Sie diese Option aus, um den Nahtlosmodus einzustellen.
<b>Multimedia-Umleitung</b>	Wählen Sie diese Option für die Multimedia-Weiterleitung.
<b>USB-Festplatten zuweisen zu</b>	Wählen Sie aus der Dropdownliste den Speicherplatz für die Zuweisung zum USB.
<b>Funktionsweise des Sitzungsfensters</b>	Wählen Sie diese Option aus, um zu definieren, ob die Remoteverbindung im Vollbildschirm-Modus gestartet werden sollte. Wählen Sie entweder <b>Vollbildschirm</b> oder <b>Fenstermodus</b> .   <b>ANMERKUNG: Der Zero-Launchpad-Modus unterstützt nur Vollbildsitzungen. Der Fenstermodus startet nur auf einem einzigen Bildschirm, während Vollbildsitzungen beide Bildschirme umfassen.</b>
<b>Sitzungszuverlässigkeit</b>	Wählen Sie diese Option aus, um die ICA-Sitzungszuverlässigkeit zu aktivieren.
<b>Adresse über Firewall ändern</b>	Wählen Sie diese Option für die Aktivierung einer alternativen Adresse durch die Firewall.
<b>Suchprotokolltyp</b>	Wählen Sie diese Option zur Auswahl eines Protokolltyps. Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
<b>USB-Umleitungstechnologie</b>	Wählen Sie diese Option, um die USB-Umleitung zu aktivieren. Die USB-Umleitung ist eine Technologie, die Ihnen den Zugriff auf die USB-Geräte ermöglicht, die eine Verbindung mit dem Thin Client von innerhalb eines Remote-Desktops oder einer Anwendung herstellen.
<b>Clientname (8.6+)</b>	Geben Sie den Clientnamen für die ICA-Sitzung ein. Der Standardwert ist der Terminalname.



**Tabelle 70. Konfigurieren von Multimedia-Einstellungen**

Option	Beschreibung
<b>HDXFlashUseFlashRemoting</b>	Wählen Sie diese Option, um anzugeben, ob die HDX-Flash-Umleitung verwendet werden soll.
<b>HDXFlashEnableServerSideContentFetching</b>	Wählen Sie diese Option, um anzugeben, ob der serverseitige Inhaltsabruf aktiviert werden soll.
<b>EnableRTME</b>	Wählen Sie diese Option zum Starten des RTME-Dienstes.
<b>FlipByTimer</b>	Wählen Sie diese Option zur Auswahl einer Bildschirmaktualisierungsmethode.

## Konfigurieren von VMware Broker-Verbindungseinstellungen

Verwenden Sie die Seite mit den **VMWare Broker**-Verbindungseinstellungen zum Konfigurieren der VMWare Broker-Verbindungseinstellungen für Geräte mit ThinOS 8.5 und höher.


**Tabelle 71. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Broker-Server</b>	Geben Sie den Broker-Serverhostnamen oder die IP-Adresse an.   <b>ANMERKUNG: Sie müssen zwischen HTTP:// oder HTTPS: // wählen.</b>
<b>Sicherheitsmodus</b>	Wählen Sie diese Option aus, um einen Sicherheitsmodus festzulegen.
<b>Protokoll</b>	Wählen Sie diese Option zur Angabe des Displayprotokolls aus. Die standardmäßigen Server-Protokolle sind All, RDP, PCoIP oder Blast.
<b>Sitzungen, mit denen automatisch eine Verbindung hergestellt werden soll</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu der Sitzung herzustellen.   <b>ANMERKUNG: Beim Namen des Desktops oder der Anwendung wird zwischen Groß- und Kleinschreibung unterschieden. Verwenden Sie ein Semikolon zum Trennen mehrerer Sitzungen, die automatisch initialisiert werden müssen.</b>

## Konfigurieren der VMware Einstellungen

Verwenden Sie die Seite **VMware Einstellungen** zum Konfigurieren der globalen VDI-Einstellungen für die PCoIP-Verbindungen für Geräte mit ThinOS 8.5 und höher.



**Tabelle 72. Grundeinstellungen**

Option	Beschreibung
<b>USB-Umleitungstechnologie</b>	Wählen Sie diese Option, um die USB-Umleitung zu aktivieren. Die USB-Umleitung ist eine Technologie, die Ihnen den Zugriff auf die USB-Geräte ermöglicht, die eine Verbindung mit dem Thin Client von innerhalb eines Remote-Desktops oder einer Anwendung herstellen. Wählen Sie dazu die USB-Umleitung entweder über VMware PCoIP oder über Wyse Thin Client Extensions (TCX).   <b>ANMERKUNG: Wenn Sie die Option TCX USB-Umleitung wählen, benötigen Sie eine zusätzliche TCX Server Suite.</b>
<b>Meldung beim Trennen anzeigen</b>	Wählen Sie diese Option aus, um die Meldung beim Trennen anzuzeigen. Eine Meldung beim Trennen wird angezeigt, wenn das USB-Gerät aus dem System entfernt wurde.
<b>Zeit für Meldung zum erneuten Verbinden anzeigen</b>	Geben Sie die Zeit für die Meldung zum erneuten Verbinden ein.
<b>Zeitüberschreitung bei Fortsetzung</b>	Geben Sie den Wert für die Zeitüberschreitung bei Fortsetzung ein.

## Konfigurieren der Microsoft Broker-Verbindungseinstellungen

Verwenden Sie die Seite mit den **Microsoft Broker**-Verbindungseinstellungen für die Konfiguration von Microsoft Broker-Verbindungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 73. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Broker-Server</b>	Geben Sie den Broker-Serverhostnamen oder die IP-Adresse an.   <b>ANMERKUNG: Sie müssen zwischen HTTP:// oder HTTPS: // wählen.</b>
<b>Sitzungen, mit denen automatisch eine Verbindung hergestellt werden soll</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu der Sitzung herzustellen.   <b>ANMERKUNG: Beim Namen des Desktops oder der Anwendung wird zwischen Groß- und Kleinschreibung unterschieden. Verwenden Sie ein Semikolon zum Trennen mehrerer Sitzungen, die automatisch initialisiert werden müssen.</b>

## Konfigurieren der Microsoft RDP-Verbindungseinstellungen

Verwenden Sie die Seite **Microsoft RDP-Einstellungen** für die Konfiguration von Microsoft RDP-Verbindungseinstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 74. Konfigurieren von Grundeinstellungen**


Option	Beschreibung
<b>NLA aktivieren</b>	Mit dieser Option wird die Authentifizierung auf Netzwerkebene aktiviert. Die Benutzerauthentifizierung ist erforderlich, um eine Verbindung zum Server aufzubauen.
<b>Berichterstellung aktivieren</b>	Wählen Sie diese Option, um die Berichterstellung zu aktivieren.
<b>Aktualisierte NLA erzwingen</b>	Wählen Sie diese Option, damit der Client den RDP-Server zwingen kann, aktualisiertes CredSSP zu verwenden. Der RDP-Client trennt die Sitzung während der Einrichtung, wenn der RDP-Server nicht gepatchtes CredSSP verwendet.

**Tabelle 75. Konfigurieren von RDP8-Einstellungen**

Option	Beschreibung
<b>Bitmap Codec RemoteFX</b>	Wählen Sie diese Option aus, um die Option RemoteFX Bitmap Codec zu aktivieren. Der Standardwert ist "ja". Dell empfiehlt, dass Sie <b>Nein</b> für Wyse 3010 Thin Clients und Wyse 3020 Thin Clients wählen.
<b>TS MM aktivieren</b>	Wählen Sie diese Option aus, um die Multimediaumleitung für den Terminalserver zu aktivieren.
<b>Erweiterung erzwingen</b>	Wählen Sie diese Option aus, um das Erzwingen der Bereichsansicht zu aktivieren. Wenn Sie die Option der

Option	Beschreibung
	Bereichsansicht aktivieren, wird der Remotedesktop als ein Rechteck dargestellt, das dem Bereich Ihrer lokalen Monitore entspricht.
<b>RemoteFX Grafikkanal</b>	Wählen Sie diese Option aus, um den RemoteFX Grafikkanal zu aktivieren.
<b>UDP-Datenverkehrskanal</b>	Wählen Sie diese Option aus, um den RDP 8 UDP-Datenverkehrskanal zu aktivieren. Der Standardwert ist "ja".
<b>Videooptimiertes VOR</b>	Wählen Sie diese Option aus, um für RDP 8-Video optimierte Weiterleitung zu aktivieren. Der Standardwert ist "ja".


**Tabelle 76. Erweiterte Einstellungen konfigurieren**

Option	Beschreibung
<b>USB-Umleitungstechnologie</b>	Wählen Sie diese Option, um die USB-Umleitung zu aktivieren. Die USB-Umleitung ist eine Technologie, die Ihnen den Zugriff auf die USB-Geräte ermöglicht, die eine Verbindung mit dem Thin Client von innerhalb eines Remote-Desktops oder einer Anwendung herstellen. Wählen Sie dazu die USB-Umleitung entweder über VMware PCoIP oder über Wyse Thin Client Extensions (TCX).   <b>ANMERKUNG: Wenn Sie die Option TCX USB-Umleitung wählen, benötigen Sie eine zusätzliche TCX Server Suite.</b>
<b>Farbtiefe</b>	Wählen Sie diese Option zum Konfigurieren des RDP-Protokolls.
<b>Maximaler Bitmap-Cache</b>	Für das Einstellen des maximalen Bitmap-Cache für Ihre RDP-Sitzung geben Sie eine Zahl von 128 bis 1024 ein.
<b>Ausgerichtete Sitzungsbreite von 4 Pixeln</b>	Wählen Sie diese Option aus, um die ausgerichtete Sitzungsbreite von 4 Pixeln zu aktivieren.
<b>Netzwerk automatisch erkennen</b>	Wählen Sie diese Option aus, um das Terminalserver-Gateway automatisch zu ermitteln.
<b>H.264 für RDP aktivieren</b>	Wählen Sie diese Option für das Aktivieren des H.264-Codierungsvorgangs für RDP-Verbindungen.

## Konfigurieren von vWorkspace Broker-Verbindungseinstellungen

Verwenden Sie die Seite mit den **vWorkspace Broker**-Verbindungseinstellungen zum Konfigurieren der vWorkspace Broker-Verbindungseinstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 77. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Broker-Server</b>	Geben Sie den Broker-Serverhostnamen oder die IP-Adresse ein.   <b>ANMERKUNG: Sie müssen zwischen HTTP:// oder HTTPS: // wählen.</b>
<b>vWorkspace-Gateway aktivieren</b>	Wählen Sie diese Option aus, um die Verwendung der vWorkspace-Gateway-Funktionalität zu aktivieren.

Option	Beschreibung
Sitzungen, mit denen automatisch eine Verbindung hergestellt werden soll	<p>Wählen Sie diese Option aus, um automatisch eine Verbindung zu der Sitzung herzustellen.</p> <p><b>ANMERKUNG:</b> Beim Namen des Desktops oder der Anwendung wird zwischen Groß- und Kleinschreibung unterschieden. Verwenden Sie ein Semikolon zum Trennen mehrerer Sitzungen, die automatisch initialisiert werden müssen.</p>

## Konfigurieren von AWS Broker-Verbindungseinstellungen

Verwenden Sie die Seite mit den **AWS-Broker**-Verbindungseinstellungen zum Konfigurieren der AWS-Broker-Verbindungseinstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 78. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
Broker-Server	<p>Geben Sie den Broker-Serverhostnamen oder die IP-Adresse an.</p> <p><b>ANMERKUNG:</b> Sie müssen zwischen HTTP:// oder HTTPS:// wählen.</p>
Sicherheitsmodus	<p>Wählen Sie diese Option zur Angabe der Client-Konnektivität, wenn Sie keine sichere Verbindung zum Server gewährleisten können.</p>
Sitzungen, mit denen automatisch eine Verbindung hergestellt werden soll	<p>Wählen Sie diese Option aus, um automatisch eine Verbindung zu der Sitzung herzustellen.</p> <p><b>ANMERKUNG:</b> Beim Namen des Desktops oder der Anwendung wird zwischen Groß- und Kleinschreibung unterschieden. Verwenden Sie ein Semikolon zum Trennen mehrerer Sitzungen, die automatisch initialisiert werden müssen.</p>

## Konfigurieren von direkten RDP-Verbindungseinstellungen

Verwenden Sie die Seite mit den Einstellungen für die **Direkte RDP-Verbindung** zum Konfigurieren der RDP-Verbindungen, auf die Geräte mit ThinOS 8.5 und höher zugreifen können.

**Tabelle 79. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
Verbindungsname	Geben Sie den Namen der Verbindung mit maximal 38 Zeichen an.
Benutzername	Geben Sie einen Benutzernamen für die Anmeldung an der Anwendung ein.
Hostname oder IP-Adresse	Geben Sie den Host-Namen oder die IP-Adresse der Verbindung ein.
Befehl starten	Geben Sie die Zeichenfolge von Befehlen ein, die nach der Anmeldung am Server ausgeführt werden muss.
Kennwort	Geben Sie das Kennwort für die Anmeldung an der Anwendung ein.

Option	Beschreibung
	<p><b>ANMERKUNG:</b> Das Kennwort wird nicht verschlüsselt. Dell empfiehlt, dass Sie das Kennwort nicht angeben. Sie werden aufgefordert, das Kennwort einzugeben, wenn die Verbindung hergestellt wird.</p>
<b>Domainname</b>	Geben Sie den Domainnamen für das Windows-Netzwerk mit maximal 19 Zeichen ein.
<b>Automatischer Start</b>	Wählen Sie diese Option zum automatischen Neustart der Verbindung.
<b>Nach Trennung erneut verbinden</b>	Wählen Sie diese Option aus, um die Verbindung automatisch wiederherzustellen, nachdem sie getrennt wurde.
<b>Auf Bildschirm</b>	<p>Wählen Sie aus der Dropdown-Liste die gewünschte Anzeige aus, auf der Sie die RDP-Sitzung starten möchten.</p> <p>Wenn der im Bildschirmparameter für Ihre RDP-Verbindung definierte Wert höher ist als die Anzahl der an den Thin Client angeschlossenen Displays, wird die Bildschirmauflösung als Standard festgelegt.</p>

**Tabelle 80. Lokale Ressourcen konfigurieren**


Option	Beschreibung
<b>Drucker zuordnen</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu den lokalen Druckern herzustellen, wenn die Sitzung gestartet wird.
<b>Serielle Schnittstellen zuordnen</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu den lokalen seriellen Schnittstellen herzustellen, wenn die Sitzung gestartet wird.
<b>Smartcards zuordnen</b>	Wählen Sie diese Option aus, um die Smartcards an die Remotesitzung umzuleiten.
<b>USB-Laufwerke zuordnen</b>	Wählen Sie diese Option aus, um das USB-Laufwerk automatisch zuzuordnen, wenn die Sitzung gestartet wird.
<b>Lokale Festplatten zuordnen</b>	Wählen Sie diese Option aus, um die lokalen Festplatten automatisch zuzuordnen, wenn die Sitzung gestartet wird.

**Tabelle 81. Konfigurieren von Sitzungseinstellungen**

Option	Beschreibung
<b>Audiowiedergabe</b>	<p>Diese Option hilft Ihnen festzulegen, wie Ton in der Remote-Sitzung abgespielt werden muss. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Nicht wiedergeben</li> <li>• Lokal wiedergeben</li> <li>• Über Fernbedienung wiedergeben</li> </ul>
<b>RDP-Audioaufzeichnung</b>	Wählen Sie diese Option aus, um die Tonaufzeichnung im Remote-Zugriff zu ermöglichen.

Option	Beschreibung
<b>Standardfarbtiefe für die Verbindungen</b>	Wählen Sie diese Option zum Definieren der Bildschirm-Farbtiefe der Verbindung.

**Tabelle 82. Erweiterte Einstellungen konfigurieren**

Option	Beschreibung
<b>Verbindungsanzeige</b>	Wählen Sie diese Option aus, um die Bildschirmauflösung auf dem Remotedesktop festzulegen.
<b>Komprimierung deaktivieren</b>	Wählen Sie diese Option aus, um die Dateien zur Reduzierung der benötigten Download-Zeit zu komprimieren.
<b>Netzwerk automatisch erkennen</b>	Wählen Sie diese Option aus, um das Terminalserver-Gateway automatisch zu ermitteln.
<b>Zeitgeber für Mauswarteschlange</b>	Zum Festlegen des Zeitgebers für die Mauswarteschlange in einer ICA- oder RDP-Sitzung, geben Sie eine Zahl zwischen 0 und 99 ein.
<b>Funktionsweise des Sitzungsfensters</b>	Wählen Sie diese Option aus, um zu definieren, ob die Remoteverbindung in einem Vollbildschirm-Modus gestartet werden sollte. Wählen Sie je nach Wunsch entweder <b>Vollbild</b> oder <b>Fenstermodus</b> .   <b>ANMERKUNG: Der Zero-Launchpad-Modus unterstützt nur Vollbildsitzungen. Der Fenstermodus startet nur auf einem einzigen Bildschirm, während Vollbildsitzungen beide Bildschirme umfassen.</b>

**Tabelle 83. Konfigurieren von Terminal Gateway-Einstellungen**


Option	Beschreibung
<b>Terminalserver-Gateway verwenden</b>	Wählen Sie diese Option zur Angabe der Anmeldedaten für den Windows Terminal-Server. Wenn diese Option aktiviert ist, geben Sie die folgenden Einzelheiten ein: <ul style="list-style-type: none"> <li>• RD-Host-Name oder IP-Adresse</li> <li>• RD-Benutzername</li> <li>• RD-Kennwort</li> <li>• RD-Domainname</li> </ul>

## Konfigurieren von direkten ICA-Verbindungseinstellungen


Verwenden Sie die Seite mit den Einstellungen für die **Direkte ICA-Verbindung** zum Konfigurieren der ICA-Verbindungen, auf die Geräte mit ThinOS 8.5 und höher zugreifen können.

**Tabelle 84. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Verbindungsname</b>	Geben Sie den Namen der Verbindung mit maximal 38 Zeichen an.
<b>Benutzername</b>	Geben Sie einen Benutzernamen für die Anmeldung an der Anwendung ein.

Option	Beschreibung
<b>Kennwort</b>	Geben Sie das Kennwort für die Anmeldung an der Anwendung ein.   <b>ANMERKUNG: Das Kennwort wird nicht verschlüsselt. Dell empfiehlt, dass Sie das Kennwort nicht angeben. Sie werden aufgefordert, das Kennwort einzugeben, wenn die Verbindung hergestellt wird.</b>
<b>Domainname</b>	Geben Sie den Domainnamen für das Windows-Netzwerk mit maximal 19 Zeichen ein.
<b>Automatischer Start</b>	Wählen Sie diese Option zum automatischen Neustart der Verbindung.
<b>Nach Trennung erneut verbinden</b>	Wählen Sie diese Option aus, um die Verbindung automatisch wiederherzustellen, nachdem sie getrennt wurde.

**Tabelle 85. Konfigurieren der Verbindungseinstellungen**

Option	Beschreibung
<b>Host oder Anwendung</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
<b>Hostname oder IP-Adresse</b>	Geben Sie den Host-Namen oder die IP-Adresse der Verbindung ein.
<b>Browser-IP</b>	Geben Sie die Liste der IP-Adressen oder DNS-registrierten Namen ein.
<b>Verschlüsselung</b>	Wählen Sie diese Option zum Einstellen einer Verschlüsselungsebene aus. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>Auflösung</b>	Wählen Sie diese Option aus, um die Auflösung Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Auflösung für Ihren Monitor aus.   <b>ANMERKUNG: Wenn Sie eine nicht unterstützte Auflösung wählen, ignoriert das Gerät die Einstellung.</b>

**Tabelle 86. Lokale Ressourcen konfigurieren**

Option	Beschreibung
<b>Drucker zuordnen</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu den lokalen Druckern herzustellen, wenn die Sitzung gestartet wird.
<b>Serielle Schnittstellen zuordnen</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu den lokalen seriellen Schnittstellen herzustellen, wenn die Sitzung gestartet wird.
<b>Smartcards zuordnen</b>	Wählen Sie diese Option aus, um die Smartcards an die Remotesitzung umzuleiten.

**Tabelle 87. Konfigurieren der Anmeldeinstellungen**

Option	Beschreibung
<b>Anmeldemethode</b>	Wählen Sie diese Option zum Auswählen der Anmeldemethode.
<b>Befehl zum Starten der Anwendung</b>	Geben Sie den Befehl zum Starten der Anwendung ein.
<b>Befehl zum Starten des Arbeitsverzeichnisses</b>	Geben Sie den Befehl zum Starten des Arbeitsverzeichnisses ein.

**Tabelle 88. Konfigurieren von Sitzungseinstellungen**

Option	Beschreibung
<b>Audioqualität</b>	Wählen Sie diese Option aus, um die Audioqualität festzulegen.
<b>Adresse über Firewall ändern</b>	Wählen Sie diese Option für die Aktivierung einer alternativen Adresse durch die Firewall.
<b>Sitzungszuverlässigkeit</b>	Wählen Sie diese Option aus, um die ICA-Sitzungszuverlässigkeit zu aktivieren.
<b>Für langsame Linkgeschwindigkeit optimieren</b>	Aktivieren Sie das Kontrollkästchen, um die Sitzungseinstellungen für eine niedrige Linkgeschwindigkeit zu optimieren.
<b>Schriftartglättung</b>	Wählen Sie diese Option, um die Schriftglättung zu aktivieren. Die Schriftglättung ist eine Methode zum Erzielen schärferer Schriftarten bei Bildschirmen mit niedriger Auflösung.
<b>Funktionsweise des Sitzungsfensters</b>	Wählen Sie diese Option aus, um zu definieren, ob die Remoteverbindung in einem Vollbildschirm-Modus gestartet werden sollte. Wählen Sie je nach Wunsch entweder <b>Vollbild</b> oder <b>Fenstermodus</b> .  <div style="border-left: 1px solid black; padding-left: 5px; margin-left: 10px;"> <p><b>ANMERKUNG:</b> Der Zero-Launchpad-Modus unterstützt nur Vollbildsitzungen. Der Fenstermodus startet nur auf einem einzigen Bildschirm, während Vollbildsitzungen beide Bildschirme umfassen.</p> </div>

## Konfigurieren der globalen Druckereinstellungen

Verwenden Sie die Seite **Globale Einstellungen** zur Konfiguration von globalen Druckereinstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 89. Konfigurieren der Standard-Druckereinstellungen**

Option	Beschreibung
<b>Standarddrucker</b>	Wählen Sie diese Option aus, um einen Drucker als Standarddrucker festzulegen.
<b>PrinterMap-Einstellungen</b>	Die hochgeladenen Dateien unter <b>Anwendungen und Daten &gt; Datei-Repository &gt; Bestandsaufnahme</b> werden angezeigt. Wählen Sie aus dem Dropdownmenü die Zuweisungsdatei aus.

## Konfigurieren der Druckereinstellungen

Verwenden Sie die Seite mit den **Drucker**-Einstellungen zum Konfigurieren eines neuen Druckers für Geräte mit ThinOS 8.5 und höher.

**Tabelle 90. Konfigurieren der Druckerauswahl**

Option	Beschreibung
<b>Druckertyp</b>	Wählen Sie aus dem Dropdownmenü den Druckertyp aus. Es gibt folgende Typen von Druckern: <ul style="list-style-type: none"> <li>• Lokaler Drucker</li> <li>• LPD-Drucker</li> <li>• SMB-Drucker</li> </ul>
<b>Lokaler Drucker</b>	Wählen Sie aus dem Dropdownmenü die lokale Druckerverbindung aus.

**Tabelle 91. Konfigurieren der Druckereinstellungen**

Option	Beschreibung
<b>Name</b>	Geben Sie den Namen des freigegebenen Druckers ein.
<b>LocalName</b>	Diese Option gilt nur für LPD-Drucker. Geben Sie den Namen des Druckers ein.
<b>Host</b>	Diese Option gilt nur für lokale LPD-Drucker. Geben Sie die IP-Adresse des LPD-Diensthosts ein.
<b>Warteschlange</b>	Diese Option gilt nur für LPD-Drucker. Geben Sie den Warteschlangennamen des Druckers ein.
<b>Benutzername</b>	Diese Option gilt nur für SMB-Drucker. Geben Sie den Benutzernamen ein.
<b>Kennwort</b>	Diese Option gilt nur für SMB-Drucker. Geben Sie das Kennwort ein.
<b>Domain</b>	Diese Option gilt nur für SMB-Drucker. Geben Sie den Domännennamen ein.
<b>Drucker-ID</b>	Geben Sie die Drucker-ID an. Die Drucker-ID gibt den Windows-Druckertreibernamen an. Die Standard-Drucker-ID ist <b>Generisch/Nur Text</b> . Diese Wert unterscheidet Groß- und Kleinschreibung.
<b>Klasse</b>	Geben Sie die Klasse in das entsprechende Feld ein. Die folgenden Optionen sind die vordefinierten Klassen: <ul style="list-style-type: none"> <li>• PCL4</li> <li>• PCL5</li> <li>• PS</li> <li>• TXT</li> </ul>
<b>Aktiviert</b>	Aktivieren Sie das Kontrollkästchen, um den Drucker zu aktivieren.
<b>EnableLPD</b>	Diese Option gilt nur für lokale Drucker und SMB-Drucker. Aktivieren Sie das Kontrollkästchen, um den LPD-Dienst zu aktivieren.

## Konfigurieren von globalen WLAN-Einstellungen

Verwenden Sie die Seite **Globale WLAN-Einstellungen** zur Konfiguration von globalen WLAN-Einstellungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 92. Konfigurieren von globalen WLAN-Einstellungen**

Option	Beschreibung
<b>Roaming-Empfindlichkeit</b>	Wählen Sie diese Option zur Auswahl der Empfindlichkeit des Wireless Roaming.
<b>Band deaktivieren</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Die Konfiguration <b>Band deaktivieren</b> kann verwendet werden, um das 2,4G- oder 5G-802.11-Band zu deaktivieren. Der Standardwert ist <b>Kein Band deaktivieren</b> .
<b>Band bevorzugen</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Die Konfiguration <b>Band bevorzugen</b> kann verwendet werden, um eine Priorität für ein kabelloses Verbindungsband festzulegen, und um den 2,4G- oder 5G-Zugangspunkt zu wählen, um eine Verbindung herzustellen. Der Standardwert ist <b>Kein Band bevorzugen</b> .
<b>DisableN</b>	Wählen Sie das Kontrollkästchen, um den 802.11n-Modus zu deaktivieren.
<b>WLAN deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der WLAN-Funktion. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Wenn Sie die Option <b>EnetUp</b> aus dem Dropdownmenü auswählen, wird das WLAN deaktiviert, wenn das Ethernet aktiv ist und ausgeführt wird.

## Konfigurieren von WLAN-Verbindungen

Verwenden Sie die Seite **WLAN-Verbindungen** zum Konfigurieren der Thin Client WLAN-Verbindungen für Geräte mit ThinOS 8.5 und höher.

**Tabelle 93. Konfigurieren von Authentifizierungseinstellungen**

Option	Beschreibung
<b>Sicherheitstyp</b>	Wählen Sie diese Option aus, um die Authentifizierungsmethode anzugeben. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Öffnen</li> <li>• Open(WEP)</li> <li>• SharedKey</li> <li>• WPA-Personal</li> <li>• WPA-Enterprise</li> <li>• WPA2-Personal</li> <li>• WPA2-Enterprise</li> </ul>
<b>Verschlüsselung</b>	Diese Option gilt nur für Open (WEP), SharedKey, WPA-Personal und WPA-Enterprise. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>Web-Schlüssel1,2,3 und 4</b>	Diese Option gilt nur für Open(WEP) und SharedKey. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>WPA-Schlüssel</b>	Diese Option gilt nur für WPA-Personal und WPA2-Personal. Geben Sie den WPA-Schlüssel in das entsprechende Feld ein.

Option	Beschreibung
<b>Netzwerktyp</b>	Diese Option gilt nur für WPA-Personal, WPA-Enterprise, WPA2-Personal und WPA2-Enterprise. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.

**Tabelle 94. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>SSID</b>	Geben Sie den Namen der SSID-Verbindung (Service Set Identifier) ein.
<b>Modus</b>	Wählen Sie aus dem Dropdownmenü den gewünschten Modus aus.

**Tabelle 95. Konfigurieren von IEEE 802.1x-Einstellungen für WPA-Enterprise und WPA2-Enterprise**

Option	Beschreibung
<b>EAP-Typ</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>FAST-Typ</b>	Diese Option gilt nur für EAP-FAST[8.3]. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>LEAP-Benutzername</b>	Diese Option gilt nur für EAP-LEAP. Geben Sie den Leap-Benutzernamen in das entsprechende Feld ein.
<b>LEAP-Kennwort</b>	Diese Option gilt nur für EAP-LEAP. Geben Sie das LEAP-Kennwort in das entsprechende Feld ein.
<b>Servervalidierung</b>	Diese Option gilt nur für EAP-TLS und EAP-PEAP. Aktivieren Sie das Kontrollkästchen, um die Server-Verbindung zu validieren.
<b>Serverprüfung</b>	Diese Option gilt nur für EAP-TLS und EAP-PEAP. Aktivieren Sie das Kontrollkästchen, um die Server-Verbindung zu überprüfen.
<b>Server Name</b>	Diese Option gilt nur für EAP-TLS und EAP-PEAP. Geben Sie den Servernamen ein.
<b>Dateiname des Client-Zertifikats</b>	Diese Option gilt nur für EAP-TLS. Geben Sie den Dateinamen des Clientzertifikats ein.
<b>PrivateKey – Kennwort des Client-Zertifikats</b>	Diese Option gilt nur für EAP-TLS. Geben Sie den PrivateKey – Kennwort des Client-Zertifikats in das entsprechende Feld ein.
<b>TLS-Authentifizierungstyp</b>	Diese Option gilt nur für EAP-TLS. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>PEAP TLS-Version</b>	Diese Option gilt nur für EAP-TLS. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>PEAP-Typ</b>	Diese Option gilt nur für EAP-PEAP. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>EAP-Identität</b>	Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3]. Geben Sie die EAP-Identität ein.
<b>Benutzername</b>	Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3]. Geben Sie den Benutzernamen ein.
<b>Kennwort</b>	Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3]. Geben Sie das Kennwort ein.

Option	Beschreibung
<b>Domäne verbergen</b>	Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3]. Aktivieren Sie das Kontrollkästchen, um die Domäne zu verbergen.
<b>Domain</b>	Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3]. Geben Sie den Domänennamen ein.
<b>Einfache Anmeldung aktivieren</b>	Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3]. Wählen Sie das Kontrollkästchen zum Aktivieren der Funktion "einfache Anmeldung" aus.

## Konfigurieren von LAN-Verbindungen

Verwenden Sie die Seite **LAN-Verbindungen (8.6+)** zum Konfigurieren der LAN-Verbindungen für Geräte mit ThinOS 8.6 und höher.

**Tabelle 96. Konfigurieren von IEEE 802.1x-Einstellungen**

Option	Beschreibung
<b>Netzwerktyp</b>	<p>Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Das System startet automatisch neu und die Änderungen am Netzwerktyp werden angewendet.</p> <p><b>ANMERKUNG:</b> Wenn Sie Änderungen an dieser Einstellung vornehmen, wird der Thin Client neu gestartet. Ab ThinOS 8.5_020 können Sie den Neustart verzögern, indem Sie in den Allgemeinen Einstellungen die Option An Neustart erinnern aktivieren.</p>
<b>Ethernet-Geschwindigkeit</b>	<p>Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Die ausgewählte Option wird im nichtflüchtigen Speicher gespeichert. Das System startet automatisch neu und die Änderungen an der Ethernet-Geschwindigkeit werden angewendet.</p> <p><b>ANMERKUNG:</b> Wenn Sie Änderungen an dieser Einstellung vornehmen, wird der Thin Client neu gestartet. Ab ThinOS 8.5_020 können Sie den Neustart verzögern, indem Sie in den Allgemeinen Einstellungen die Option An Neustart erinnern aktivieren.</p>
<b>Aktivieren der IEEE802.1x-Authentifizierung</b>	<p>Mit dieser Option wird die IEEE802.1x-Authentifizierung aktiviert. IEEE 802.1X ist ein IEEE-Standard für die portbasierte Netzwerk-Zugriffssteuerung (PNAC). Er ist Bestandteil der IEEE 802.1-Gruppe von Netzwerkprotokollen. Er stellt eine Authentifizierungsmethode für die Geräte mit LAN oder WLAN bereit.</p>
<b>EAP-Typ</b>	<p>Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Die verfügbaren Optionen sind:</p> <ul style="list-style-type: none"> <li>• <b>Light Weight Extensible Authentication Protocol (EAP-LEAP):</b> Dies ist ein Authentifizierungsprotokoll, das bei Drahtlosnetzwerken und Punkt-zu-Punkt-Verbindungen verwendet wird. LEAP ist speziell für eine sicherere Authentifizierung für 802.11-WLANs (Wireless Local Area Network) mit Unterstützung der 802.1X-Portzugriffssteuerung ausgelegt.</li> <li>• <b>Transport Layer Security (EAP-TLS):</b> bietet Client- und Serverauthentifizierung. Dieses Protokoll wird häufig für</li> </ul>

Option	Beschreibung
	<p>Drahtlosnetzwerke verwendet und bietet eine sicherere Authentifizierung für Wireless-Clients und Server.</p> <ul style="list-style-type: none"> <li>• <b>Protected Extensible Authentication Protocol (EAP-PEAP):</b> Dieses Protokoll erfasst das Extensible Authentication Protocol (EAP) innerhalb eines verschlüsselten und authentifizierten TLS-Tunnels (Transport Layer Security). Es bietet Client- und Serverauthentifizierung.</li> <li>• <b>Flexible Authentication via Secure Tunneling (EAP-FAST[8.3]):</b> wird in Drahtlosnetzwerken und Punkt-zu-Punkt-Verbindungen zur Durchführung der Sitzungsauthentifizierung verwendet. EAP-FAST[8.3] ist ein Ersatz für das Lightweight Extensible Authentication Protocol (LEAP). LEAP ist ein Authentifizierungsprotokoll für Drahtlosnetzwerke, das bekannte Sicherheitslücken bei Verwendung mit schwachen Kennwörtern aufweist. EAP-FAST schließt diese Sicherheitslücken mittels Authentifizierung über einen TLS-Tunnel, der mit geschützten Zugriffsdaten (Protected Access Credential, PAC) hergestellt wird.</li> </ul>
<b>FAST-Typ</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Diese Option gilt nur für EAP-FAST[8.3].
<b>LEAP-Benutzername</b>	Geben Sie den Leap-Benutzernamen in das entsprechende Feld ein. Diese Option gilt nur für EAP-LEAP.
<b>LEAP-Kennwort</b>	Geben Sie das LEAP-Kennwort in das entsprechende Feld ein. Diese Option gilt nur für EAP-LEAP.
<b>Servervalidierung</b>	Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass das System die Serververbindung überprüft. Diese Option gilt nur für EAP-TLS und EAP-PEAP.
<b>Serverprüfung</b>	Aktivieren Sie das Kontrollkästchen, um die Server-Verbindung zu überprüfen. Diese Option gilt nur für EAP-TLS und EAP-PEAP.
<b>Server Name</b>	Geben Sie den Servernamen ein. Diese Option gilt nur für EAP-TLS und EAP-PEAP.
<b>Dateiname des Client-Zertifikats</b>	Geben Sie den Dateinamen des Clientzertifikats ein. Diese Option gilt nur für EAP-TLS.
<b>PrivateKey – Kennwort des Client-Zertifikats</b>	Geben Sie den PrivateKey – Kennwort des Client-Zertifikats in das entsprechende Feld ein. Diese Option gilt nur für EAP-TLS.
<b>TLS-Authentifizierungstyp</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Diese Option gilt nur für EAP-TLS.
<b>PEAP TLS-Version</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Diese Option gilt nur für EAP-TLS.
<b>PEAP-Typ</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. Diese Option gilt nur für EAP-PEAP.
<b>EAP-Identität</b>	Geben Sie die EAP-Identität ein. Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3].
<b>Benutzername</b>	Geben Sie den Benutzernamen ein. Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3].
<b>Kennwort</b>	Geben Sie das Kennwort ein. Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3].
<b>Domäne verbergen</b>	Aktivieren Sie das Kontrollkästchen, um die Domäne zu verbergen. Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3].

Option	Beschreibung
<b>Domain</b>	Geben Sie den Domänennamen ein. Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3].
<b>Einfache Anmeldung aktivieren</b>	Wählen Sie das Kontrollkästchen zum Aktivieren der Funktion "einfache Anmeldung" aus. Diese Option gilt nur für EAP-PEAP und EAP-FAST[8.3].

## Konfigurieren von SCEP-Einstellungen

Verwenden Sie die Seite **SCEP-Einstellungen (8.6+)** zum Konfigurieren der SCEP-Einstellungen für ThinOS 8.6 und neuere Versionen.

**Tabelle 97. Konfigurieren von SCEP 8.6+-Einstellungen**

Option	Beschreibung
<b>Automatische SCEP-Registrierung</b>	Wählen Sie diese Option für die Aktivierung der automatischen Zertifikatregistrierung mithilfe des SCEP-Servers der Umgebung.
<b>Automatische Verlängerung</b>	Wählen Sie diese Option für die Aktivierung der automatischen Zertifikatsverlängerung. Der Thin Client versucht, die angeforderten Zertifikate manuell oder automatisch über SCEP zu verlängern. Die Verlängerung, die nach der Hälfte des Gültigkeitszeitraums des vorhandenen Zertifikats initiiert wurde, ist abgelaufen.
<b>CA-Zertifikate installieren</b>	Wählen Sie diese Option zur Installation des Zertifikats der Stamm-CA als vertrauenswürdigen Zertifikat.
<b>Land</b>	Geben Sie den Ländernamen ein. Der Ländername muss aus zwei Großbuchstaben bestehen.
<b>Zustand</b>	Geben Sie den Namen des Staats/Bundeslands ein.
<b>Standort</b>	Geben Sie den Standortnamen ein.
<b>Unternehmen</b>	Geben Sie den Unternehmensnamen ein.
<b>Organisationseinheit</b>	Geben Sie den Namen der Organisationseinheit ein.
<b>Allgemeiner Name</b>	Geben Sie den allgemeinen Namen wie z. B. „\$TN.dellwyse.com“ ein. Sie können den Terminalnamen als Teil des allgemeinen Namens verwenden.
<b>E-Mail</b>	Geben Sie die E-Mail-Adresse ein.
<b>Schlüsselverwendung</b>	Wählen Sie die bevorzugte Schlüsselverwendung.
<b>Schlüssellänge</b>	Wählen Sie aus der Dropdownliste die Schlüssellänge des Clientzertifikats in Bit aus.
<b>Alternativer Antragstellernamen</b>	Geben Sie den alternativen Namen für das Clientzertifikat ein. Es handelt sich um eine Liste mit Namen wie z. B. E-Mail-Adressen, IP-Adressen, URLs und DNS, bei der Sie ein Semikolon (;) als Trennzeichen verwenden müssen.
<b>Anfrage-URL</b>	Geben Sie die Dienst-URL des SCEP-Servers ein.
<b>Hash-Typ des CA-Zertifikats</b>	Wählen Sie aus der Dropdownliste den Hash-Wert aus, der verwendet wird, um die Zertifikatauthentifizierung zu überprüfen.

Option	Beschreibung
Hash des CA-Zertifikats	Geben Sie den MD5-Hashwert ein, um die CA-Echtheit zu überprüfen.
Registrierungskennwort	Geben Sie das Registrierungskennwort ein.
Registrierungskennwort verschlüsseln	Aktivieren Sie das Kontrollkästchen zum Aktivieren der Verschlüsselung für das Registrierungskennwort.
SCEP-Administrator-URL	Geben Sie die SCEP-Administrator-URL ein.
SCEP-Benutzer	Geben Sie den SCEP-Administratorbenutzernamen ein.
SCEP-Benutzerkennwort	Geben Sie das SCEP-Administratorkennwort ein.
SCEP-Benutzerkennwort verschlüsseln	Wählen Sie diese Option aus, um das Kennwort festzulegen. Geben Sie das verschlüsselte SCEP-Administratorkennwort ein, das Sie unter <a href="https://scep.dellwyse.com/CertSrv/mscep_admin">https://scep.dellwyse.com/CertSrv/mscep_admin</a> erhalten haben.
SCEP-Benutzerdomain	Geben Sie die SCEP-Benutzerdomain ein.

## Konfigurieren von Proxy-Einstellungen

Verwenden Sie die Seite **Proxy (8.6+)** zum Konfigurieren der Proxy-Einstellungen für Geräte mit ThinOS 8.6 und höher.

**Tabelle 98. Konfigurieren der Proxy-Servereinstellungen für 8.6+**

Option	Beschreibung
Proxy-Einstellungen	Aktivieren Sie das Kontrollkästchen zum Aktivieren der Proxy-Einstellungen, die im nichtflüchtigen Speicher gespeichert sind.
App-Liste	Diese Liste enthält Informationen darüber, welche Anwendung den konfigurierten Proxy verwendet.
Proxy-Protokoll mit Global, Http, Https und Socks5 aktivieren	Wählen Sie aus der Dropdownliste das Proxy-Protokoll mit Global, Http, Https und Socks5 aus. Wenn Sie <b>Ja</b> in der Dropdownliste <b>Proxy-Protokoll mit Global, Http, Https und Socks5 aktivieren</b> auswählen, dann geben Sie den <b>Servernamen</b> , den <b>Benutzernamen</b> und das <b>Kennwort</b> ein. Um zu überprüfen, ob das Kennwort verschlüsselt ist oder nicht, wählen Sie die Option <b>Verschlüsseln</b> .

## Bearbeiten von Windows Embedded Standard-Richtlinieneinstellungen

Zum Bearbeiten der Richtlinieneinstellungen für Windows Embedded Standard (WES) führen Sie die folgenden Schritte aus:

- 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. Die Windows Embedded Standard Thin Client-Richtlinieneinstellungen umfassen die folgenden Optionen:
  - Systempersonalisierung

- Desktoperlebnis
- Netzwerk
- Sicherheit und Sperrmodus
- Andere Einstellungen
- Citrix Remote-Verbindungen
- VMware Remote-Verbindungen
- RDP Remote-Verbindungen
- Browser-Remote-Verbindungen
- BIOS-Einstellungen für mobilen Latitude Thin Client
- BIOS-Einstellungen für Wyse 7040 Thin Client
- Geräteinfo
- Wyse Easy Setup
- VNC-Einstellungen
- Domäneneinstellungen
- BIOS-Einstellungen für WES 5070

4 Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Konfigurieren der Systempersonalisierung

Verwenden Sie die Systempersonalisierungsseite zum Konfigurieren der Thin Client-Einstellungen, wie z. B. Anzeige, Tastatur, Maus, Zeitzone und Audio-Optionen für Windows Embedded Standard-Geräte.

**Tabelle 99. Konfigurieren von Anzeigeoptionen**

Option	Beschreibung
<b>Dualmonitor aktivieren</b>	Wählen Sie diese Option aus, um die Dualmonitor-Funktion zu aktivieren. Wenn diese Option ausgewählt ist, ist die Option <b>Anzeigemodus</b> verfügbar.
<b>Anzeigemodus</b>	<p>Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Diese Anzeigen duplizieren</li> <li>• Diese Anzeigen erweitern</li> </ul> <p>Wenn Sie <b>Diese Bildschirme erweitern</b> auswählen, sind folgende Optionen verfügbar:</p> <ul style="list-style-type: none"> <li>• <b>Monitorauflösung (sekundär)</b>—Wählen Sie diese Option aus, um die Auflösung Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Auflösung aus, die am besten Ihrem Monitortyp entspricht.</li> <li>• <b>Monitorkennung (sekundär)</b>—Wählen Sie diese Option aus, um eine Kennung für den Monitor einzustellen. Wählen Sie aus dem Dropdownmenü eine geeignete Monitoridentifizierungsnummer.</li> <li>• <b>Monitorausrichtung (sekundär)</b>—Wählen Sie diese Option aus, um eine Ausrichtung für den Monitor einzustellen. Wählen Sie im Dropdownmenü nach Bedarf eine der Optionen für die Monitorausrichtung aus: <ul style="list-style-type: none"> <li>– Querformat</li> <li>– Hochformat</li> <li>– Querformat umgedreht</li> <li>– Hochformat umgedreht</li> </ul> </li> </ul>

Option	Beschreibung
<b>Monitorauflösung (primär)</b>	Wählen Sie diese Option aus, um die Auflösung Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Auflösung aus, die am besten Ihrem Monitortyp entspricht.
<b>Anzeigenkennung (primär)</b>	Wählen Sie diese Option aus, um eine Anzeigenkennung für Ihren Monitor einzugeben. Wählen Sie aus dem Dropdownmenü eine geeignete Monitoridentifizierungsnummer.
<b>Monitordrehung (primär)</b>	Wählen Sie diese Option aus, um eine Ausrichtungsoption für den Monitor einzustellen. Wählen Sie im Dropdownmenü nach Bedarf eine der Optionen für die Monitorausrichtung aus: <ul style="list-style-type: none"> <li>• Querformat</li> <li>• Hochformat</li> <li>• Querformat umgedreht</li> <li>• Hochformat umgedreht</li> </ul>

**Tabelle 100. Konfigurieren von Mausoptionen, grundlegenden Mausoptionen sowie Optionen für Mauszeiger und Mausvertikale**

Option	Beschreibung
<b>Mausgeschwindigkeit</b>	Wählen Sie diese Option aus, um die Geschwindigkeit des Mauszeigers beim Bewegen der Maus anzugeben.
<b>Linkshänder-Maus</b>	Wählen Sie diese Option aus, um die linke und rechte Maustaste zu vertauschen.
<b>KlickEinrasten</b>	Wählen Sie diese Option aus, um mit dem Mauszeiger ohne Gedrückthalten der Maustaste zu markieren oder zu ziehen. Wählen Sie zum Einstellen des Parameters <b>Klick-Einrasten-Zeit</b> aus dem Dropdownmenü die gewünschte Zeit für die die Maustaste gedrückt gehalten werden muss, bevor das Klicken gesperrt wird.
<b>Doppelklickgeschwindigkeit</b>	Wählen Sie diese Option, um das Zeitintervall zwischen zwei aufeinanderfolgenden Mausklicks festzulegen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>Mauszeiger finden</b>	Wählen Sie diese Option aus, wenn Sie den Mauszeiger finden möchten, wenn er nicht in Bewegung ist. <b>ANMERKUNG:</b> Sie können die <code>strg</code> -Taste auf der Tastatur drücken, um den Mauszeiger zu finden, wenn er nicht in Bewegung ist.
<b>Mauszeiger ausblenden</b>	Wählen Sie diese Option zum Ausblenden des Mauszeigers, wenn er nicht in Bewegung ist. <b>ANMERKUNG:</b> Um den Mauszeiger zu finden, wenn er nicht in Bewegung ist, drücken Sie die Taste <code>strg</code> .
<b>Zeigerpfadlänge</b>	Wählen Sie diese Option zum Definieren der Länge des Zeigerpfads, wenn der Mauszeiger bewegt wird.
<b>Zur Standardschaltfläche springen</b>	Wählen Sie diese Option aus, um in Dialogfeldern automatisch zur Standardschaltfläche zu springen.
<b>Scrollzeilen</b>	Wählen Sie diese Option aus, um die Anzahl der gleichzeitig gescrollten Zeilen beim vertikalen Scrollen zu definieren.

**Tabelle 101. Konfigurieren von Zeitzoneoptionen**

Option	Beschreibung
<b>Zeitserver (NTP-Server)</b>	Wählen Sie diese Option zum Anzeigen der Zeitserver zum Aktivieren der lokalen Zeitsynchronisierung. Geben Sie die NTP-Server jeweils getrennt durch ein Komma ein.
<b>Name der Zeitzone</b>	Wählen Sie diese Option zum Einstellen der Zeitzone auf Ihrem Gerät. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Zeitzone.

**Tabelle 102. Konfigurieren von Audio-Optionen**

Option	Beschreibung
<b>Audio stumm schalten</b>	Wählen Sie diese Option aus, um den Ton Ihres Geräts stummzuschalten.
<b>Audiolautstärke</b>	Wählen Sie diese Option aus, um die Lautstärke Ihres Geräts anzupassen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Lautstärkeoption.
<b>Mikrofon stumm schalten</b>	Wählen Sie diese Option aus, um das Mikrofon stummzuschalten.
<b>Mikrofonlautstärke</b>	Wählen Sie diese Option aus, um die Lautstärke des Mikrofons einzustellen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Lautstärkeoption.

## Desktop-Erfahrung konfigurieren

Verwenden Sie diese Seite zum Konfigurieren der Thin Client Einstellungen, wie z. B. Desktop-Hintergrundbild und Desktopfarbe für Windows Embedded Standard-Geräte.

**Tabelle 103. Desktop-Erfahrung konfigurieren**

Option	Beschreibung
<b>Desktophintergrund</b>	<p>Wählen Sie diese Option aus, um ein Hintergrundbild für Ihren Desktop festzulegen.</p> <p>Nach Aktivierung der Option Desktop-Hintergrundbild gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> <li>Wählen Sie aus der Dropdownliste <b>Hintergrundbild-Datei</b> ein Hintergrundbild für Ihren Desktop aus.</li> </ul> <p><b>i ANMERKUNG:</b> Wählen Sie nur ein Hintergrundbild aus der Liste der Hintergrundbilder, die in das Datei-Repository hochgeladen wurden.</p> <ul style="list-style-type: none"> <li>Wählen Sie aus der Dropdownliste <b>Hintergrundbild-Layout</b> eines der folgenden Layouts für Ihr Desktop-Hintergrundbild: <ul style="list-style-type: none"> <li>Zentriert</li> <li>Nebeneinander</li> <li>Strecken</li> <li>Füllen</li> </ul> </li> </ul>
<b>Desktopfarbe</b>	Wählen Sie diese Option aus, um eine Hintergrundfarbe für den lokalen Desktop festzulegen.

# Konfigurieren der Netzwerkeinstellungen

Verwenden Sie diese Seite zum Konfigurieren der Netzwerkeinstellungen für Windows Embedded Standard-Geräte.

**Tabelle 104. Konfigurieren der Netzwerkeinstellungen**

Option	Beschreibung
<b>WLAN-Status</b>	<p>Wählen Sie diese Option aus, um den Status "drahtloser Funkempfänger" zu aktivieren.</p> <p><b>ANMERKUNG:</b> Diese Option ist ähnlich zum Ein- oder Auszuschalten des Geräts.</p>
<b>Windows Wireless-Profil</b>	<p>Wählen Sie diese Option aus, um ein Windows Wireless-Profil festzulegen. Wählen Sie aus dem Dropdownmenü Ihr bevorzugtes Windows Wireless-Profil aus.</p> <p><b>ANMERKUNG:</b> Wählen Sie nur ein Profil aus der Liste der Wireless-Profile, die in das Datei-Repository hochgeladen wurden.</p>

# Konfigurieren der Sicherheits- und Sperrmoduseinstellungen

Verwenden Sie diese Seite für die Konfiguration der Sicherheits- und Sperrmoduseinstellungen.

# Andere Einstellungen konfigurieren

Verwenden Sie diese Seite zum Konfigurieren der Thin Client Einstellungen, wie z. B. Strom, freigegebene Laufwerke und Uhrinstellungen für Windows Embedded Standard-Geräte.

**Tabelle 105. Konfigurieren des Gerätemodus**

Option	Beschreibung
<b>Gerätemodus</b>	<p>Wählen Sie diese Option zum Einstellen eines geeigneten Modus für das Gerät aus. Die Option „Gerätemodus“ startet die Anwendung in einem Kioskmodus und ohne Zugriff auf den Desktop oder andere Anwendungen. Sie können den Gerätemodus mithilfe der konfigurierten Tasten aufheben. Zum Beispiel: Strg + Umschalttaste + A. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"><li>• Aus</li><li>• Generisch</li><li>• VMware View</li><li>• Citrix</li><li>• Internet Explorer</li><li>• RDP</li></ul>

**Tabelle 106. Konfigurieren der Energieeinstellungen**

Option	Beschreibung
<b>Energieplan des Geräts</b>	<p>Wählen Sie diese Option, um einen Energiesparplan für Ihr Gerät zu wählen. Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>· Ausgeglichen</li> <li>· Energiesparmodus</li> </ul>

**Tabelle 107. Energieeinstellungen im Akkubetrieb konfigurieren**

Option	Beschreibung
<b>Energiesparplan des Geräts</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der das Gerät in den Ruhemodus versetzt wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Bildschirm abdunkeln</b>	Wählen Sie diese Option aus, um die Zeit festzulegen, nach der die Anzeige abgeblendet wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Anzeige ausschalten</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der die Anzeige ausgeschaltet wird. Wählen Sie eine Verzögerungszeit aus der Dropdownliste aus.

**Tabelle 108. Energieeinstellungen beim Anschluss an Stromversorgung konfigurieren**

Option	Beschreibung
<b>Energiesparplan des Geräts</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der das Gerät in den Ruhemodus versetzt wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Bildschirm abdunkeln</b>	Wählen Sie diese Option aus, um die Zeit festzulegen, nach der die Anzeige abgeblendet wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Anzeige ausschalten</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der die Anzeige ausgeschaltet wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.

**Tabelle 109. Konfigurieren freigegebener Geräte**

Option	Beschreibung
<b>Freigegebenes Laufwerk</b>	<p>Wählen Sie diese Option zum Hinzufügen eines freigegebenen Laufwerks an Ihr Gerät. Klicken Sie auf <b>Freigegebenes Gerät hinzufügen</b>. Geben Sie den Freigabennamen, den Pfad des Remote-Laufwerks, den Benutzernamen und das Kennwort für das freigegebene Laufwerk ein.</p> <p><b>!</b> <b>ANMERKUNG:</b> Zum Löschen eines freigegebenen Laufwerks aus der Liste wählen Sie das freigegebene Laufwerk, das Sie entfernen möchten, und klicken Sie auf <b>Entfernen</b>.</p>

**Tabelle 110. Konfigurieren der Uhreinstellungen**

Option	Beschreibung
<b>Uhr1</b>	Wählen Sie diese Option aus, um Uhr 1 Ihres Geräts zu konfigurieren. Nachdem Sie Uhr 1 aktivieren, legen Sie den <b>Anzeigennamen</b> für die Uhr fest. Wählen Sie aus dem Dropdownmenü die <b>Zeitzone</b> für Uhr 1.
<b>Uhr2</b>	Wählen Sie diese Option aus, um Uhr 2 Ihres Geräts zu konfigurieren. Nachdem Sie Uhr 2 aktivieren, legen Sie den <b>Anzeigennamen</b> für die Uhr fest. Wählen Sie aus dem Dropdownmenü die <b>Zeitzone</b> für Uhr 2.

## Konfigurieren von Remote-Verbindungseinstellungen – Citrix

Verwenden Sie diese Seite zum Konfigurieren der Citrix-Verbindungseinstellungen, wie z. B. Anzeige, Serveroptionen und Flash-Umleitung für die Windows Embedded Standard-Geräte.

**Tabelle 111. Grundlegende Optionen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um einen Namen für die Verbindungsidentifikation festzulegen.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option aus, um das automatische Starten der Sitzung nachdem Sie sich angemeldet haben zu aktivieren.
<b>Verbindungstyp</b>	Wählen Sie diese Option aus, um einen Verbindungstyp festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Veröffentlichte Anwendungen (XenApp)</li> <li>· Serververbindung (XenDesktop)</li> <li>· Gateway</li> <li>· Storefront</li> </ul>
<b>Broker-Server</b>	Wählen Sie diese Option aus, um die Citrix-Server aufzulisten. Geben Sie die Liste der ICA-Browser für die Verbindung durch Kommas getrennt ein.
<b>Veröffentlichte Anwendungen</b>	Wählen Sie diese Option zur Angabe einer veröffentlichten Anwendung, die Sie starten möchten.
<b>Single Sign On</b>	Wählen Sie diese Option zur Aktivierung der Funktion "Einmaliges Anmelden" für die Verbindung aus. Wenn Sie die "Einmalige Anmeldung" aktivieren, verwenden Sie Ihre Windows-Anmeldeinformationen für die Verbindung mit dem Citrix-Server. Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.
<b>Benutzername</b>	Wählen Sie diese Option aus, um einen Benutzernamen für die Citrix-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist. Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.

Option	Beschreibung
<b>Kennwort</b>	Wählen Sie diese Option aus, um ein Kennwort für die Citrix-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist. Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.
<b>Domainname</b>	Wählen Sie diese Option aus, um einen Domainnamen für die Citrix-Verbindung zu definieren. Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.
<b>Fenstergröße</b>	Wählen Sie diese Option zur Angabe der Fenstergröße für die Citrix-Verbindung. Wählen Sie aus dem Dropdownmenü die Fenstergröße aus. Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.
<b>Bildschirm-Farbtiefe</b>	<p>Wählen Sie diese Option zum Definieren der Bildschirm-Farbtiefe der Citrix-Verbindung.</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Bessere Geschwindigkeit 16 Bit</li> <li>• Bessere Darstellung 32 Bit</li> </ul> <p>Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.</p>
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, um automatisch die Verbindung wiederherzustellen, wenn die Verbindung abbricht. Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.
<b>Audioqualität</b>	<p>Wählen Sie diese Option, um die Tonqualität für die Citrix-Verbindung zu wählen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Standardaudioeinstellung des Benutzers</li> <li>• High Definition</li> <li>• Für Sprache optimiert</li> <li>• Niedrige Bandbreite</li> <li>• Aus</li> </ul>
<b>Passthrough für Tastenkombinationen des Benutzers</b>	<p>Wählen Sie diese Option, um anzugeben, auf welches Fenster die Tastenkombinationen des Windows-Benutzers angewendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Standard-Passthrough für Tastenkombinationen des Benutzers</li> <li>• Auf dem lokalen Desktop</li> <li>• Auf dem Remotedesktop</li> <li>• Nur auf Vollbild-Desktops</li> </ul> <p>Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Veröffentlichte Anwendungen (XenApp)</b> auswählen.</p>
<b>Speichernamen</b>	Geben Sie den Speichernamen des Citrix Servers oder der StoreFront ein. Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp Serververbindung (XenDesktop)</b> oder <b>StoreFront</b> auswählen.
<b>Authentifizierungsmethoden</b>	Mit dieser Option wird der allgemeine Authentifizierungstyp aktiviert. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:

Option	Beschreibung
	<ul style="list-style-type: none"> <li>· Eingabeaufforderung für Anmeldeinformationen</li> <li>· Authentifizierung von Benutzername und Kennwort</li> <li>· Smartcard-Authentifizierung</li> <li>· Einmaliges Anmelden (Domain-Passthrough-Authentifizierung)</li> </ul> <p>Diese Option wird aktiviert, wenn Sie als <b>Verbindungstyp StoreFront</b> auswählen.</p>

**ANMERKUNG:**

- Nachfolgend sind die Voraussetzungen aufgeführt, unter denen End-to-End-Passthrough-Authentifizierung aktiviert wird, wenn Sie als Authentifizierungsmethode **einmaliges Anmelden** auswählen:
  - Einmaliges Anmelden für den Citrix-Empfänger muss auf dem Gerät aktiviert sein.
  - Das Zielgerät muss der Domäne hinzugefügt werden.
  - Der Domänenbenutzer muss sich am Gerät anmelden.
- Nachfolgend sind die Voraussetzungen aufgeführt, unter denen End-to-End-Passthrough-Authentifizierung aktiviert wird, wenn Sie als Authentifizierungsmethode **Smart-Card-Authentifizierung** auswählen:
  - Einmaliges Anmelden für den Citrix-Empfänger muss auf dem Gerät aktiviert sein.
  - Das Zielgerät muss der Domäne hinzugefügt werden.
  - Der Domänenbenutzer muss sich mit der Smart Card am Gerät anmelden.

Weitere Informationen finden Sie im Artikel *Configure domain pass-through authentication* (Domänen-Passthrough-Authentifizierung konfigurieren) unter [docs.citrix.com](https://docs.citrix.com).

**Tabelle 112. Anwendungsanzeige**

Option	Beschreibung
<b>Desktopanzeige</b>	Wählen Sie diese Option zum Anzeigen der Citrix-Verbindung auf Ihrem Desktop. Wenn Sie diese Option aktivieren, geben Sie den <b>Namen des Desktopordners</b> für die Verbindung ein.
<b>Startmenüanzeige</b>	Wählen Sie diese Option, um die Startmenüanzeige auf dem Verbindungsdesktop zu aktivieren. Nachdem Sie diese Option aktiviert haben, geben Sie den <b>Ordner der Startmenüanzeige</b> für die Verbindung ein.
<b>Taskleistanzeige</b>	Durch Auswahl dieser Option wird die Citrix-Verbindung im Infobereich angezeigt.


**Tabelle 113. Serveroptionen**

Option	Beschreibung
<b>Anmeldemethode</b>	Wählen Sie diese Option zur Auswahl einer Anmeldemethode für Ihre Citrix-Verbindung. <ul style="list-style-type: none"> <li>· Standard-Anmeldemethode</li> <li>· Geforderte Anmeldemethode</li> </ul>

**Tabelle 114. Erweiterte Einstellungen**

Option	Beschreibung
Vollbildschirm-Popup deaktivieren	Wählen Sie diese Option zum Deaktivieren der Vollbildschirm-Pop-up-Warnung.
Anmeldung – Verbindung zu aktiven und getrennten Sitzungen herstellen	Wählen Sie diese Option aus, um nach dem Anmelden eine Verbindung zu den aktiven und getrennten Sitzungen herzustellen.
Menü – Verbindung zu aktiven und getrennten Sitzungen herstellen	Wählen Sie diese Option aus, um eine Verbindung zu aktiven und getrennten Sitzungen herzustellen.
Über Menü erneut verbinden	Wählen Sie diese Option aus, um sich über das Client-Menü erneut mit vorhandenen Sitzungen zu verbinden.

**Tabelle 115. Flash-Umleitung**


Option	Beschreibung
Flash-Remoting verwenden	Wählen Sie diese Option aus, um die Flash-Inhalte auf dem Client-Gerät anstatt auf dem Remote-Server darzustellen.
Serverseitigen Inhaltsabruf aktivieren	Wählen Sie diese Option aus, um Inhalte vom Server herunterzuladen und anschließend an das Benutzergerät zu senden.
Server-HTTP-Cookies verwenden	Wählen Sie diese Option zum Synchronisieren der clientseitigen HTTP-Cookies mit den serverseitigen.
URL-Umschreibungsregeln für clientseitigen Inhaltsabruf	Wählen Sie diese Option aus, um Regeln zum Umleiten von Benutzergeräten an andere Server für den clientseitigen Abruf hinzuzufügen. Klicken Sie auf <b>Element hinzufügen</b> und geben Sie den Namen der Inhaltsregel und den Wert der Inhaltsregel an.   <b>ANMERKUNG: Zum Löschen eines Elements aus der Liste wählen Sie das Element, das Sie entfernen möchten, und klicken Sie auf Entfernen.</b>

## Konfigurieren von Remote-Verbindungseinstellungen – VMware

Verwenden Sie diese Seite zum Konfigurieren der VMware-Verbindungseinstellungen für Windows Embedded Standard-Geräte.

**Tabelle 116. Konfigurieren von Remote-Verbindungen – VMware**

Option	Beschreibung
Verbindungsname	Wählen Sie diese Option aus, um den Namen für die Identifizierung der Verbindung zu definieren.
Verbindung bei Anmeldung automatisch starten	Wählen Sie diese Option aus, um das automatische Starten der Verbindung nachdem Sie sich angemeldet haben zu aktivieren.
VMware Serveradresse	Wählen Sie diese Option zur Eingabe der Serveradresse der VMware-Verbindung.
Protokoll	Wählen Sie diese Option aus, um das Protokoll für die VMware-Verbindung zu wählen. Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:  <ul style="list-style-type: none"> <li>• PCOIP</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>· RDP</li> <li>· Blast</li> </ul>
<b>Als aktueller Benutzer anmelden</b>	Wählen Sie diese Option zur Aktivierung der Funktion "Einmaliges Anmelden" für die Verbindung aus. Wenn Sie die Option <b>Als aktueller Benutzer anmelden</b> aktivieren, verwenden Sie Ihre Windows-Anmeldeinformationen für die Verbindung mit dem VMware-Server.
<b>Benutzername</b>	Wählen Sie diese Option aus, um einen Benutzernamen für die VMware-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Kennwort</b>	Wählen Sie diese Option aus, um ein Kennwort für die VMware-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Domainname</b>	Wählen Sie diese Option aus, um einen Domainnamen für die VMware-Verbindung zu definieren.
<b>Sicherheitsmodus</b>	Wählen Sie diese Option zur Angabe der Client-Konnektivität, wenn Sie keine sichere Verbindung zum Server gewährleisten können.
<b>Vollbildschirm-Modus</b>	Wählen Sie diese Option, um das VMware-Verbindungsfenster im Vollbildschirm-Modus auszuführen. Wenn Sie den Vollbildschirm-Modus nicht auswählen, wählen Sie aus dem Dropdownmenü die <b>Fenstergröße</b> .
<b>Dropdown-Menüleiste für Vollbildschirm anzeigen</b>	Durch Auswahl dieser Option wird das Dropdownmenü <b>Vollbildschirm-Modus</b> für Ihre Verbindung angezeigt.
<b>Diesen Desktop automatisch starten</b>	Wählen Sie diese Option zur Angabe eines veröffentlichten Desktops zum Starten nach dem erfolgreichen Verbindungsaufbau.
<b>Automatisch neu verbinden</b>	<p>Wählen Sie diese Option aus, um sich automatisch wieder zu verbinden, wenn die Verbindung getrennt wird.</p> <p>Wenn die Option <b>Automatisch neu verbinden</b> aktiviert ist, stellt VMware die Verbindung automatisch wieder her, um Anwendungen zu öffnen.</p> <p>Wenn die Option <b>Automatisch neu verbinden</b> deaktiviert ist, werden Sie nicht zur erneuten Verbindung aufgefordert und die Funktion zum automatisch neu Verbinden schlägt fehl.</p> <p> <b>ANMERKUNG: VMware unterstützt die automatische Wiederverbindung nur für die Anwendung</b></p>
<b>Broker</b>	Wählen Sie diese Option aus, um den Hostnamen oder die IP-Adresse des <b>View Connection</b> Brokers zu definieren.
<b>Brokerverlauf</b>	Wählen Sie diese Option aus, um den zuvor verwendeten Hostnamen oder die IP-Adresse des <b>View Connection</b> Brokers zu definieren.

Nachdem die VMware-Konfigurationen angewendet wurden, werden zwei VMware-Verknüpfungssymbole auf dem Desktop des Benutzers angezeigt,

- VMware-Symbol – Standard
- VMware-Symbol mit dem im Wyse Management Suite-Server angegebenen Namen.

Dell empfiehlt, dass Sie nur das VMware-Verknüpfungssymbol mit dem neuen Verbindungsnamen verwenden. Verwenden Sie für Unterstützung der einmaligen Anmeldung auch den VMware Client 4.0 und spätere Versionen.

## Konfigurieren von Remote-Verbindungseinstellungen – RDP

Verwenden Sie diese Seite zum Konfigurieren der RDP-Verbindungseinstellungen, wie z. B. RD-Gateway, Anzeige und lokale Ressourceneinstellungen für die Windows Embedded Standard-Geräte.

**Tabelle 117. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um den Namen für die Identifizierung der Verbindung zu definieren.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option aus, um das automatische Starten der Verbindung nachdem Sie sich angemeldet haben zu aktivieren.
<b>Serveradresse</b>	Wählen Sie diese Option zur Eingabe der Serveradresse der Verbindung.
<b>Single Sign On</b>	Wählen Sie diese Option zur Aktivierung der Funktion "Einmaliges Anmelden" für die Verbindung aus. Wenn Sie die Option <b>Als aktueller Benutzer anmelden</b> aktivieren, verwenden Sie Ihre Windows-Anmeldeinformationen für die Verbindung mit dem Server.
<b>Benutzername</b>	Wählen Sie diese Option aus, um einen Benutzernamen für die Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Kennwort</b>	Wählen Sie diese Option aus, um ein Kennwort für die Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Domainname</b>	Wählen Sie diese Option aus, um einen Domainnamen für die Verbindung zu definieren.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, um das automatische Wiederverbinden zu aktivieren, wenn die Verbindung getrennt wird.

**Tabelle 118. RD-Gateway konfigurieren**

Option	Beschreibung
<b>RD-Gateway-Einstellungen verwenden</b>	<p>Wählen Sie diese Option zum Konfigurieren der Einstellungen für das RD-Gateway. Nachdem Sie die Option aktivieren, geben Sie den <b>RD-Server</b>namen für das Gateway ein.</p> <p>Wählen Sie aus dem Dropdownmenü <b>Anmeldemethode für RD-Gateway</b> die Anmeldeinformationen aus, um die Verbindung mit dem RD Gateway zu validieren:</p> <ul style="list-style-type: none"> <li>• Nach Kennwort für NTLM fragen</li> <li>• Smart Card</li> <li>• Spätere Auswahl zulassen</li> <li>•</li> </ul> <p>Wählen Sie aus dem Dropdownmenü <b>Nutzungsmethode des RD-Gateways</b> eine der folgenden Möglichkeiten zur Nutzung eines Remote-Desktop-Servers:</p> <ul style="list-style-type: none"> <li>• RD-Gateway-Server nicht verwenden – alle IP-Adressen</li> <li>• RD-Gateway-Servereinstellungen verwenden</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>RD-Gateway-Servereinstellungen nur für nicht lokale IP-Adressen verwenden</li> <li>Standardeinstellungen verwenden</li> <li>Nur lokale IP-Adressen</li> </ul>

**Tabelle 119. Konfigurieren der Anzeigeeinstellungen**

Option	Beschreibung
<b>Vollbildschirm-Modus</b>	Wählen Sie diese Option, um das Verbindungsfenster im Vollbildschirm-Modus auszuführen. Nach dem Vollbildschirm-Modus aktiviert ist, wählen Sie aus dem Dropdownmenü die Fenstergröße aus.
<b>Verbindungsleiste anzeigen</b>	Wählen Sie diese Option, um die Verbindungsleiste im Vollbildschirm-Modus anzuzeigen.
<b>Multimonitor-Unterstützung</b>	Wählen Sie diese Option aus, um die Multimonitor-Funktion zu aktivieren.
<b>Bildschirm-Farbtiefe (in Bits)</b>	Wählen Sie diese Option zum Definieren der Bildschirm-Farbtiefe der Verbindung. <ul style="list-style-type: none"> <li>RDP 15 Bit High Color</li> <li>RDP 16 Bit High Color</li> <li>RDP 24 Bit True Color</li> <li>RDP 32 Bit höchste Qualität</li> </ul>

**Tabelle 120. Konfigurieren anderer Einstellungen – Erlebnis**

Option	Beschreibung
<b>Verbindungsgeschwindigkeit zur Optimierung der Leistung</b>	Wählen Sie diese Option aus, um die Verbindungsgeschwindigkeit der Leistung gemäß zu optimieren.
<b>Desktophintergrund</b>	Wählen Sie diese Option für die Aktivierung des Desktophintergrunds für die Verbindung aus.
<b>Visuelle Stile</b>	Wählen Sie diese Option für die Aktivierung der visuellen Stile für die Verbindung aus.
<b>Schriftartglättung</b>	Wählen Sie diese Option für die Aktivierung der Schriftartenglättung für die Verbindung aus.
<b>Persistentes Bitmap-Caching</b>	Wählen Sie diese Option aus, um persistentes Bitmap-Caching für die Verbindung zu aktivieren.
<b>Desktopzusammensetzung</b>	Wählen Sie diese Option für die Aktivierung der Desktopzusammensetzung für die Verbindung aus.
<b>Cursoreinstellung deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der Cursoreinstellung für die Verbindung aus.
<b>Fensterinhalt beim Ziehen anzeigen</b>	Wählen Sie diese Option aus, um den Fensterinhalt beim Verschieben des Fensters anzuzeigen.
<b>Menü- und Fensteranimation</b>	Wählen Sie diese Option aus, um das Menü und die Fensteranimation für die Verbindung zu aktivieren.

Option	Beschreibung
<b>Weiterleitung des Servernamens verwenden</b>	Wählen Sie diese Option aus, um die Verwendung der Weiterleitung des Servernamens zu verwenden.
<b>Wenn Serverauthentifizierung fehlschlägt</b>	Wählen Sie diese Option aus, um die Maßnahme festzulegen, die ergriffen werden soll, wenn die Serverauthentifizierung fehlschlägt. <ul style="list-style-type: none"> <li>• Verbinden ohne Warnmeldung</li> <li>• Nicht verbinden</li> <li>• Warnen</li> </ul>

**Tabelle 121. Lokale Ressourcen konfigurieren**

Option	Beschreibung
<b>Zwischenablage umleiten</b>	Wählen Sie diese Option für die Verwendung der lokalen Zwischenablage des Geräts in der Remoteverbindung aus.
<b>COM-Ports umleiten</b>	Wählen Sie diese Option für die Verwendung des lokalen COM-Ports (seriell) des Geräts in der Remoteverbindung aus.
<b>DirectX umleiten</b>	Wählen Sie diese Option aus, um DirectX auf dem Client-Computer umzuleiten und damit die Option in der Remoteverbindung verfügbar ist.
<b>Laufwerke umleiten</b>	Wählen Sie diese Option für die Verwendung der lokalen Laufwerke des Geräts in der Remoteverbindung aus.
<b>POS-Geräte umleiten</b>	Wählen Sie diese Option aus, um Point-of-Service-Geräte, wie z. B. Barcodeleser und magnetische Leser des Geräts in der Remoteverbindung zu verwenden.
<b>Alle Drucker weiterleiten</b>	Wählen Sie diese Option für die Verwendung des lokalen Druckers des Geräts in der Remoteverbindung.
<b>Smart Card umleiten</b>	Wählen Sie diese Option für die Verwendung der lokalen Smart Cards des Geräts in der Remoteverbindung.
<b>RemoteFX-USB-Geräteumleitung aktivieren</b>	Wählen Sie diese Option zum Aktivieren oder Deaktivieren der RemoteFX-USB-Geräteumleitung.
<b>Umleitung von angeschlossenen USB-Geräten später aktivieren</b>	Wählen Sie diese Option zum Aktivieren oder Deaktivieren der Umleitung der USB-Geräte aus der RDP-Sitzung.
<b>Umleitung anderer unterstützter Plug-and-Play-Geräte aktivieren</b>	Wählen Sie diese Option zum Aktivieren oder Deaktivieren der Umleitung anderer Plug-and-Play-Geräte.

## Konfigurieren von Remote-Verbindungseinstellungen – Browser

Verwenden Sie diese Seite zum Konfigurieren der Browser-Verbindungseinstellungen, wie z. B. IE Proxy und Favoriten, für die Windows Embedded Standard-Geräte.

**Tabelle 122. Grundeinstellungen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um einen Namen für die Identifizierung der Verbindung zu definieren.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option aus, um das automatische Starten der Verbindung nachdem Sie sich angemeldet haben zu aktivieren.
<b>URL</b>	Wählen Sie diese Option zur Angabe der Standard-URL für den Browser aus.
<b>Sicherheitsstufe der Internetzone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer in der Internetzone festzulegen.
<b>Sicherheitsstufe der lokalen Zone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer in der lokalen Zone festzulegen.
<b>Sicherheitsstufe in der vertrauenswürdigen Zone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer auf vertrauenswürdigen Sites festzulegen.
<b>Sicherheitsstufe in der eingeschränkten Zone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer auf eingeschränkten Sites festzulegen.

**Tabelle 123. Einstellungen für IE-Favoriten (Internet Explorer) und vertrauenswürdige Sites**

Option	Beschreibung
<b>IE-Favoriten</b>	<p>Wählen Sie diese Option zum Hinzufügen Ihres Favoriten und vertrauenswürdigen Sites. Führen Sie folgende Schritte durch, um Ihre Favoriten und vertrauenswürdigen Sites hinzuzufügen:</p> <ol style="list-style-type: none"> <li>1 Klicken Sie auf <b>Site hinzufügen</b> und geben Sie den Namen des Ordners, die URL und eine Beschreibung ein.</li> <li>2 Klicken Sie auf <b>Verknüpfung erstellen</b>, um eine Verknüpfung für die Site zu erstellen.</li> <li>3 Klicken Sie auf <b>Entfernen</b> zum Löschen einer Site aus der Liste.</li> </ol> <p><b>ANMERKUNG:</b>            URL muss mit https:// beginnen, wenn das Kontrollkästchen <b>Vertrauenswürdige Sites</b> ausgewählt wurde.</p>
<b>Serverüberprüfung (https:) für alle Sites der Zone erforderlich machen</b>	Wählen Sie diese Option zum Aktivieren einer Serverüberprüfung für alle Sites in der Zone aus.

**Tabelle 124. Internet Explorer – IE-Proxy-Einstellungen**

Option	Beschreibung
<b>Proxy aktivieren</b>	Wählen Sie diese Option aus, um den Proxy für den Browser zu konfigurieren.

**Tabelle 125. Firewall**

Option	Beschreibung
<b>Domain-Firewall</b>	Wählen Sie diese Option aus, um die Domain-Firewall zu aktivieren.
<b>Private Firewall</b>	Wählen Sie diese Option aus, um die Private Firewall zu aktivieren.

Option	Beschreibung
<b>Öffentliche Firewall</b>	Wählen Sie diese Option aus, um die Öffentliche Firewall zu aktivieren.

**Tabelle 126. Aero – gültig für Windows Embedded Standard 7**

Option	Beschreibung
<b>Aero</b>	<p>Wählen Sie diese Option für die Aktivierung der Funktion "Aero" für den Browser.</p> <p><b>ANMERKUNG:</b> Diese Funktion steht nur auf Windows Embedded Standard 7 zur Verfügung.</p>

## Konfigurieren der BIOS-Einstellungen für mobilen Latitude Thin Client

Verwenden Sie diese Seite zum Definieren der BIOS-Einstellungen für mobile Latitude Thin Clients.

**Tabelle 127. Systemkonfiguration**

Option	Beschreibung
<b>Serielle Schnittstelle 1</b>	<p>Markieren Sie dieses Kontrollkästchen, um festzulegen, wie die serielle Schnittstelle an der Docking-Station funktioniert. Diese Option ermöglicht es Ihnen, Ressourcenkonflikte zwischen Geräten zu verhindern, indem Sie die Adresse des Ports deaktivieren oder neu zuordnen.</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> Port ist deaktiviert.</li> <li>• <b>COM1</b> – Der Port wird für die Adresse 3F8h mit IRQ 4 konfiguriert.</li> <li>• <b>COM2</b> – Der Port wird für die Adresse 2F8h mit IRQ 3 konfiguriert.</li> <li>• <b>COM3</b> – Der Port wird für die Adresse 3F8h mit IRQ 4 konfiguriert.</li> <li>• <b>COM4</b> – Der Port wird für die Adresse 2F8h mit IRQ 3 konfiguriert.</li> </ul>
<b>Tongerät</b>	Markieren Sie dieses Kontrollkästchen, um das Tongerät zu aktivieren.
<b>Mikrofon</b>	Markieren Sie dieses Kontrollkästchen, um das Mikrofon zu aktivieren.
<b>Lautsprecher</b>	Markieren Sie dieses Kontrollkästchen, um den Lautsprecher zu aktivieren.

**Tabelle 128. USB-Konfiguration**

Option	Beschreibung
<b>Externe USB-Anschlüsse</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät an diesem Port aktiviert wird. Das Gerät wird auch für das Betriebssystem verfügbar gemacht. Wenn ein USB-Anschluss deaktiviert ist, kann das System kein dort angeschlossenes Gerät erkennen.

**Tabelle 129. WLAN-Einstellungen konfigurieren**

Option	Beschreibung
EnableBluetooth	Markieren Sie dieses Kontrollkästchen, um Bluetooth zu aktivieren.
WLAN/GPS	Markieren Sie dieses Kontrollkästchen, um WLAN/GPS zu aktivieren.
Wireless LAN	Markieren Sie dieses Kontrollkästchen, um Wireless LAN zu aktivieren.

**Tabelle 130. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
Setupsperre durch Administrator	Markieren Sie dieses Kontrollkästchen, um zu verhindern, dass Benutzer auf das <b>Setup</b> zugreifen, wenn das Administratorkennwort festgelegt wurde.

**Tabelle 131. Administratorkennworteinstellungen**

Option	Beschreibung
Administratorkennwort aktivieren	Wählen Sie dieses Kontrollkästchen aus, um das BIOS-Administratorkennwort zu aktivieren. Erfolgreiche Änderungen an diesem Kennwort werden sofort wirksam.
Administratorkennwort	Geben Sie das neue BIOS-Administratorkennwort ein. Diese Option ist nur verfügbar, wenn Sie das Kontrollkästchen <b>Administratorkennwort aktivieren</b> auswählen.

**Tabelle 132. Konfigurieren der Energieverwaltungseinstellungen**

Option	Beschreibung
Wake On LAN	Aktivieren Sie diese Option, um das Gerät über die Wyse Management Suite-Konsole einzuschalten. Um diese Maßnahme durchzuführen, führen Sie den Befehl "Wake-on-LAN (WOL)" auf der Seite <b>Geräte</b> aus.
Bei Netzanschluss reaktivieren	Aktivieren Sie diese Option, um das Gerät nach Wiederherstellung der Stromversorgung (nach einem Stromausfall) automatisch zu starten.

**Tabelle 133. Konfigurieren der Einstellungen für das automatische Einschalten**

Option	Beschreibung
Automatische Einschaltung	Wählen Sie aus der Dropdownliste die Tageszeit aus, zu der das System automatisch eingeschaltet werden soll.

**Tabelle 134. Neustart-Zeitplan konfigurieren**

Option	Beschreibung
Neustartoption	Einige BIOS-Einstellungen machen einen Systemneustart erforderlich. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Sofort neu starten: Das System startet sofort neu.</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>• Später neu starten: Wählen Sie <b>Neustart-Stunde</b> und <b>Neustart-Minute</b> aus, um den Zeitpunkt für den Systemneustart festzulegen,</li> <li>• Keinen Neustart durchführen: Das System wird nicht neu gestartet.</li> </ul>

## Wyse 7040 Thin Client BIOS-Einstellungen konfigurieren

Verwenden Sie diese Seite, um die BIOS-Einstellungen für Wyse 7040 Thin Clients zu konfigurieren.

**Tabelle 135. Systemkonfiguration**

Option	Beschreibung
<b>Tongerät</b>	Markieren Sie dieses Kontrollkästchen, um das Tongerät zu aktivieren.
<b>Mikrofon</b>	Markieren Sie dieses Kontrollkästchen, um das Mikrofon zu aktivieren.
<b>Lautsprecher</b>	Markieren Sie dieses Kontrollkästchen, um den Lautsprecher zu aktivieren.

**Tabelle 136. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
<b>Setupsperre durch Administrator</b>	Markieren Sie dieses Kontrollkästchen, um zu verhindern, dass Benutzer auf das <b>Setup</b> zugreifen, wenn das Administratorkennwort festgelegt wurde.

**Tabelle 137. Konfigurieren der Administratorkennworteinstellungen**

Option	Beschreibung
<b>Administratorkennwort aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, um das BIOS-Administratorkennwort zu aktivieren. Erfolgreiche Änderungen an diesem Kennwort werden sofort wirksam.
<b>Administratorkennwort</b>	Geben Sie das neue BIOS-Administratorkennwort ein. Diese Option ist nur verfügbar, wenn Sie das Kontrollkästchen <b>Administratorkennwort aktivieren</b> auswählen.

**Tabelle 138. Konfigurieren der Einstellungen für das automatische Einschalten**

Option	Beschreibung
<b>Automatische Einschaltung</b>	Wählen Sie aus der Dropdownliste die Tageszeit aus, zu der das System automatisch eingeschaltet werden soll

**Tabelle 139. Neustart-Zeitplan konfigurieren**

Option	Beschreibung
<b>Neustartoption</b>	Einige BIOS-Einstellungen machen einen Systemneustart erforderlich. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:

Option	Beschreibung
	<ul style="list-style-type: none"> <li>• Sofort neu starten: Das System startet sofort neu.</li> <li>• Später neu starten: Wählen Sie <b>Neustart-Stunde</b> und <b>Neustart-Minute</b> aus, um den Zeitpunkt für den Systemneustart festzulegen,</li> <li>• Keinen Neustart durchführen: Das System wird nicht neu gestartet.</li> </ul>

**Tabelle 140. USB-Konfiguration**

Option	Beschreibung
<b>Vordere USB-Anschlüsse aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät an diesem Port aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, wird das Gerät auch für das Betriebssystem verfügbar gemacht. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System kein dort angeschlossenes Gerät erkennen.
<b>Hintere USB-Anschlüsse aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät an diesem Port aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, wird das Gerät auch für das Betriebssystem verfügbar gemacht. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System kein dort angeschlossenes Gerät erkennen.

**Tabelle 141. Konfigurieren der Energieverwaltungseinstellungen**

Option	Beschreibung
<b>Bei Netzanschluss reaktivieren</b>	Wählen Sie aus der Dropdownliste eine Option aus, um anzugeben, wie das System reagieren muss, wenn der Netzstrom nach einem Stromausfall wiederhergestellt wurde. Dies sind die möglichen Optionen: <ul style="list-style-type: none"> <li>• Aus</li> <li>• Zuletzt</li> <li>• Ein</li> </ul>
<b>Wake On LAN</b>	Wählen Sie aus der Dropdownliste eine Option aus, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird. Sie können einen Thin Client dazu bringen, aus dem ausgeschalteten Zustand über ein LAN-Signal oder ein Wireless-LAN-Signal hochgefahren zu werden.

## Geräteinformationen konfigurieren

Verwenden Sie die Seite **Geräteinformationen**, um die Gerätedetails anzuzeigen.

**Tabelle 142. Geräteinformationen konfigurieren**

Option	Beschreibung
<b>Standort</b>	Geben Sie den Gerätestandort ein.
<b>Kontakt</b>	Geben Sie die Kontaktdaten des Geräts ein.
<b>Benutzerdefiniert 1 bis 3</b>	Geben Sie benutzerdefinierte Werte ein.

# Konfigurieren von Wyse Easy Setup-Einstellungen

Die Seite **Wyse Easy Setup** dient zur Konfiguration der Wyse Easy Setup-Einstellungen für die Systemsteuerung und die Benutzeroberfläche.

**Tabelle 143. System konfigurieren**

Option	Beschreibung
<b>Region &amp; Sprache</b>	Ermöglicht Ihnen den Zugriff auf die Optionen zu Region und Sprache in der Systemsteuerung.
<b>Datum &amp; Uhrzeit</b>	Ermöglicht Ihnen den Zugriff auf die Optionen zu Datum und Uhrzeit in der Systemsteuerung.
<b>Anzeige</b>	Ermöglicht Ihnen den Zugriff auf die Anzeigeeoptionen in der Systemsteuerung.
<b>Netzwerk</b>	Ermöglicht Ihnen den Zugriff auf die Netzwerkooptionen in der Systemsteuerung des lokalen Systems.
<b>Erleichterter Zugriff</b>	Ermöglicht Ihnen den Zugriff auf die Optionen für einen leichten Zugriff in der Systemsteuerung.
<b>Ton</b>	Ermöglicht Ihnen den Zugriff auf die Tonooptionen in der Systemsteuerung.

**Tabelle 144. Konfigurieren von Peripheriegeräten**

Option	Beschreibung
<b>Maus</b>	Ermöglicht Ihnen den Zugriff auf die Mausoptionen in der Systemsteuerung.
<b>Tastatur</b>	Ermöglicht Ihnen den Zugriff auf die Tastaturoptionen in der Systemsteuerung.

**Tabelle 145. Konfigurieren des Kioskmodus**

Option	Beschreibung
<b>Kioskmodus</b>	Wählen Sie diese Option, um den standardmäßigen Windows Desktop durch den Wyse Easy Setup Desktop, Wyse Easy Setup Remote-Verbindungen und Wyse Easy Setup Anwendungen zu ersetzen.
<b>Anwendungen</b>	Geben Sie die Einzelheiten zum Registrieren einer neuen Anwendung ein.
<b>Aktion beim Beenden der Anwendung</b>	Wählen Sie aus der Dropdownliste Aktion beim Beenden der Anwendung eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"><li>• Herunterfahren beim Beenden</li><li>• Neu starten beim Beenden</li><li>• Logout beim Beenden</li><li>• Persistent beim Beenden</li></ul>

Option	Beschreibung
	Diese Einstellung gilt, wenn Sie mindestens eine der Remote-Verbindungen konfiguriert haben.
<b>Anwendungszustand – Wiederholungsversuche</b>	Geben Sie in der Wyse Easy Setup-Shell an, wie oft versucht werden soll, die Anwendung zu öffnen.
<b>Anwendungszustand – Wiederholungsintervall</b>	Geben Sie das Zeitintervall für zwei aufeinanderfolgende Versuche zum Öffnen der Anwendung in der Wyse Easy Setup-Shell an.

**Tabelle 146. Personalisierung**

Option	Beschreibung
<b>Hintergrund</b>	Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Grafik. Das Bild sollte in das Datei-Repository hochgeladen und als Hintergrundbild angezeigt werden.
<b>Logo</b>	Wählen Sie aus der Dropdownliste die Logo Dateien aus, die in <b>Apps &amp; Daten &gt; Datei-Repository &gt; Bestand</b> hochgeladen werden.

**Tabelle 147. Konfigurieren der Taskleiste**

Option	Beschreibung
<b>Datum &amp; Uhrzeit</b>	Ermöglicht dem Benutzer die Einstellung der Option für Datum und Uhrzeit auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
<b>Ton</b>	Ermöglicht dem Benutzer die Einstellung von Tonparametern auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
<b>Netzwerk</b>	Ermöglicht dem Benutzer die Ansicht von Netzwerkoptionen auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
<b>Bildschirmtastatur</b>	Ermöglicht dem Benutzer die Ansicht der Bildschirmtastatur auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
<b>Taskleistenmenü anzeigen</b>	Ermöglicht den Zugriff auf das <b>Taskleisten</b> -Menü in der Wyse Easy Setup-Benutzeroberfläche.

**Tabelle 148. Startmenü konfigurieren**

Option	Beschreibung
<b>Abschaltung zulassen</b>	Ermöglicht dem Benutzer das Herunterfahren des Systems auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
<b>Neustart zulassen</b>	Ermöglicht dem Benutzer den Systemneustart auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
<b>Abmeldung zulassen</b>	Ermöglicht dem Benutzer die Systemabmeldung auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
<b>Startmenü anzeigen</b>	Ermöglicht den Zugriff auf das <b>Startmenü</b> in der Wyse Easy Setup-Benutzeroberfläche.
<b>Hilfe aktivieren</b>	Ermöglicht den Zugriff auf die <b>Hilfe</b> -Option in der Wyse Easy Setup-Benutzeroberfläche.

# Konfigurieren der VNC-Einstellungen

Verwenden Sie diese Seite zum Konfigurieren der VNC-Einstellungen.

**Tabelle 149. Konfigurieren von VNC**

Option	Beschreibung
VNC aktivieren	Wählen Sie diese Option aus, um den VNC-Server zu aktivieren.
VNC-Benutzeraufforderung	Wenn Sie diese Option auswählen, müssen Sie VNC-Shadowing annehmen oder ablehnen.
Erforderliches Kennwort für VNC-Benutzer	Wählen Sie diese Option aus, um das VNC-Kennwort festzulegen.
Primäres VNC-Kennwort	Wählen Sie diese Option aus, um das VNC-Kennwort zu ändern. Geben Sie das neue Kennwort mit bis zu acht Zeichen ein.
VNC-Kennwort für Modus "Nur anzeigen"	Ermöglicht die Arbeit im schreibgeschützten Modus bei der Anmeldung unter Verwendung dieses Kennworts.

# Konfigurieren von Domäneneinstellungen

Lesen Sie die Anweisungen auf dem Bildschirm, um ein IoT Enterprise-Gerät mit Windows Embedded Standard 7, Windows Embedded 8 Standard oder Windows 10 zur Active Directory-Domäne des Unternehmens hinzuzufügen.

**Tabelle 150. Konfigurieren von Domäneneinstellungen**

Option	Beschreibung
Domäne oder Arbeitsgruppe	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
Name der Domäne oder Arbeitsgruppe	Geben Sie den FQDN der Domain an.
Benutzername	Geben Sie den Benutzernamen ein. Das Konto sollte über die Option <b>Zu Domain hinzufügen</b> verfügen.
Kennwort	Geben Sie das Kennwort ein.
Konto-OE	Geben Sie den Speicherort der Organisationseinheit ein, an dem das Computerobjekt erstellt werden soll.
Automatische Anmeldung	Aktivieren Sie das Kontrollkästchen zur Anzeige des Windows-Anmeldebildschirms.

# Konfiguration der BIOS-Einstellungen für Wyse 5070 Thin-Client mit Windows 10 IoT Enterprise


Verwenden der Seite für die BIOS-Einstellungen, um die BIOS-Einstellungen für den Wyse 5070 Thin Client und den Wyse 5070 Extended Thin Client mit Windows 10-IoT Enterprise zu konfigurieren.

**Tabelle 151. Systemkonfiguration**

Option	Beschreibung
<b>Audio aktivieren</b>	Markieren Sie dieses Kontrollkästchen, um das Audiogerät zu aktivieren.
<b>Mikrofon aktivieren</b>	Markieren Sie dieses Kontrollkästchen, um das Mikrofon zu aktivieren.
<b>Enable Internal Speaker (Internen Lautsprecher aktivieren)</b>	Markieren Sie dieses Kontrollkästchen, um den internen Lautsprecher zu aktivieren.
<b>Paralleler Port</b>	<p>Wählen Sie aus der Dropdownliste die Option aus, mit der bestimmt wird, wie die parallele Schnittstelle an der Docking-Station funktioniert.</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> Port ist deaktiviert.</li> <li>• <b>AT:</b> Port ist für IBM AT-Kompatibilität konfiguriert.</li> <li>• <b>PS2:</b> Port ist für IBM PS2-Kompatibilität konfiguriert.</li> <li>• <b>ECP:</b> Port ist für das ECP-Protokoll (Extended Capability Port) konfiguriert.</li> </ul> <p><b>ANMERKUNG:</b> Diese Option steht für den Wyse 5070 Extended Thin Client zur Verfügung, wenn die Add-on-Karte installiert ist.</p>
<b>Serielle Schnittstelle 1</b>	<p>Wählen Sie aus der Dropdownliste die Option aus, mit der man ermittelt, wie die serielle Schnittstelle an der Docking-Station funktioniert. Diese Option ermöglicht es Ihnen, Ressourcenkonflikte zwischen Geräten zu verhindern, indem Sie die Adresse des Ports deaktivieren oder neu zuordnen.</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> Port ist deaktiviert.</li> <li>• <b>COM1</b> – Der Port wird für die Adresse 3F8h mit IRQ 4 konfiguriert.</li> <li>• <b>COM2</b> – Der Port wird für die Adresse 2F8h mit IRQ 3 konfiguriert.</li> <li>• <b>COM3</b> – Der Port wird für die Adresse 3F8h mit IRQ 4 konfiguriert.</li> <li>• <b>COM4</b> – Der Port wird für die Adresse 2F8h mit IRQ 3 konfiguriert.</li> </ul>

**Tabelle 152. USB-Konfiguration**

Option	Beschreibung
<b>Vordere USB-Anschlüsse aktivieren</b>	<p>Wählen Sie dieses Kontrollkästchen aus, damit das Betriebssystem die am vorderseitigen USB-Anschluss angeschlossenen Geräte erkennen kann. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System das am vorderseitigen USB-Anschluss angeschlossene Gerät nicht erkennen.</p> <p><b>ANMERKUNG:</b> Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</p>
<b>Vorderer Anschluss oben</b>	Wählen Sie diese Option, um den oberen USB-Anschluss an der Vorderseite des Thin Client zu aktivieren.
<b>Vorderer Anschluss oben Mitte</b>	Wählen Sie diese Option, um den oberen mittigen USB-Anschluss an der Vorderseite des Thin Client zu aktivieren.
<b>Vorderer Anschluss unten Mitte</b>	Wählen Sie diese Option, um den unteren mittigen USB-Anschluss an der Vorderseite des Thin Client zu aktivieren.

Option	Beschreibung
<b>Vorderer Anschluss unten</b>	Wählen Sie diese Option, um den unteren USB-Anschluss an der Vorderseite des Thin Client zu aktivieren.
<b>Hintere USB-Anschlüsse aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Betriebssystem die am rückseitigen USB-Anschluss angeschlossenen Geräte erkennen kann. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System das am rückseitigen USB-Anschluss angeschlossene Gerät nicht erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>
<b>Rückseitiger Anschluss oben links</b>	Wählen Sie diese Option, um den USB-Anschluss oben links an der Vorderseite des Thin Client zu aktivieren.
<b>Rückseitiger Anschluss oben rechts</b>	Wählen Sie diese Option, um den USB-Anschluss oben rechts an der Vorderseite des Thin Client zu aktivieren.
<b>Rückseitiger Anschluss unten links</b>	Wählen Sie diese Option, um den USB-Anschluss unten links an der Vorderseite des Thin Client zu aktivieren.
<b>Rückseitiger Anschluss unten rechts</b>	Wählen Sie diese Option, um den USB-Anschluss unten rechts an der Vorderseite des Thin Client zu aktivieren.

**Tabelle 153. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
<b>Sperre für Administrator-Setup aktivieren</b>	Wählen Sie diese Option, um Benutzer vom Aufrufen des Setups abzuhalten, wenn ein Administratorenkennwort festgelegt worden ist.

**Tabelle 154. Konfigurieren der Energieverwaltungseinstellungen**

Option	Beschreibung
<b>Wake On LAN</b>	Wählen Sie aus der Dropdownliste eine Option aus, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird. Sie können einen Thin Client dazu bringen, aus dem ausgeschalteten Zustand über ein LAN-Signal hochgefahren zu werden.
<b>AC-Wiederherstellung</b>	Wählen Sie aus der Dropdownliste eine Option aus, um anzugeben, wie das System funktioniert, wenn der Netzstrom wiederhergestellt wurde.

**Tabelle 155. WLAN-Einstellungen konfigurieren**

Option	Beschreibung
<b>WLAN/WiGig</b>	Wählen Sie dieses Kontrollkästchen zum Aktivieren der internen Wireless-Geräte.
<b>Bluetooth</b>	Markieren Sie dieses Kontrollkästchen, um Bluetooth-Geräte zu aktivieren.

**Tabelle 156. Konfigurieren der Einstellungen für das automatische Einschalten**

Option	Beschreibung
<b>Auto On Time (Automatisch pünktlich)</b>	Wählen Sie aus der Dropdownliste die Tageszeit aus, zu der das System automatisch eingeschaltet werden soll.

**Tabelle 157. Neustart-Zeitplaneinstellungen**

Option	Beschreibung
<b>Neustartoption</b>	<p>Einige BIOS-Einstellungen machen einen Systemneustart erforderlich. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Sofort neu starten: Das System startet sofort neu.</li> <li>• Später neu starten: Wählen Sie <b>Neustart-Stunde</b> und <b>Neustart-Minute</b> aus, um den Zeitpunkt für den Systemneustart festzulegen,</li> <li>• Keinen Neustart durchführen: Das System wird nicht neu gestartet.</li> </ul>

## Konfiguration der BIOS-Einstellungen für Wyse 5470 All-in-One Thin-Client mit Windows 10 IoT Enterprise

Verwenden der Seite für die BIOS-Einstellungen, um die BIOS-Einstellungen für den Wyse 5470 All-in-One Thin Client mit Windows 10-IoT Enterprise zu konfigurieren.


**Tabelle 158. Systemkonfiguration**

Option	Beschreibung
<b>Audio aktivieren</b>	Markieren Sie dieses Kontrollkästchen, um das Audiogerät zu aktivieren.
<b>Mikrofon aktivieren</b>	Markieren Sie dieses Kontrollkästchen, um das Mikrofon zu aktivieren.
<b>Internen Lautsprecher aktivieren</b>	Markieren Sie dieses Kontrollkästchen, um den internen Lautsprecher zu aktivieren.
<b>Schaltflächen auf dem Bildschirm</b>	Markieren Sie dieses Kontrollkästchen, um die Schaltflächen auf Bildschirm zu aktivieren.
<b>SATA-0</b>	Markieren Sie dieses Kontrollkästchen, um SATA-0 zu aktivieren.
<b>Integriertes NIC</b>	<p>Wählen Sie aus der Drop-Down-Liste die Option aus, um den integrierten LAN-Controller zu steuern. Die verfügbaren Optionen sind:</p> <ul style="list-style-type: none"> <li>• Deaktiviert: Das interne LAN ist deaktiviert und für das Betriebssystem nicht sichtbar, wenn es keine IP-Adresse besitzt.</li> <li>• Aktiviert: Das interne LAN ist aktiviert.</li> <li>• Mit PXE aktiviert – Das interne LAN ist aktiviert mit PXE-Start.</li> </ul>

**Tabelle 159. Video**

Option	Beschreibung
<b>Primärer Videogerätschlitz</b>	Wählen Sie aus der Drop-Down-Liste Ihren primären Videogerätschlitz aus.

**Tabelle 160. USB-Konfiguration**

Option	Beschreibung
<b>Hintere USB-Anschlüsse aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Betriebssystem die am rückseitigen USB-Anschluss angeschlossenen Geräte erkennen kann. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System das am rückseitigen USB-Anschluss angeschlossene Gerät nicht erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>
<b>Rückseitiger Anschluss oben links</b>	Wählen Sie diese Option, um den USB-Anschluss oben links an der Rückseite des Thin Client zu aktivieren.
<b>Rückseitiger Anschluss oben rechts</b>	Wählen Sie diese Option, um den USB-Anschluss oben rechts an der Rückseite des Thin Client zu aktivieren.
<b>Rückseitiger Anschluss unten links</b>	Wählen Sie diese Option, um den USB-Anschluss unten links an der Vorderseite des Thin Client zu aktivieren.
<b>Rückseitiger Anschluss unten rechts</b>	Wählen Sie diese Option, um den USB-Anschluss unten rechts an der Vorderseite des Thin Client zu aktivieren.

**Tabelle 161. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
<b>Sperre für Administrator-Setup aktivieren</b>	Wählen Sie diese Option, um Benutzer vom Aufrufen des Setups abzuhalten, wenn ein Administratorenkennwort festgelegt worden ist.

**Tabelle 162. Konfigurieren der Energieverwaltungseinstellungen**

Option	Beschreibung
<b>Wake On LAN</b>	Wählen Sie aus der Dropdownliste eine Option aus, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird. Sie können einen Thin Client dazu bringen, aus dem ausgeschalteten Zustand über ein LAN-Signal hochgefahren zu werden.
<b>AC-Wiederherstellung</b>	Wählen Sie aus der Dropdownliste eine Option aus, um anzugeben, wie das System funktioniert, wenn der Netzstrom wiederhergestellt wurde.

**Tabelle 163. WLAN-Einstellungen konfigurieren**

Option	Beschreibung
<b>WLAN/BT</b>	Wählen Sie dieses Kontrollkästchen zum Aktivieren der internen Wireless-Geräte.

**Tabelle 164. Konfigurieren von Einstellungen der POST-Funktionsweise**

Option	Beschreibung
<b>Numlock-LED</b>	Aktivieren Sie dieses Kontrollkästchen, um die Num-Taste beim Starten des Systems zu aktivieren.
<b>Tastaturfehler</b>	Wählen Sie das Kontrollkästchen, um mit der Tastatur zusammenhängende Fehler beim Starten des Systems anzuzeigen.
<b>Schnellstart</b>	Aktivieren Sie dieses Kontrollkästchen, um den Startvorgang durch das Auslassen einiger Kompatibilitätsschritte zu beschleunigen.
<b>BIOS-POST-Zeit verlängern</b>	Aktivieren Sie dieses Kontrollkästchen, um eine zusätzliche Verzögerung vor dem Neustart zu erstellen, mit der Sie Post-Statusmeldungen anzeigen können.
<b>Aktivieren des Vollbildschirm-Logos</b>	Markieren Sie dieses Kontrollkästchen, um das Vollbildlogo zu aktivieren.

**Tabelle 165. BIOS-Administratorkennwort konfigurieren**

Option	Beschreibung
<b>Administratorkennwort</b>	Wählen Sie dieses Kontrollkästchen aus, um das Administratorkennwort festzulegen.

**Tabelle 166. Konfigurieren der Einstellungen für das automatische Einschalten**

Option	Beschreibung
<b>Zeitpunkt des automatischen Einschaltens</b>	Wählen Sie aus der Dropdownliste die Tageszeit aus, zu der das System automatisch eingeschaltet werden soll.

**Tabelle 167. Neustart-Zeitplaneinstellungen**

Option	Beschreibung
<b>Neustartoption</b>	<p>Einige BIOS-Einstellungen machen einen Systemneustart erforderlich. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Sofort neu starten: Das System startet sofort neu.</li> <li>• Später neu starten: Wählen Sie <b>Neustart-Stunde</b> und <b>Neustart-Minute</b> aus, um den Zeitpunkt für den Systemneustart festzulegen,</li> <li>• Keinen Neustart durchführen: Das System wird nicht neu gestartet.</li> </ul>

## Bearbeiten der Einstellungen für die Linux-Richtlinie

Gehen Sie folgendermaßen vor, um die Linux-Richtlinieneinstellungen zu bearbeiten:

- 1 Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
- 2 Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
- 3 Klicken Sie auf **Linux**.  
Die Seite **Linux** wird angezeigt. Die Linux-Thin Client-Richtlinieneinstellungen umfassen die folgenden Optionen:
  - Systempersonalisierung

- Desktoperlebnis
- Anmeldeerlebnis
- Netzwerk
- Sicherheit
- Zentrale Konfiguration
- Andere Einstellungen
- Globale VDI-Einstellungen
- Citrix Remoteverbindung
- VMware Remoteverbindung
- RDP Remote-Verbindungen
- Browser-Remote-Verbindungen
- Erweitert

4 Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Konfigurieren der Systempersonalisierung

Verwenden Sie die Seite **Systempersonalisierung** zum Konfigurieren der Systempersonalisierung.

**Tabelle 168. Konfigurieren der Systempersonalisierung**

Option	Beschreibung
<b>Monitorauflösung (primär)</b>	Wählen Sie diese Option aus, um die Monitorauflösung festzulegen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Monitorauflösung.
<b>Monitordrehung</b>	Wählen Sie diese Option aus, um die Orientierung des Monitors zu definieren. Wählen Sie aus der Dropdownliste entweder <b>Vertikal</b> oder <b>Horizontal</b> nach Ihren Wünschen.
<b>Dualmonitor aktivieren</b>	Wählen Sie diese Option aus, um die Dualmonitor-Funktion zu aktivieren. Wenn Sie dieses Kontrollkästchen auswählen, werden die folgenden Optionen angezeigt: <ul style="list-style-type: none"> <li>• Spiegelungsmodus – Die Anzeige wird gespiegelt.</li> <li>• Span-Modus – Die Anzeige wird auf beide Monitore erweitert. Wählen Sie aus der Dropdownliste eine der Optionen aus: <ul style="list-style-type: none"> <li>– Nach links</li> <li>– Nach rechts</li> <li>– Unten</li> <li>– Oben</li> </ul> </li> </ul>
<b>Layout</b>	Wählen Sie diese Option, um das Tastaturlayout des Thin Client festzulegen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>Systemsprache</b>	Wählen Sie diese Option zum Einstellen der Sprache für das System aus. Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
<b>Mausgeschwindigkeit</b>	Wählen Sie diese Option aus, um die Geschwindigkeit des Mauszeigers beim Bewegen der Maus anzugeben. Der Bereich der Mausgeschwindigkeit beträgt 0 bis 6.
<b>Linkshänder-Maus</b>	Wählen Sie diese Option aus, um die Mousausrichtung auf die linke Position einzustellen. Wenn dieses Kontrollkästchen nicht markiert ist, ist die Mousausrichtung auf die rechte Position eingestellt.

Option	Beschreibung
<b>Zeitzone</b>	Wählen Sie diese Option zum Einstellen der Zeitzone basierend auf Ihrem Standort. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Zeitzone.
<b>Zeitformat</b>	Wählen Sie diese Option aus, um das Zeitformat auszuwählen. Wählen Sie aus dem Dropdownmenü entweder das 12- oder 24-Stunden-Format.
<b>Zeitserver (NTP-Server)</b>	Wählen Sie diese Option aus, um die Zeitserver aufzulisten. Zeitserver ermöglichen es dem NTP-Server, die Zeit zu synchronisieren.
<b>Audiolautstärke</b>	Wählen Sie diese Option, um die Audiolautstärke des Thin Client festzulegen. Der Bereich der Audiolautstärke liegt zwischen 0 und 100.
<b>Audio stumm schalten</b>	Wählen Sie diese Option, um den Thin Client stummzuschalten.
<b>Mikrofonlautstärke</b>	Wählen Sie diese Option, um die Mikrofonlautstärke des Thin Client festzulegen. Der Bereich der Mikrofonlautstärke liegt zwischen 0 und 100.
<b>Mikrofon stumm schalten</b>	Wählen Sie diese Option aus, um das Mikrofon stummzuschalten.

## Desktop-Erfahrung konfigurieren

Verwenden Sie die Seite **Desktopterlebnis** zum Konfigurieren der Desktop-Einstellungen, wie z. B. Desktop-Hintergrundbild, Hintergrundbild-Layout und Desktop-Tastaturbefehle.

**Tabelle 169. Desktop-Erfahrung konfigurieren**

Option	Beschreibung
<b>Desktophintergrund</b>	Wählen Sie diese Option, um das Standard-Hintergrundbild zu ändern.
<b>Hintergrundbild-Datei</b>	Wählen Sie diese Option, um Ihr bevorzugtes Hintergrundbild auszuwählen. In das Datei-Repository hochgeladene Bilder werden angezeigt.
<b>Hintergrundbild-Layout</b>	Wählen Sie diese Option, um das Hintergrundbild-Layout einzustellen. Wählen Sie aus der Dropdown-Liste Ihr bevorzugtes Hintergrundbild-Layout. Das standardmäßige Hintergrundbild-Layout ist <b>zentriert</b> .
<b>Tastenkombinationen</b>	Wählen Sie diese Option zum Deaktivieren der Tastenkombinationen für die folgenden Aktionen: <ul style="list-style-type: none"> <li>• Aktuell aktives Fenster schließen</li> <li>• Aktuell aktives Fenster minimieren</li> <li>• Aktuell aktives Fenster maximieren/Maximierung des aktuell aktiven Fensters aufheben</li> <li>• Maximierung des aktuell aktiven Fensters aufheben</li> <li>• Größe des aktuell aktiven Fensters ändern</li> <li>• Aktuell aktives Fenster verschieben</li> <li>• Maustastenänderung</li> <li>• Hauptmenü des Bedienfelds anzeigen</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>• Hauptmenüliste des Bedienfelds anzeigen</li> <li>• Fenster "Befehl ausführen" anzeigen</li> <li>• Bildschirmschoner aktivieren</li> <li>• Desktop anzeigen</li> <li>• Zwischen offenen Fenstern umschalten</li> <li>• Aktuell aktives Fenster zwischen Vollbild- und normalem Modus umschalten</li> <li>• Menüoptionen für aktuelles Fenster anzeigen</li> <li>• Druck – Einen Screenshot erstellen</li> </ul>

## Konfigurieren von Anmeldeerlebnis-Einstellungen

Verwenden Sie diese Seite, um Einstellungen zu konfigurieren, wie z. B. automatische Anmeldung, Anmelde-Bannernachricht und Kennwörter für Administratoren, Thinuser und Root-Benutzer.

**Tabelle 170. Konfigurieren von Anmeldeerlebnis-Einstellungen**

Option	Beschreibung
<b>Automatische Anmeldung</b>	Wählen Sie diese Option für die automatische Anmeldung des Thin Clients aus, ohne dass ein Eingreifen des Benutzers erforderlich ist. Verwenden Sie die Option <b>Benutzername für die automatische Anmeldung</b> zur Auswahl des Standardbenutzers für die Anmeldung.
<b>Benutzername für die automatische Anmeldung</b>	Wählen Sie das Kontrollkästchen <b>Automatische Anmeldung</b> zum Definieren des Standardbenutzers für die automatische Anmeldung. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option. <ul style="list-style-type: none"> <li>• Administrator</li> <li>• Thinuser</li> <li>• Gast</li> </ul>
<b>Banner im Anmeldefenster aktivieren</b>	Wählen Sie diese Option zum Konfigurieren einer Bannernachricht, die auf dem Anmeldebildschirm angezeigt wird.  Die Option <b>Bannernachricht</b> wird angezeigt, wenn Sie das Kontrollkästchen <b>Banner im Anmeldefenster aktivieren</b> wählen. Geben Sie einen benutzerdefinierten Text im Kästchen ein, der auf dem Anmeldebildschirm angezeigt werden soll.
<b>Root-Kennwort</b>	Geben Sie das Kennwort ein, wenn Sie das Root-Kennwort ändern möchten.
<b>Administratorkennwort</b>	Geben Sie das Kennwort ein, wenn Sie das Administratorkennwort ändern möchten.
<b>Thinuser-Kennwort</b>	Geben Sie das Kennwort ein, wenn Sie das Thinuser-Kennwort ändern möchten.
<b>Gastkennwort</b>	Geben Sie das Kennwort ein, wenn Sie das Gastkennwort ändern möchten.

# Konfigurieren der Netzwerkeinstellungen

Verwenden Sie diese Seite zum Konfigurieren der Netzwerkeinstellungen.

**Tabelle 171. Konfigurieren der Netzwerkeinstellungen**

Option	Beschreibung
<b>Name der Wireless-Verbindung</b>	Geben Sie den Namen der Verbindung ein.
<b>SSID</b>	Geben Sie den Namen der SSID-Verbindung (Service Set Identifier) ein.
<b>Sicherheitsmodus</b>	Wählen Sie aus dem Dropdownmenü den gewünschten Typ des Sicherheitsmodus aus. Geben Sie die Einzelheiten zum Sicherheitsmodus in die entsprechenden Felder ein.

# Konfigurieren der Sicherheitseinstellungen

Verwenden Sie diese Seite zum Konfigurieren von Sicherheitsoptionen.

**Tabelle 172. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
<b>Algorithmus für Kennwortverschlüsselung</b>	Wählen Sie diese Option zur Auswahl des Algorithmus für die Kennwortverschlüsselung. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"><li>• Base-64</li><li>• AES</li><li>• Nur-Text</li></ul> Der Standardwert beträgt <b>Base-64</b> .
<b>Zurücksetzen mit G-Taste aktivieren</b>	Standardmäßig ist die Funktion "Zurücksetzen mit G-Taste" aktiviert. Das Zurücksetzen auf die Werkseinstellungen des Geräts kann ausgeführt werden, wenn die G-Taste während des Starts gedrückt wird.
<b>Zertifikate installieren</b>	Wählen Sie diese Option zur Auswahl des Zertifikats, das Sie auf dem Gerät installieren möchten.  Wählen Sie aus dem Dropdownmenü die Zertifikate, die dem Datei-Repository hinzugefügt werden sollen.
<b>SSH aktivieren</b>	Wählen Sie diese Option aus, um Secure Shell (SSH) auf dem Gerät zu aktivieren.
<b>"Root"-SSH-Anmeldung zulassen</b>	Wählen Sie diese Option aus, um die "Root"-SSH-Anmeldung zuzulassen.
<b>VNC-Server aktivieren</b>	Wählen Sie diese Option aus, um den VNC-Server zu aktivieren.
<b>Eingabe des Kennworts durch Benutzer erforderlich machen</b>	Wählen Sie diese Option aus, um das VNC-Kennwort festzulegen.
<b>VNC-Kennwort</b>	Wählen Sie diese Option aus, um das VNC-Kennwort einzugeben.

Option	Beschreibung
<b>Benutzer bei VNC-Sitzungsstart Eingabeaufforderung anzeigen</b>	Wählen Sie diese Option aus, damit eine Pop-Up-Meldung zum Akzeptieren der eingehenden VNC-Verbindungsanfrage angezeigt wird.
<b>USB-Sperre</b>	Wählen Sie diese Option zur Begrenzung der Nutzung von USB-Anschlüssen. Die gültigen Optionen sind: <ul style="list-style-type: none"> <li>· Alle zulassen: Erlaubt den Zugriff auf alle USB-Anschlüsse.</li> <li>· Alle ablehnen: Verweigert den Zugriff auf alle USB-Anschlüsse.</li> <li>· Alle außer HID ablehnen: Verweigert den Zugriff auf alle USB-Ports mit Ausnahme jener für Eingabegeräte wie Maus, Tastatur usw.</li> <li>· Klasse ablehnen: Verweigert den Zugriff nur auf USB-Ports, die einer bestimmten abgelehnten Klasse angehören.</li> </ul>

## Konfigurieren von zentralen Konfigurationseinstellungen

Verwenden Sie diese Seite, um den Dateiserver, den Firmware-Server, den Root-Pfad und die entsprechenden Anmeldeinformationen von Benutzern einzugeben.

**Tabelle 173. Konfigurieren von zentralen Konfigurationseinstellungen**

Option	Beschreibung
<b>Dateiserverpfad</b>	Geben Sie den vollständigen Pfad des Ordners an, in dem der Ordner <b>wlx</b> liegt. Unterstützte Protokolle umfassen FTP, HTTP, und HTTPS.  Das Standardprotokoll ist FTP.
<b>Dateiserver-Benutzername</b>	Geben Sie den Benutzernamen für den Zugriff auf den Dateiserver ein.
<b>Dateiserver-Kennwort</b>	Geben Sie das Kennwort für den Zugriff auf den Dateiserver ein.
<b>Root-Pfad</b>	Dieser Root-Pfad wird für den Zugriff auf Dateien auf dem Server verwendet. Der Verzeichnisname <b>/wlx</b> wird vor der Verwendung an den Root-Pfad-Eintrag angehängt. Falls kein Root-Pfad angegeben wird, wird <b>/Wyse</b> berücksichtigt.
<b>Firmware-Server/-Pfad</b>	Geben Sie den vollständigen Pfad des Ordners an, in dem die Firmware-Abbilder liegen. Unterstützte Protokolle umfassen FTP, HTTP, und HTTPS.  Das Standardprotokoll ist FTP.
<b>Firmware-Server-Benutzername</b>	Geben Sie den Benutzernamen für den Zugriff auf den Firmware-Server ein.
<b>Firmware-Server-Kennwort</b>	Geben Sie das Kennwort für den Zugriff auf den Firmware-Server ein.
<b>Firmware-Root-Pfad</b>	Dieser Root-Pfad wird für den Zugriff auf Firmware-Abbilder auf dem Server verwendet. Der Verzeichnisname <b>/wtx</b> wird vor der Verwendung an den Root-Pfad-Eintrag angehängt. Falls der Root-Pfad nicht angegeben wird, wird <b>/wyse</b> berücksichtigt.

## Andere Einstellungen konfigurieren

Verwenden Sie diese Seite zum Konfigurieren von anderen Optionen.

**Tabelle 174. Andere Einstellungen konfigurieren**

Option	Beschreibung
<b>Automatisches Hochfahren</b>	Wählen Sie diese Option, damit das System startet, wenn die Stromversorgung wiederhergestellt ist, ohne darauf zu warten, dass der Netzschalter gedrückt wird.
<b>Betriebsschalter-Aktion</b>	Wählen Sie aus dem Dropdownmenü eine der Optionen zur Angabe der standardmäßigen Maßnahme aus, die durchgeführt wird, wenn Sie den Betriebsschalter drücken. <ul style="list-style-type: none"><li>• Interaktiv</li><li>• Neustart</li><li>• Herunterfahren</li><li>• Kein</li></ul>
<b>DHCP-Anbieter-ID</b>	Wählen Sie diese Option, um die DHCP-Anbieter-ID zu ändern. Die Standard-Anbieter-ID ist <b>wyse-5000</b> .
<b>Browserstartseite</b>	Wählen Sie diese Option aus, um die Browserstartseite festzulegen. Geben Sie die URL-Adresse Ihrer Wahl ein, um die Browserstartseite festzulegen.

## Konfigurieren von globalen VDI-Einstellungen

Verwenden Sie diese Seite zum Konfigurieren der globalen Einstellungen für Citrix und VMware View Clients.

**Tabelle 175. Konfigurieren von allgemeinen Citrix-Einstellungen**

Option	Beschreibung
<b>ICA-Suchprotokoll</b>	Wählen Sie diese Option, um das Standard-Suchprotokoll festzulegen.
<b>Browser-IP</b>	Geben Sie die Browser-IP-Adresse ein.
<b>Speichername</b>	Wählen Sie diese Option aus, um den Speichernamen anzugeben.
<b>Domainname</b>	Geben Sie den Domännennamen ein.
<b>PN-Desktopsetup (Alle Anwendungen anzeigen)</b>	Wählen Sie diese Option aus, um das PN-Desktop-Setup zu aktivieren. Wenn diese Option aktiviert ist, werden alle veröffentlichten Anwendungen auf dem Desktop angezeigt.
<b>Multimedia-Umleitung (MMR) aktivieren</b>	Wählen Sie diese Option aus, um die Multimedia-Umleitung zu aktivieren.
<b>H.264-Dekodierungssupport aktivieren</b>	Wählen Sie diese Option für das Aktivieren des H.264-Dekodierungssupports für ICA-Verbindungen.

Option	Beschreibung
<b>HDX Webcam Bildfrequenz</b>	Wählen Sie diese Option aus, um die bevorzugte Framerate für die HDX-Webcam festzulegen.
<b>HDX Webcam Bildbreite</b>	Wählen Sie diese Option zum Einstellen der Breite der Bild-Anfrage von der HDX-Webcam.
<b>HDX Webcam Bildhöhe</b>	Wählen Sie diese Option zum Einstellen der Höhe der Bild-Anfrage von der HDX-Webcam.
<b>Audiobandbreiten-Grenze</b>	Wählen Sie diese Option aus, um die Bandbreite für den Audioeingang festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Niedrig</li> <li>· Mittel</li> <li>· Hoch</li> </ul>
<b>UDP-Audio aktivieren</b>	Wählen Sie diese Option aus, um den Transport von Audiodaten über UDP zu aktivieren.
Flash-Umleitungsrichtlinie	Wählen Sie diese Option, um die Flash-Umleitungsrichtlinie festzulegen. Wählen Sie aus dem Dropdownmenü entweder Zulassen oder Verweigern für die Flash-Umleitungsrichtlinie.
<b>Unsichtbarer Tasten-Passthrough</b>	Wählen Sie die Option aus, um zu bestimmen, wie die Zuordnung bestimmter Tastenkombinationen bei Verbindung mit ICA-Sitzungen verwendet wird  Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Lokal</li> <li>· Remote</li> <li>· Nur Vollbild</li> </ul>
<b>Alternative Adresse verwenden</b>	Wählen Sie diese Option zur Verwendung einer alternativen IP-Adresse aus dem ICA-Master-Browser zum Passieren von Firewalls.
<b>ICA-Proxytyp</b>	Wählen Sie diese Option zur Auswahl des Proxy-Typs für die ICA-Verbindung. Der Standardwert ist <b>Kein</b> .

**Tabelle 176. Konfigurieren von Citrix USB-Umleitungseinstellungen**

Option	Beschreibung
<b>USB-Umleitung angeschlossener Geräte vor ICA-Sitzungsstart zulassen</b>	Wählen Sie diese Option für den ICA-Desktopgerätemodus aus. Diese Option ermöglicht die USB-Umleitung der angeschlossenen Geräte, bevor die ICA-Sitzung gestartet wird.
<b>USB-Umleitung aktivieren</b>	Wählen Sie diese Option aus, um die Citrix USB-Umleitung zu allen Geräten zu aktivieren.  Sie können festlegen, welche Geräte und Gerätefamilien in Citrix-Sitzungen über die USB-Umleitungsrichtlinie gestattet oder verweigert werden können.

**Tabelle 177. Konfigurieren der Citrix-Festplattenzuordnung**

Option	Beschreibung
<b>Dynamische ICA-Laufwerkszuordnung aktivieren</b>	Wählen Sie diese Option aus, um Double Dynamische ICA-Festplattenzuordnung zu aktivieren. Wenn diese Option deaktiviert ist, können Sie die einzelnen Laufwerke für verschiedene Laufwerkstypen hinzufügen. Dementsprechend werden nur einzelne Laufwerke in der ICA-Sitzung umgeleitet.

**Tabelle 178. Konfigurieren der VMware USB-Umleitung**

Option	Beschreibung
<b>USB-Umleitung aktivieren</b>	Wählen Sie diese Option aus, um die VMware USB-Umleitung zu allen Geräten zu aktivieren.  Sie können festlegen, welche Geräte und Gerätefamilien in VMware-Sitzungen über die USB-Umleitungsrichtlinie gestattet oder verweigert werden können.

## Konfigurieren von Remote-Verbindungseinstellungen – Citrix

Verwenden Sie diese Seite zum Erstellen einer Citrix Broker-Verbindung. Konfigurationseinstellungen für Citrix-Verbindungen variieren je nach Verbindungstyp.

**Tabelle 179. Konfigurieren von Remote-Verbindungseinstellungen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um einen Namen zur Identifizierung der Verbindung einzugeben.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option zum automatischen Starten der Verbindung, nachdem Sie sich angemeldet haben.
<b>Verbindungstyp</b>	Wählen Sie diese Option aus, um einen Verbindungstyp festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Serververbindung</li> <li>• Veröffentlichte Anwendung</li> <li>• Store Front</li> </ul>
<b>Citrix Server-FQDN oder -IP-Adresse</b>	Wählen Sie diese Option zur Eingabe der IP-Adresse oder FQDN des Citrix Servers. Diese Option wird angezeigt, wenn Sie als Verbindungstyp <b>veröffentlichte Anwendung</b> oder <b>Storefront</b> gewählt haben.
<b>Veröffentlichte Anwendung</b>	Wählen Sie diese Option zur Angabe der veröffentlichten Anwendung, die zu starten ist. Diese Option wird angezeigt, wenn Sie als Verbindungstyp <b>veröffentlichte Anwendung</b> oder <b>Storefront</b> gewählt haben.
<b>Verbindungsserver</b>	Wählen Sie diese Option zur Eingabe der IP-Adresse oder FQDN des Citrix Verbindungsservers.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein.

Option	Beschreibung
<b>Kennwort</b>	Geben Sie das Kennwort ein.
<b>Domainname</b>	Geben Sie den Domänennamen ein.
<b>Speichername</b>	Geben Sie den Speichernamen des Citrix Servers ein. Diese Option wird angezeigt, wenn Sie als Verbindungstyp <b>veröffentlichte Anwendung</b> oder <b>Storefront</b> gewählt haben.
<b>Suchprotokoll</b>	Wählen Sie diese Option aus, um ein Suchprotokoll für sichere und nicht sichere Verbindungen festzulegen. Wählen Sie aus der Dropdownliste eine der beiden folgenden Optionen aus: <ul style="list-style-type: none"> <li>• http</li> <li>• https</li> </ul>
<b>Niedrige Bandbreite</b>	Wählen Sie diese Option, um langsame Bandbreite zu optimieren.
<b>Ton aktivieren</b>	Wählen Sie diese Option, um die Tonausgabe zu aktivieren.
<b>Smart Card-Anmeldung</b>	Wählen Sie diese Option aus, um die Smart-Card-Funktion für ICA-Verbindungen zu aktivieren.
<b>Verschlüsselungsstufe</b>	Wählen Sie diese Option zum Einstellen einer Verschlüsselungsebene aus. Wählen Sie im Dropdownmenü eine beliebige der folgenden Verschlüsselungsebenen aus: <ul style="list-style-type: none"> <li>• Einfach</li> <li>• RC5 (128 Bit – Nur Anmeldung)</li> <li>• RC5 (40 Bit)</li> <li>• RC5 (56 Bit)</li> <li>• RC5 (128 Bit)</li> </ul>
<b>Fenstergröße</b>	Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Standard</li> <li>• Nahtlos</li> <li>• 640 x 480</li> <li>• 1024 x 768</li> <li>• 800 x 600</li> <li>• 1280 x 1024</li> <li>• 1600 x 1200</li> <li>• Vollbild</li> </ul>
<b>Bildschirm-Farbtiefe</b>	Wählen Sie diese Option aus, um die Bildschirm-Farbtiefe festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• 64 K</li> <li>• 256</li> <li>• 16 M</li> </ul>
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung zur Citrix-Sitzung wiederherstellt.

Option	Beschreibung
<b>Verzögerung vor erneutem Verbindungsversuch</b>	Wählen Sie diese Option aus, um die Zeit in Sekunden festzulegen, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.
<b>Ping vor Verbindung</b>	Sie können die Ping-Option aktivieren, um sicherzustellen, dass der Host erreichbar ist.
<b>Anmeldung durch Einfügen mit Mitteltaste aktivieren</b>	Sie können die Einfügeoption für die Anmeldung aktivieren.
<b>Komprimierung</b>	Sie können die Komprimierung während einer Sitzung aktivieren oder deaktivieren.

## Konfigurieren von Remote-Verbindungseinstellungen – VMware

Verwenden Sie diese Seite zum Erstellen einer VMware View Broker-Verbindung.

**Tabelle 180. Konfigurieren von VMware Remote-Verbindungen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um einen Namen zur Identifizierung der Verbindung einzugeben.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option zum automatischen Starten der Verbindung, nachdem Sie sich angemeldet haben.
<b>VMWare Serveradresse</b>	Geben Sie den Hostnamen oder die IP-Adresse des VMware View-Servers ein.
<b>VMWare Serverportnummer</b>	Geben Sie die Portnummer des Hosts ein.
<b>Sichere Verbindung (SSL) verwenden</b>	Wählen Sie diese Option aus, um die SSL-Verbindung zu verwenden.
<b>Protokoll</b>	Wählen Sie diese Option aus, um <b>PCoIP</b> oder <b>RDP</b> als Protokoll auszuwählen.
<b>NLA aktivieren</b>	Mit dieser Option wird die Authentifizierung auf Netzwerkebene aktiviert. Wenn die Option <b>RDP</b> als Protokoll eingestellt ist, wird diese Option angezeigt.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein
<b>Kennwort</b>	Geben Sie das Kennwort ein.
<b>Domainname</b>	Geben Sie den Domännennamen ein.
<b>Interaktiver Modus</b>	Wählen Sie diese Option aus, um den interaktiven Benutzermodus zu aktivieren.
<b>Server-URL/Hostfeld sperren</b>	Wählen Sie diese Option aus, um die Server-URL zu sperren.

Option	Beschreibung
<b>Sicherheitsmodus</b>	Wählen Sie diese Option aus, um den Sicherheitsmodus einzustellen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Niemals Verbindung zu nicht vertrauenswürdigen Servern herstellen</li> <li>· Vor Verbindung mit nicht vertrauenswürdigen Server warnen</li> <li>· Serveridentitäts-Zertifikate nicht überprüfen.</li> </ul>
<b>Vollbildschirm-Modus</b>	Wählen Sie diese Option zum Anzeigen der Remote-Sitzung im Vollbildschirm-Modus.
<b>Fenstergröße</b>	Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Alle Monitore verwenden</li> <li>· Vollbild</li> <li>· Großer Bildschirm</li> <li>· Kleiner Bildschirm</li> <li>· 1024 x 768</li> <li>· 800 x 600</li> <li>· 640 x 480</li> </ul>
<b>Dropdownmenüleiste für Vollbild deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren des Dropdownmenüs im Vollbildschirm-Modus.
<b>Diesen Desktop automatisch starten</b>	Wählen Sie diese Option, um den Namen des veröffentlichten Desktops anzugeben, der bei erfolgreicher Verbindung automatisch gestartet werden soll.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung zur VMware-Sitzung wiederherstellt.
<b>Verzögerung vor erneutem Verbindungsversuch</b>	Geben Sie die Zeit in Sekunden an, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.
<b>Benutzername mit Domain</b>	Wählen Sie diese Option, um der Domäne einen Benutzernamen zuzuordnen.
<b>Nicht authentifizierter Zugriff</b>	Wählen Sie diese Option, um einen nicht authentifizierten Zugriff auf die Anwendung zu verhindern.
<b>Ping vor Verbindung</b>	Wählen Sie diese Option, um das System vor der Verbindung anzupingen.
<b>MMR aktivieren</b>	Wählen Sie diese Option aus, um MMR zu aktivieren oder zu deaktivieren:
<b>Interaktiver Modus</b>	Wählen Sie diese Option aus, um den interaktiven Modus zu aktivieren.
<b>Beenden bei Trennung der Verbindung deaktivieren</b>	Wählen Sie diese Option, um die Auflistung der Systeme nach dem Abmelden von der Sitzung zu deaktivieren.
<b>SSL-Protokoll</b>	Diese Option konfiguriert die Verschlüsselungsliste so, dass die Verwendung von kryptografischen Protokollen vor dem Aufbau einer SSL-Verbindung eingeschränkt wird.

Option	Beschreibung
<b>SSL-Verschlüsselung</b>	Diese Option konfiguriert die Verschlüsselungsliste so, dass die Verwendung von kryptografischen Protokollen vor dem Aufbau einer SSL-Verbindung eingeschränkt wird.

## Konfigurieren von Remote-Verbindungseinstellungen – RDP

Verwenden Sie diese Seite zum Erstellen einer RDP-Broker-Verbindung.

**Tabelle 181. Konfigurieren von Remote-Verbindungseinstellungen – RDP**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um den Namen für die Identifizierung der Verbindung einzugeben.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option zum automatischen Starten der Verbindung, nachdem Sie sich angemeldet haben.
<b>Serveradresse</b>	Geben Sie den Servernamen oder die IP-Adresse an.
<b>Smart Card-Anmeldung</b>	Mit dieser Option wird die Smart Card-Authentifizierung aktiviert.
<b>Authentifizierung auf Netzwerkebene (NLA) verwenden</b>	Mit dieser Option wird die Authentifizierung auf Netzwerkebene aktiviert.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein.
<b>Kennwort</b>	Geben Sie das Kennwort ein.
<b>Domainname</b>	Geben Sie den Domänennamen ein.
<b>Fenstergröße</b>	Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Standard</li> <li>• 640 x 480</li> <li>• 1024 x 768</li> <li>• 800 x 600</li> <li>• 1280 x 1024</li> <li>• 1600 x 1200</li> <li>• Vollbild</li> </ul>
<b>Alle Drucker weiterleiten</b>	Wählen Sie diese Option, um alle Drucker an die Remoteverbindung weiterzuleiten.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung zur RDP-Sitzung wiederherstellt.
<b>Verzögerung vor erneutem Verbindungsversuch</b>	Geben Sie die Zeit in Sekunden an, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.

Option	Beschreibung
<b>Laufwerkzuordnung</b>	<p>Wählen Sie diese Option aus, um Laufwerke in der RDP-Sitzung zuzuweisen. Klicken Sie auf die Schaltfläche <b>Laufwerkszuweisung hinzufügen</b> und geben Sie die folgenden Details ein:</p> <ul style="list-style-type: none"> <li>· Laufwerksbuchstaben – Wählen Sie aus dem Dropdownmenü den Laufwerksbuchstaben.</li> <li>· Laufwerkstyp – Wählen Sie einen der folgenden Laufwerktypen: <ul style="list-style-type: none"> <li>– USB-Festplatte oder Speicherstick</li> <li>– USB-CD-ROM</li> <li>– USB-Floppy</li> </ul> </li> </ul>
<b>RD-Gateway-Einstellungen verwenden</b>	<p>Wählen Sie diese Option zum Verwenden der RD-Gateway-Einstellungen. Die Optionen <b>RD-Server</b> und <b>Remote-Desktop-Anmeldeinformationen für RD-Gateway verwenden</b> werden angezeigt.</p>
<b>RD-Server</b>	<p>Wählen Sie diese Option zur Angabe der Hostadresse des RD-Gateways aus.</p>
<b>Remote-Desktop-Anmeldeinformationen für RD-Gateway verwenden</b>	<p>Wählen Sie diese Option zur Verwendung der Remote Desktop Anmeldeinformationen für das RD-Gateway aus.</p> <p>Wenn Sie das Kontrollkästchen deaktivieren, werden die Optionen <b>RD-Benutzername</b>, <b>RD-Kennwort</b> und <b>RD-Domainname</b> angezeigt.</p>
<b>RD-Benutzername</b>	<p>Geben Sie einen RD-Benutzernamen für die Anmeldung am RD-Gateway ein.</p>
<b>RD-Kennwort</b>	<p>Geben Sie das RD-Kennwort für die Anmeldung am RD-Gateway ein.</p>
<b>RD-Domainname</b>	<p>Geben Sie den RD-Domainnamen für die Anmeldung am RD-Gateway ein.</p>
<b>Ping vor Verbindung</b>	<p>Diese Option wird verwendet, um die Ping-Option für nicht veröffentlichte Anwendungsverbindungen zu aktivieren.</p>
<b>Bei Trennung benachrichtigen</b>	<p>Diese Option sendet eine Benachrichtigung, wenn das System die Verbindung trennt.</p>
<b>Komprimierung</b>	<p>Diese Option aktiviert die Komprimierungsfunktion auf einem System.</p>
<b>Niedrige Bandbreite</b>	<p>Diese Option gibt eine niedrige Bandbreite bekannt.</p>
<b>Tastaturereignisse nicht erfassen</b>	<p>Diese Option ermöglicht die Tastatureingabeerfassung in einer direkten RDP-Sitzung.</p>
<b>Geschwindigkeitsstufe</b>	<p>Diese Option zeigt die Geschwindigkeitsstufe an.</p>
<b>Töne</b>	<p>Diese Option wird verwendet, um Töne zu aktivieren oder zu deaktivieren.</p>
<b>Verschlüsselungsstufe</b>	<p>Diese Option wird zur Datenverschlüsselung verwendet.</p>

# Konfigurieren von Remote-Verbindungseinstellungen – Browser

Verwenden Sie diese Seite zum Konfigurieren der Browser-Remote-Verbindungen.

**Tabelle 182. Konfigurieren von Remote-Verbindungseinstellungen – Browser**

Option	Beschreibung
<b>Verbindungsname</b>	Geben Sie den Namen für die Identifizierung der Verbindung ein.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option zum automatischen Starten der Verbindung während der Anmeldung.
<b>URL</b>	Geben Sie die Start-URL an.
<b>Kioskmodus</b>	Wählen Sie diese Option aus, um den Kioskmodus zu aktivieren.
<b>Fenstergröße</b>	Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü die gewünschte Größe des Fensters.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung des Browsers wiederherstellt.
<b>Verzögerung vor erneutem Verbindungsversuch</b>	Geben Sie die Zeit in Sekunden an, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.

## Erweiterte Einstellungen konfigurieren

Konfigurationen können auf das Linux Client-Gerät durch die Eingabe der INI-Parameter in den **Erweiterten Optionen** angewendet werden. Dell empfiehlt, dass Sie keine INI-Parameter für Richtlinien einschließen, die bereits in anderen Optionen konfiguriert sind. Kennwortkodierung und -Verschlüsselung werden nicht auf die Kennwortparameter angewendet.

**Tabelle 183. Erweiterte Einstellungen konfigurieren**

Option	Beschreibung
<b>Keine globale INI</b>	Wenn diese Option ausgewählt ist, werden die globalen INI-Parameter nicht vom Dateiserver geladen.  Geben Sie die INI-Parameter von Zeile 1 bis Zeile 20 für die Thin Clients ein.

## Bearbeiten der Einstellungen für die ThinLinux-Richtlinie

Gehen Sie folgendermaßen vor, um die ThinLinux-Richtlinieneinstellungen zu konfigurieren:

- 1 Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
- 2 Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.

3 Klicken Sie auf **ThinLinux**.

Die Seite **ThinLinux** wird angezeigt. Die ThinLinux-Thin Client-Richtlinieneinstellungen umfassen die folgenden Optionen:

- Systempersonalisierung
- Desktoperlebnis
- Anmeldeerlebnis
- Netzwerk
- Sicherheit
- Zentrale Konfiguration
- Andere Einstellungen
- Globale VDI-Einstellungen
- Citrix Remote-Verbindungen
- VMware Remote-Verbindungen
- RDP Remote-Verbindungen
- Browser-Remote-Verbindungen
- Erweiterte Einstellungen
- Geräteinfo
- BIOS-Einstellungen für ThinLinux 3040
- BIOS-Einstellungen für ThinLinux 5070
- Proxy-Einstellungen

4 Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

## Konfigurieren der Systempersonalisierung

Verwenden Sie die Seite **Systempersonalisierung** zum Konfigurieren der Systempersonalisierung.

**Tabelle 184. Konfigurieren der Tastatureinstellungen**

Option	Beschreibung
<b>Layout</b>	Wählen Sie diese Option, um das Tastaturlayout des Thin Client festzulegen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.

**Tabelle 185. Konfigurieren von Spracheinstellungen**

Option	Beschreibung
<b>Systemsprache</b>	Wählen Sie diese Option zum Einstellen der Sprache für das System aus. Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.

**Tabelle 186. Konfigurieren der Mauseinstellungen**

Option	Beschreibung
<b>Mausgeschwindigkeit</b>	Wählen Sie diese Option aus, um die Geschwindigkeit des Mauszeigers beim Bewegen der Maus anzugeben. Der Bereich der Mausgeschwindigkeit beträgt 0 bis 6.
<b>Linkshänder-Maus</b>	Wählen Sie diese Option aus, um die Funktion der linken und rechten Maustaste zu vertauschen.

**Tabelle 187. Konfigurieren von Zeitzoneneinstellungen**

Option	Beschreibung
<b>Zeitzone</b>	Wählen Sie diese Option zum Einstellen der Zeitzone basierend auf Ihrem Standort. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Zeitzone.
<b>Zeitformat</b>	Wählen Sie diese Option aus, um das Zeitformat auszuwählen. Wählen Sie aus dem Dropdownmenü für das Zeitformat entweder das 12- oder 24-Stunden-Format.
<b>Zeitserver (NTP-Server)</b>	Wählen Sie diese Option aus, um die Zeitserver aufzulisten. Zeitserver ermöglichen es dem NTP-Server, die Zeit zu synchronisieren. Mehrere Server sind zulässig, die Servernamen müssen durch Kommas getrennt werden.

**Tabelle 188. Konfigurieren von Audioeinstellungen**

Option	Beschreibung
<b>Audiolautstärke</b>	Wählen Sie diese Option, um die Audiolautstärke des Thin Client festzulegen. Der Bereich der Audiolautstärke liegt zwischen 0 und 100.
<b>Audio stumm schalten</b>	Wählen Sie diese Option, um den Thin Client stummzuschalten.
<b>Mikrofonlautstärke</b>	Wählen Sie diese Option, um die Mikrofonlautstärke des Thin Client festzulegen. Der Bereich der Mikrofonlautstärke liegt zwischen 0 und 100.
<b>Mikrofon stumm schalten</b>	Wählen Sie diese Option aus, um das Mikrofon stummzuschalten.

## Desktop-Erfahrung konfigurieren

Verwenden Sie diese Seite zum Konfigurieren der Desktop-Einstellungen, wie z. B. Desktop-Hintergrundbild, Hintergrundbild-Layout und Desktop-Tastaturbefehle.

**Tabelle 189. Standard-Desktop-Symbole ausblenden**

Option	Beschreibung
<b>Desktop-Symbole ausblenden</b>	Wählen Sie aus dem Dropdown-Menü Ihre bevorzugte Option.
<b>Google Chrome ausblenden</b>	Wählen Sie diese Option, wenn Sie das Google Chrome-Webbrowser-Symbol ausblenden möchten, sodass es nicht auf dem Desktop angezeigt wird. Diese Option wird aktiviert, wenn Sie <b>Benutzerdefinierte Einstellungen</b> aus dem Dropdown-Menü <b>Desktop-Symbole ausblenden</b> auswählen.
<b>Mozilla Firefox ausblenden</b>	Wählen Sie diese Option, wenn Sie das Mozilla Firefox-Webbrowser-Symbol ausblenden möchten, sodass es nicht auf dem Desktop angezeigt wird. Diese Option wird aktiviert, wenn Sie <b>Benutzerdefinierte Einstellungen</b> aus dem Dropdown-Menü <b>Desktop-Symbole ausblenden</b> auswählen.
<b>Einstellungen ausblenden</b>	Wählen Sie diese Option, wenn Sie das Symbol der Einstellungen-App ausblenden möchten, sodass es nicht auf dem Desktop angezeigt wird. Diese Option wird aktiviert, wenn Sie

Option	Beschreibung
	<b>Benutzerdefinierte Einstellungen</b> aus dem Dropdown-Menü <b>Desktop-Symbole ausblenden</b> auswählen.

**Tabelle 190. Visuelles Erlebnis**

Option	Beschreibung
<b>Desktophintergrund</b>	Wählen Sie diese Option, um das Standard-Hintergrundbild zu ändern.
<b>Hintergrundbild-Datei</b>	Wählen Sie diese Option, um Ihr bevorzugtes Hintergrundbild auszuwählen. In das Datei-Repository hochgeladene Bilder werden angezeigt.
<b>Hintergrundbild-Layout</b>	Wählen Sie diese Option, um das Hintergrundbild-Layout einzustellen. Wählen Sie aus der Dropdown-Liste Ihr bevorzugtes Hintergrundbild-Layout. Das standardmäßige Hintergrundbild-Layout ist <b>zentriert</b> .

**Schnellasten** – Wählen Sie eine beliebige Kombination der folgenden Kontrollkästchen zum Deaktivieren der Schnellasten und ihrer jeweiligen Funktion:

Tastenkombinationen für die folgenden Aktionen konfigurieren:

- Aktuell aktives Fenster minimieren
- Aktuell aktives Fenster maximieren/Maximierung des aktuell aktiven Fensters aufheben
- Maximierung des aktuell aktiven Fensters aufheben
- Größe des aktuell aktiven Fensters ändern
- Aktuell aktives Fenster verschieben
- Desktop anzeigen
- Zwischen offenen Fenstern umschalten
- Aktuell aktives Fenster zwischen Vollbild- und normalem Modus umschalten
- Druck (einen Screenshot erstellen): Sie können das Kontrollkästchen zum Aktivieren oder Deaktivieren der Druck-Option (Screenshot) markieren.

## Konfigurieren des Anmeldeerlebnisses

Verwenden Sie diese Seite, um Einstellungen zu konfigurieren, wie z. B. automatische Anmeldung, Anmelde-Bannernachricht und Kennwörter für Administratoren, Thinuser und Root-Benutzer.

**Tabelle 191. Konfigurieren des Anmeldeerlebnisses**

Option	Beschreibung
<b>Automatische Anmeldung</b>	Wählen Sie diese Option für die automatische Anmeldung des Thin Clients aus, ohne dass ein Eingreifen des Benutzers erforderlich ist.
<b>Banner im Anmeldefenster aktivieren</b>	Wählen Sie diese Option zum Konfigurieren einer Bannernachricht, die auf dem Anmeldebildschirm angezeigt wird.
<b>Bannernachricht</b>	Die Option <b>Bannernachricht</b> wird angezeigt, wenn Sie das Kontrollkästchen <b>Banner im Anmeldefenster aktivieren</b> wählen. Geben Sie einen benutzerdefinierten Text im Kästchen ein, der auf dem Anmeldebildschirm angezeigt werden soll.

Option	Beschreibung
<b>Root-Kennwort</b>	Geben Sie das Kennwort ein, wenn Sie das Root-Kennwort ändern möchten.
<b>Thinuser-Kennwort</b>	Geben Sie das Kennwort ein, wenn Sie das Thinuser-Kennwort ändern möchten.

## Konfigurieren der Netzwerkeinstellungen

Verwenden Sie diese Seite zum Konfigurieren der Netzwerkeinstellungen.

**Tabelle 192. Konfigurieren der Netzwerkeinstellungen**

Option	Beschreibung
<b>Name der Wireless-Verbindung</b>	Geben Sie den Namen der Verbindung ein
<b>SSID</b>	Geben Sie den Namen der SSID-Verbindung (Service Set Identifier) ein.
<b>Sicherheitsmodus</b>	Wählen Sie aus dem Dropdownmenü den gewünschten Typ des Sicherheitsmodus aus. Geben Sie die Einzelheiten zum Sicherheitsmodus in die entsprechenden Felder ein.

## Konfigurieren der Sicherheitseinstellungen

Verwenden Sie diese Seite für die Konfiguration der Sicherheitsrichtlinieneinstellungen.

**Tabelle 193. Konfigurieren der USB-Regel**

Option	Beschreibung
<b>USB-Sperre</b>	<p>Wählen Sie aus der Dropdown-Liste eine der folgenden Optionen aus, um die Verwendung von USB-Ports einzuschränken:</p> <ul style="list-style-type: none"> <li>• Alle zulassen</li> <li>• Alle ablehnen</li> <li>• Alle außer HID ablehnen</li> <li>• Klasse ablehnen: Basierend auf der USB-Klasse können Sie den Zugriff auf das USB-Gerät verweigern.</li> </ul> <p><b>ANMERKUNG:</b> Diese Einstellung wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>Klasse ablehnen</b>	<p>Wählen Sie eine der folgenden Optionen, um USB-Geräte anhand ihrer Klasse zu deaktivieren:</p> <ul style="list-style-type: none"> <li>• Speicher</li> <li>• Audio</li> <li>• Smart Card</li> <li>• Video</li> <li>• Drucker</li> </ul>

Tabelle 194. Firewall-Einstellungen

Option	Beschreibung
Firewall-Einstellungen	<p>Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Nein</li> <li>• Ja</li> <li>• Ja mit Skript</li> </ul> <p><b>ANMERKUNG:</b> Diese Einstellung wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
Regeln	<p>Diese Option wird aktiviert, wenn Sie für die <b>Firewall-Einstellungen Ja mit Skript</b> auswählen. Sie können auswählen, ob die <code>txt</code>-Datei in das Inventar hochgeladen wird.</p>

Tabelle 195. Konfigurieren der allgemeinen Einstellungen

Option	Beschreibung
Zurücksetzen mit G-Taste aktivieren	<p>Standardmäßig ist die Funktion "Zurücksetzen mit G-Taste" aktiviert. Das Zurücksetzen auf Werkseinstellungen des Geräts kann ausgeführt werden, wenn die G-Taste während des Starts gedrückt wird.</p>
Zertifikate installieren	<p>Wählen Sie diese Option zur Auswahl des Zertifikats, das Sie auf dem Gerät installieren möchten.</p> <p>Wählen Sie aus dem Dropdownmenü die Zertifikate, die dem Datei-Repository hinzugefügt werden sollen.</p>

Tabelle 196. Konfigurieren von SSH-Einstellungen

Option	Beschreibung
SSH aktivieren	<p>Wählen Sie diese Option aus, um Secure Shell (SSH) auf dem Gerät zu aktivieren.</p>
"Root"-SSH-Anmeldung zulassen	<p>Wählen Sie diese Option aus, um die "Root"-SSH-Anmeldung zuzulassen.</p>

Tabelle 197. Konfigurieren der VNC-Einstellungen

Option	Beschreibung
VNC-Server aktivieren	<p>Wählen Sie diese Option aus, um den VNC-Server zu aktivieren.</p>
Eingabe des Kennworts durch Benutzer erforderlich machen	<p>Wählen Sie diese Option aus, um das VNC-Kennwort festzulegen.</p>
VNC-Kennwort	<p>Wählen Sie diese Option aus, um das VNC-Kennwort einzugeben.</p>
Benutzer bei VNC-Sitzungsstart Eingabeaufforderung anzeigen	<p>Wählen Sie diese Option aus, damit eine Pop-Up-Meldung zum Akzeptieren der eingehenden VNC-Verbindungsanfrage angezeigt wird.</p>

# Konfigurieren von zentralen Konfigurationseinstellungen

Verwenden Sie diese Seite, um den Dateiserver, den Firmware-Server, den Root-Pfad und die entsprechenden Anmeldeinformationen von Benutzern einzugeben.



**Tabelle 198. Konfigurieren von zentralen Konfigurationseinstellungen**

Option	Beschreibung
<b>Dateiserver/-pfad</b>	Geben Sie den vollständigen Pfad des Ordners an, in dem der Ordner <b>wlx2</b> liegt. Unterstützte Protokolle umfassen FTP, HTTP, und HTTPS.  Das Standardprotokoll ist FTP.
<b>Dateiserver-Benutzername</b>	Geben Sie den Benutzernamen für den Zugriff auf den Dateiserver ein.
<b>Dateiserver-Kennwort</b>	Geben Sie das Kennwort für den Zugriff auf den Dateiserver ein.
<b>Root-Pfad</b>	Dieser Root-Pfad wird für den Zugriff auf Dateien auf dem Server verwendet. Der Verzeichnisname <b>/wlx2</b> wird vor der Verwendung an den Root-Pfad-Eintrag angehängt. Falls kein Root-Pfad angegeben wird, wird <b>/Wyse</b> berücksichtigt.
<b>Verzögerte Aktualisierung aktivieren</b>	Wählen Sie diese Option aus, um den Upgrade- oder Downgrade-Vorgang für Hintergrundabbilder oder Add-ons zu aktivieren.
<b>Server/Pfad für verzögerte Aktualisierung</b>	Geben Sie den vollständigen Pfad des Ordners an, in dem die Firmware-Abbilder liegen. Unterstützte Protokolle umfassen FTP, HTTP, und HTTPS.  Das Standardprotokoll ist FTP.
<b>Benutzername für Server für verzögerte Aktualisierung</b>	Geben Sie den Benutzernamen für den Zugriff auf den Server für die verzögerte Aktualisierung ein.
<b>Kennwort für Server für verzögerte Aktualisierung</b>	Geben Sie das Kennwort für den Zugriff auf den Server für die verzögerte Aktualisierung ein.
<b>Modus für verzögerte Aktualisierung</b>	Wählen Sie diese Option aus, um den Aktualisierungsmodus für den verzögerten Aktualisierungsvorgang festzulegen.
<b>Auf Werkseinstellungen zurücksetzen</b>	Wählen Sie diese Option, um das Gerät nach der Abbilderstellung auf die Werkseinstellungen zurückzusetzen.
<b>Herunterstufen des Basisimages erlauben</b>	Wählen Sie diese Option aus, um das Zurücksetzen auf Basisabbild zu aktivieren.

## Andere Einstellungen konfigurieren

Verwenden Sie diese Seite zum Konfigurieren von anderen Optionen.

Tabelle 199. Andere Einstellungen konfigurieren

Option	Beschreibung
<b>Automatisches Hochfahren</b>	Wählen Sie diese Option, damit das System startet, wenn die Stromversorgung wiederhergestellt ist, ohne darauf zu warten, dass der Netzschalter gedrückt wird.   <b>ANMERKUNG: Diese Option wird in ThinLinux 2.0 nicht unterstützt.</b>
<b>Betriebsschalter-Aktion</b>	Wählen Sie im Dropdownmenü eine beliebige der Optionen aus: <ul style="list-style-type: none"> <li>• Interaktiv</li> <li>• Neustart</li> <li>• Herunterfahren</li> <li>• Kein</li> </ul> <p>Diese Option definiert die durchzuführende Aktion, wenn Sie den Betriebsschalter betätigen.</p>
<b>DHCP-Anbieter-ID</b>	Wählen Sie diese Option, um die DHCP-Anbieter-ID zu ändern. Die Standard-Anbieter-ID ist <b>wyse-5000</b> .
<b>Browserstartseite</b>	Wählen Sie diese Option aus, um die Browserstartseite festzulegen. Geben Sie die URL-Adresse Ihrer Wahl ein, um die Browserstartseite festzulegen.
<b>Zeitüberschreitung für Bildschirmsperre anzeigen</b>	Wählen Sie aus dem Dropdown-Menü den Wert für die Zeitüberschreitung der Bildschirmsperre.   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>

## Konfigurieren von globalen VDI-Einstellungen

Die folgenden globalen VDI-Einstellungen können unter "ThinLinux Richtlinieneinstellungen" konfiguriert werden. In den globalen VDI-Einstellungen können Sie die globalen Einstellungen für Citrix und VMware View festlegen.

Tabelle 200. ICA COM-Port-Zuordnung

Option	Beschreibung
<b>Laufwerkzuordnung</b>	Verwenden Sie diese Option, um die COM-Ports einem COM-Laufwerk zuzuordnen.   <b>ANMERKUNG: Diese Option gilt für Thin Clients mit ThinLinux 2.1 und neueren Versionen.</b>

Tabelle 201. Konfigurieren von allgemeinen Citrix-Einstellungen

Option	Beschreibung
<b>ICA-Suchprotokoll</b>	Wählen Sie diese Option, um das Standard-Suchprotokoll festzulegen.
<b>ICA-PAM-Anmeldung</b>	Wählen Sie diese Option zum Konfigurieren der PAM-Anmeldung.
<b>Browser-IP</b>	Geben Sie die Browser-IP-Adresse ein.

Option	Beschreibung
<b>Speichername</b>	Legen Sie den Speichernamen fest.
<b>Domainname</b>	Geben Sie den Domännennamen ein.
<b>PN-Desktopsetup (Alle Anwendungen anzeigen)</b>	Wählen Sie diese Option aus, um das PN-Desktop-Setup zu aktivieren. Wenn diese Option aktiviert ist, werden alle veröffentlichten Anwendungen auf dem Desktop angezeigt.
<b>Multimedia-Umleitung (MMR) aktivieren</b>	Wählen Sie diese Option aus, um die Multimedia-Umleitung zu aktivieren.
<b>H.264-Dekodierungssupport aktivieren</b>	Wählen Sie diese Option für das Aktivieren des H.264-Dekodierungssupports für ICA-Verbindungen.
<b>HDX Webcam Bildfrequenz</b>	Wählen Sie diese Option aus, um die bevorzugte Framerate für die HDX-Webcam festzulegen.
<b>HDX Webcam Bildbreite</b>	Wählen Sie diese Option zum Einstellen der Breite der Bild-Anfrage von der HDX-Webcam.
<b>HDX Webcam Bildhöhe</b>	Wählen Sie diese Option zum Einstellen der Höhe der Bild-Anfrage von der HDX-Webcam.
<b>Audiobandbreiten-Grenze</b>	Wählen Sie diese Option aus, um die Bandbreite für den Audioeingang festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Niedrig</li> <li>• Mittel</li> <li>• Hoch</li> </ul>
<b>UDP-Audio aktivieren</b>	Wählen Sie diese Option aus, um den Transport von Audiodaten über UDP zu aktivieren.
<b>Flash-Umleitungsrichtlinie</b>	Wählen Sie diese Option aus, um die Flash-Umleitungsrichtlinie entweder zuzulassen oder zu verweigern.
<b>Unsichtbarer Tasten-Passthrough</b>	Wählen Sie die Option aus, um zu bestimmen, wie die Zuordnung bestimmter Tastenkombinationen bei Verbindung mit ICA-Sitzungen verwendet wird  Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Lokal</li> <li>• Remote</li> <li>• Nur Vollbild</li> </ul>
<b>Alternative Adresse verwenden</b>	Wählen Sie diese Option zur Verwendung einer alternativen IP-Adresse aus dem ICA-Master-Browser zum Passieren von Firewalls.
<b>ICA-Proxytyp</b>	Wählen Sie diese Option zur Auswahl des Proxy-Typs für die ICA-Verbindung. Der Standardwert ist <b>Kein</b> .

**Tabelle 202. Konfigurieren von Citrix USB-Umleitungseinstellungen**

Option	Beschreibung
<b>USB-Umleitung angeschlossener Geräte vor ICA-Sitzungsstart zulassen</b>	Markieren Sie dieses Kontrollkästchen für den ICA-Desktopgerätemodus. Diese Option ermöglicht die USB-Umleitung der Geräte, die vor dem ICA-Sitzungsstart eingesteckt wurden.
<b>USB-Umleitung aktivieren</b>	Wählen Sie diese Option aus, um die Citrix USB-Umleitung zu allen Geräten zu aktivieren.  Sie können festlegen, welche Geräten und Gerätefamilien in Citrix-Sitzungen gestattet oder verweigert werden können.

**Tabelle 203. Konfigurieren von Citrix Laufwerkzuordnungseinstellungen**

Option	Beschreibung
<b>Dynamische ICA-Laufwerkszuordnung aktivieren</b>	Wählen Sie diese Option aus, um Dynamische ICA-Laufwerkszuordnung zu aktivieren. Wenn diese Option deaktiviert ist, können Sie die einzelnen Laufwerke für verschiedene Laufwerkstypen hinzufügen. Dementsprechend werden nur einzelne Laufwerke in der ICA-Sitzung umgeleitet.
<b>Alle Laufwerke einem einzelnen Freigabennamen (WyseUSB) zuordnen</b>	Wählen Sie diese Option aus, um alle USB-Geräte-Inhalte in der ICA-Sitzung in ein einziges Verzeichnis umzuleiten: Wyse USB.

**Tabelle 204. Konfigurieren von VMware USB-Umleitungseinstellungen**

Option	Beschreibung
<b>USB-Umleitung aktivieren</b>	Wählen Sie diese Option aus, um die USB-Umleitungsrichtlinie bei VMware-Sitzungen entweder zuzulassen oder zu verweigern.

## Konfigurieren von Remote-Verbindungseinstellungen – Citrix

Verwenden Sie diese Seite zum Erstellen einer Citrix Broker-Verbindung. Konfigurationseinstellungen für Citrix-Verbindungen variieren je nach Verbindungstyp.

**Tabelle 205. Konfigurieren von Remote-Verbindungseinstellungen – Citrix**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um einen Namen zur Identifizierung der Verbindung einzugeben.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option zum automatischen Starten der Verbindung, nachdem Sie sich angemeldet haben.
<b>Verbindungstyp</b>	Wählen Sie diese Option aus, um einen Verbindungstyp festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Serververbindung</li> <li>• Veröffentlichte Anwendung</li> <li>• Store Front</li> </ul>

<b>Option</b>	<b>Beschreibung</b>
<b>Verbindungsserver</b>	Wählen Sie diese Option zur Eingabe der IP-Adresse oder FQDN des Citrix Servers.
<b>Citrix Server-FQDN oder -IP-Adresse</b>	Wählen Sie diese Option zum Zugriff auf die Citrix Server-FQDN oder IP-Adresse. Dies gilt für die Verbindungstypen "veröffentlichte Anwendung" und "StoreFront".
<b>Veröffentlichte Anwendung</b>	Wählen Sie diese Option zur Angabe der veröffentlichten Anwendung, die zu starten ist. Dies gilt für die Verbindungstypen "veröffentlichte Anwendung" und "StoreFront".
<b>Speichernamen</b>	Geben Sie den Speichernamen ein. Dies gilt für die Verbindungstypen "veröffentlichte Anwendung" und "StoreFront".
<b>Benutzername</b>	Geben Sie den Benutzernamen ein.
<b>Kennwort</b>	Geben Sie das Kennwort ein.
<b>Domainname</b>	Geben Sie den Domännennamen ein.
<b>Suchprotokoll</b>	Wählen Sie diese Option aus, um ein Suchprotokoll für sichere und nicht sichere Verbindungen festzulegen. Wählen Sie aus der Dropdownliste eine der beiden folgenden Optionen aus: <ul style="list-style-type: none"> <li>• http</li> <li>• https</li> </ul>
<b>Niedrige Bandbreite</b>	Markieren Sie das Kontrollkästchen, um die Optimierung für niedrige Bandbreite zu aktivieren.
<b>Ton aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um den Ton zu aktivieren.
<b>Smart Card-Anmeldung</b>	Wählen Sie das Kontrollkästchen zur Aktivierung der Smart Card-Anmeldung für ICA-Verbindungen aus.
<b>Verschlüsselungsstufe</b>	Wählen Sie diese Option zum Einstellen einer Verschlüsselungsebene aus. Wählen Sie im Dropdownmenü eine beliebige der folgenden Verschlüsselungsebenen aus: <ul style="list-style-type: none"> <li>• Einfach</li> <li>• RC5 (128 Bit – Nur Anmeldung)</li> <li>• RC5 (40 Bit)</li> <li>• RC5 (56 Bit)</li> <li>• RC5 (128 Bit)</li> </ul>
<b>Fenstergröße</b>	Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Standard</li> <li>• Nahtlos</li> <li>• 640 x 480</li> <li>• 1024 x 768</li> <li>• 800 x 600</li> <li>• 1280 x 1024</li> <li>• 1600 x 1200</li> <li>• Vollbild</li> </ul>

Option	Beschreibung
<b>Bildschirm-Farbtiefe</b>	Wählen Sie diese Option aus, um die Bildschirm-Farbtiefe festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· 64 K</li> <li>· 256</li> <li>· 16 M</li> </ul>
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung zur Citrix-Sitzung wiederherstellt.
<b>Verzögerung vor erneutem Verbindungsversuch</b>	Wählen Sie diese Option aus, um die Zeit in Sekunden festzulegen, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.
<b>Anmeldung durch Einfügen mit Mittelstaste</b>	Wählen Sie diese Option aus, um die Anmeldung durch Einfügen mit der Mittelstaste zuzulassen. Auf diese Weise können Sie die Aktion der Maustaste in einer Unix-Umgebung steuern.  In einer Unix-Umgebung führt die mittlere Maustaste die gleiche Einfügefunktion aus wie die Tastenkombination Strg+V in Windows.  <b>i</b>   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Ping vor Verbindung</b>	Wählen Sie diese Option, um Ping zu aktivieren. Bei nicht veröffentlichten Anwendungsverbindungen wird vor der Verbindung ein Ping (ICMP) an den Hostserver gesendet, um sicherzustellen, dass der Host erreichbar ist.  <b>i</b>   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Komprimierung</b>	Wählen Sie diese Option aus, um Komprimierung während der Sitzung zu aktivieren.  <b>i</b>   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>

## Konfigurieren von Remote-Verbindungseinstellungen – VMware


Verwenden Sie diese Seite zum Erstellen einer VMware View Broker-Verbindung.

**Tabelle 206. Konfigurieren von Remote-Verbindungseinstellungen – VMware**

Option	Beschreibung
<b>Benutzername</b>	Wählen Sie diese Option aus, um den Benutzernamen mit dem Domännennamen anzugeben.  <b>i</b>   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Nicht authentifizierter Zugriff</b>	Wählen Sie diese Option, um einen nicht authentifizierten Zugriff zu ermöglichen. Wählen Sie diese Option, um einen nicht authentifizierten Zugriff zu ermöglichen.

Option	Beschreibung
	<p><b>i</b>   <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>Ping vor Verbindung</b>	<p>Wählen Sie diese Option, um den Ping mit dem Parameter <b>Ping</b> zu aktivieren. Bei nicht veröffentlichten Anwendungsverbindungen wird vor der Verbindung ein Ping (ICMP) an den Hostserver gesendet, um sicherzustellen, dass der Host erreichbar ist.</p> <p><b>i</b>   <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>MMR aktivieren</b>	<p>Wählen Sie diese Option, um MMR in den Verbindungseinstellungen von VMWare View zu aktivieren.</p> <p><b>i</b>   <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>Interaktiver Modus</b>	<p>Wählen Sie diese Option aus, um den interaktiven Verbindungsmodus zu aktivieren.</p> <p><b>i</b>   <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>SSL-Protokoll</b>	<p>Wählen Sie diese Option aus, um die Verschlüsselungsliste so zu konfigurieren, dass die Verwendung bestimmter kryptographischer Protokolle vor dem Aufbau einer verschlüsselten SSL-Verbindung eingeschränkt wird.</p> <p>Der Standardwert für Horizon Client 3.5 und höher ist          TLSv1.0:TLSv1.1:TLSv1.2.</p> <p>Der Standardwert für Horizon Client 3.4 und niedriger ist          TLSv1.0:TLSv1.1.</p> <p><b>i</b>   <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>SSL-Verschlüsselung</b>	<p>Wählen Sie diese Option aus, um die Verschlüsselungsliste so zu konfigurieren, dass die Verwendung bestimmter kryptographischer Algorithmen vor dem Aufbau einer verschlüsselten SSL-Verbindung eingeschränkt wird.</p> <p>Der Standardwert für Horizon Client 3.5 und höher ist          !aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH.</p> <p>Der Standardwert für Horizon Client 3.4 und niedriger ist          AES:!aNULL:@STRENGTH.</p> <p><b>i</b>   <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>Beenden bei Trennung der Verbindung deaktivieren</b>	<p>Wählen Sie diese Option, um die Auflistung der View-Desktops nach dem Abmelden der Sitzung zu deaktivieren.</p> <p><b>i</b>   <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>
<b>Verbindungsname</b>	<p>Wählen Sie diese Option aus, um einen Namen zur Identifizierung der Verbindung einzugeben.</p>

Option	Beschreibung
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option zum automatischen Starten der Verbindung, nachdem Sie sich angemeldet haben.
<b>VMWare Serveradresse</b>	Geben Sie den Hostnamen oder die IP-Adresse des VMware View-Servers ein.
<b>VMWare Serverportnummer</b>	Geben Sie die Portnummer des Hosts ein.
<b>Sichere Verbindung (SSL) verwenden</b>	Wählen Sie diese Option aus, um die SSL-Verbindung zu verwenden.
<b>Protokoll</b>	Wählen Sie diese Option aus, um <b>PCoIP</b> , <b>RDP</b> oder <b>Blast</b> als Protokoll auszuwählen.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein.
<b>Kennwort</b>	Geben Sie das Kennwort ein.
<b>Domänenname</b>	Geben Sie den Domännennamen ein.
<b>NLA aktivieren</b>	Mit dieser Option wird die Authentifizierung auf Netzwerkebene aktiviert. Wenn die Option <b>RDP</b> als Protokoll eingestellt ist, wird diese Option angezeigt.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein, wenn das PCoIP-Protokoll ausgewählt ist.
<b>Kennwort</b>	Geben Sie das Kennwort ein, wenn das PCoIP-Protokoll ausgewählt ist.
<b>Domainname</b>	Geben Sie den Domännennamen ein.
<b>Interaktiver Modus</b>	Wählen Sie diese Option aus, um den interaktiven Benutzermodus zu aktivieren.
<b>Server-URL/Hostfeld sperren</b>	Aktivieren Sie das Kontrollkästchen, um die Server-URL zu sperren.
<b>Sicherheitsmodus</b>	Wählen Sie diese Option aus, um den Sicherheitsmodus einzustellen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Niemals Verbindung zu nicht vertrauenswürdigen Servern herstellen</li> <li>• Vor Verbindung mit nicht vertrauenswürdigen Server warnen</li> <li>• Serveridentitäts-Zertifikate nicht überprüfen.</li> </ul>
<b>Vollbildschirm-Modus</b>	Wählen Sie diese Option zum Anzeigen der Remote-Sitzung im Vollbildschirm-Modus.
<b>Fenstergröße</b>	Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Alle Monitore verwenden</li> <li>• Vollbild</li> <li>• Großer Bildschirm</li> <li>• Kleiner Bildschirm</li> <li>• 1024 x 768</li> <li>• 800 x 600</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>640 x 480</li> </ul>
<b>Dropdown-Menüleiste für Vollbild deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren des Dropdownmenüs im Vollbildschirm-Modus.
<b>Diesen Desktop automatisch starten</b>	Wählen Sie diese Option, um den Namen des veröffentlichten Desktops anzugeben, der bei erfolgreicher Verbindung automatisch gestartet werden soll.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung zur VMware-Sitzung wiederherstellt.
<b>Verzögerung vor erneutem Verbindungsversuch</b>	<p>Geben Sie die Zeit in Sekunden an, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.</p> <p> <b>ANMERKUNG:</b> Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</p>




## Konfigurieren von Remote-Verbindungseinstellungen – RDP

Verwenden Sie diese Seite zum Erstellen einer RDP-Broker-Verbindung.

**Tabelle 207. Konfigurieren von Remote-Verbindungseinstellungen – RDP**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um den Namen für die Identifizierung der Verbindung einzugeben.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option zum automatischen Starten der Verbindung, nachdem Sie sich angemeldet haben.
<b>Serveradresse</b>	Geben Sie den Servernamen oder die IP-Adresse an.
<b>Smart Card-Anmeldung</b>	Mit dieser Option wird die Smart Card-Authentifizierung aktiviert.
<b>Authentifizierung auf Netzwerkebene (NLA) verwenden</b>	Mit dieser Option wird die Authentifizierung auf Netzwerkebene aktiviert.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein.
<b>Kennwort</b>	Geben Sie das Kennwort ein.
<b>Domainname</b>	Geben Sie den Domännennamen ein.
<b>Fenstergröße</b>	<p>Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>Standard</li> <li>640 x 480</li> <li>1024 x 768</li> <li>800 x 600</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>• 1280 x 1024</li> <li>• 1600 x 1200</li> <li>• Vollbild</li> </ul>
<b>Alle Drucker weiterleiten</b>	Wählen Sie diese Option, um alle Drucker an die Remoteverbindung weiterzuleiten.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung zur RDP-Sitzung wiederherstellt.
<b>Verzögerung vor erneutem Verbindungsversuch</b>	Geben Sie die Zeit in Sekunden an, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.
<b>Alle Laufwerke einem einzelnen Freigabenamen zuordnen – WyseUSB</b>	Wählen Sie diese Option aus, um alle Geräte einem einzelnen freigegebenen Namen zuzuordnen: WyseUSB.
<b>Bildschirm-Farbtiefe</b>	Wählen Sie aus der Dropdown-Liste die Bildschirm-Farbtiefe aus.
<b>H.264-Dekodierungssupport aktivieren</b>	Wählen Sie diese Option, um die H.264-Dekodierungsunterstützung für Remote-Desktop-Verbindungen zu aktivieren.
<b>UDP-Netzwerkbetrieb aktivieren</b>	Wählen Sie diese Option, um das UDP-Protokoll als bevorzugtes Transportprotokoll für die Datenübertragung zu aktivieren.
<b>Ping vor Verbindung</b>	Wählen Sie diese Option, um Ping zu aktivieren. Bei nicht veröffentlichten Anwendungsverbindungen wird vor der Verbindung ein Ping (ICMP) an den Hostserver gesendet, um sicherzustellen, dass der Host erreichbar ist.  <b> ⓘ   ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Bei Trennung benachrichtigen</b>	Wählen Sie diese Option, um die Trennung zu melden.  <b> ⓘ   ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Komprimierung</b>	Wählen Sie diese Option, um das Signal zu komprimieren.  <b> ⓘ   ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Niedrige Bandbreite</b>	Wählen Sie diese Option, um den Wert der Bandbreite zu verringern.  <b> ⓘ   ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Tastaturereignisse erfassen</b>	Wählen Sie diese Option, um das Erfassen des Tastaturereignisses in jeder direkten RDP-Verbindungssitzung zu aktivieren (wird von VMware View Broker nicht unterstützt).  <b> ⓘ   ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
<b>Töne</b>	Sie können den Toneffekt über den Ton-Parameter aktivieren oder deaktivieren.  Aus: Töne deaktivieren  Lokal: Töne für lokalen Rechner aktivieren (Standard)

Option	Beschreibung
	Remote: Töne für den Remote-Computer aktivieren   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
Verschlüsselungsstufe	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Wenn der Wert "Keine" ist, dann wird keine Verschlüsselung verwendet.   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>
Geschwindigkeitsstufe	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Diese Option steuert die Leistung je nach Bandbreite.   <b>ANMERKUNG: Diese Option wird auf Thin Clients mit ThinLinux 2.1 und höher unterstützt.</b>

**Tabelle 208. Konfigurieren von RD-Gateway-Einstellungen**

Option	Beschreibung
RD-Gateway-Einstellungen verwenden	Wählen Sie diese Option zum Verwenden der RD-Gateway-Einstellungen. Die Optionen <b>RD-Server</b> und <b>Remote-Desktop-Anmeldeinformationen für RD-Gateway verwenden</b> werden angezeigt.
RD-Server	Wählen Sie diese Option zur Angabe der Hostadresse des RD-Gateways aus.
Remote-Desktop-Anmeldeinformationen für RD-Gateway verwenden	Wählen Sie diese Option zur Verwendung der Remote Desktop Anmeldeinformationen für das RD-Gateway aus.

## Konfigurieren von Remote-Verbindungseinstellungen – Browser

Verwenden Sie diese Seite zum Konfigurieren der Browser-Remote-Verbindungen.

**Tabelle 209. Konfigurieren von Remote-Verbindungseinstellungen – Browser**

Option	Beschreibung
Verbindungsname	Geben Sie den Namen für die Identifizierung der Verbindung ein.
Verbindung bei Anmeldung automatisch starten	Wählen Sie diese Option zum automatischen Starten der Verbindung während der Anmeldung.
URL	Geben Sie die Start-URL an.
Kioskmodus	Wählen Sie diese Option aus, um den Kioskmodus zu aktivieren.
RC Bedienfeld deaktivieren in Kioskmodus	Wählen Sie diese Option zum Deaktivieren des RC-Panels im Kioskmodus.
Fenstergröße	Wählen Sie diese Option aus, um eine Fenstergröße festzulegen. Wählen Sie im Dropdownmenü die gewünschte Größe des Fensters.

Option	Beschreibung
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, damit der Thin Client automatisch die Verbindung des Browsers wiederherstellt.
<b>Verzögerung vor erneutem Verbindungsversuch</b>	Geben Sie die Zeit in Sekunden an, um die ein erneuter Verbindungsversuch verzögert werden soll. Wenn Sie das Kontrollkästchen <b>Automatisch neu verbinden</b> wählen, wird diese Option angezeigt.

## Erweiterte Einstellungen konfigurieren

Konfigurationen können auf das ThinLinux Client-Gerät durch die Eingabe der INI-Parameter in den **Erweiterten Optionen** angewendet werden. Dell empfiehlt, dass Sie keine INI-Parameter für Richtlinien einschließen, die bereits in anderen Optionen konfiguriert sind. Die Kennwortkodierung und -Verschlüsselung wird nicht auf die Kennwortparameter angewendet.

**Tabelle 210. Erweiterte Einstellungen konfigurieren**

Option	Beschreibung
<b>Keine globale INI</b>	Wenn diese Option ausgewählt ist, wird der globale INI-Parameter nicht vom Dateiserver heruntergeladen.  Geben Sie die INI-Parameter von Zeile 1 bis Zeile 20 für die Thin Clients ein.

## Geräteinformationen konfigurieren

Verwenden Sie die Seite **Geräteinformationen**, um die Gerätedetails anzuzeigen.

**Tabelle 211. Geräteinformationen konfigurieren**

Option	Beschreibung
<b>Standort</b>	Geben Sie den Gerätestandort ein.
<b>Kontakt</b>	Geben Sie die Kontaktdaten des Geräts ein.
<b>Benutzerdefiniert 1 bis 3</b>	Geben Sie benutzerdefinierte Werte ein.

## Wyse 3040 Thin Client BIOS-Einstellungen konfigurieren

Verwenden Sie diese Seite, um die BIOS-Einstellungen für Wyse 3040 Thin Clients zu konfigurieren.

**Tabelle 212. Konfigurieren der allgemeinen Einstellungen**



Option	Beschreibung
<b>Gerätehinweise</b>	Geben Sie die Gerätehinweise in das entsprechende Feld ein. Zum Beispiel das Ownership Tag der Property.

**Tabelle 213. Konfigurieren der Systemeinstellungen**

Option	Beschreibung
<b>UEFI-Netzwerkstapel aktivieren</b>	Markieren Sie dieses Kontrollkästchen, um den UEFI-Netzwerkstapel zu aktivieren. Die Netzwerkprotokolle sind installiert

Option	Beschreibung
	und die pre-OS- und early-OS-Netzwerkfunktionen werden für die Verwendung einer aktivierten NICs verfügbar gemacht.
<b>Integriertes NIC</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
<b>Audio</b>	Wählen Sie diese Option aus, um das Audiogerät zu aktivieren.

**Tabelle 214. Konfigurieren der USB-Einstellungen**

Option	Beschreibung
<b>Enable USB Boot Support (USB-Start-Unterstützung aktivieren)</b>	Wählen Sie dieses Kontrollkästchen aus, um das USB-Startsetup zu aktivieren. Ermöglicht das Starten von jedem USB-Massenspeichergerädetyp.
<b>Vordere USB-Anschlüsse aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät an diesem Port aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, wird das Gerät auch für das Betriebssystem verfügbar gemacht. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System kein dort angeschlossenes Gerät erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>
<b>Dual-USB-2.0-Anschlüsse hinten links aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät an diesem Port aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, wird das Gerät auch für das Betriebssystem verfügbar gemacht. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System kein dort angeschlossenes Gerät erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>

**Tabelle 215. Konfigurieren der WLAN-Einstellungen**

Option	Beschreibung
<b>Wireless-Gerät aktivieren</b>	Wählen Sie das Kontrollkästchen zum Aktivieren der internen Wireless-Geräte.

**Tabelle 216. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
<b>Aktualisierung der UEFI-Kapsel-Firmware</b>	Wählen Sie das Kontrollkästchen aus, um das BIOS über die Aktualisierung der UEFI-Kapsel-Firmware zu aktualisieren.

**Tabelle 217. Konfigurieren der Einstellungen für das BIOS-Administratorkennwort**

Option	Beschreibung
<b>Administratorkennwort aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, um das BIOS-Administratorkennwort zu aktivieren. Erfolgreiche Änderungen an diesem Kennwort werden sofort wirksam.
<b>Administratorkennwort</b>	Geben Sie ein neues BIOS-Administratorkennwort ein. Diese Option ist nur verfügbar, wenn Sie das Kontrollkästchen <b>Administratorkennwort aktivieren</b> auswählen.

**Tabelle 218. Konfigurieren der Energieverwaltungs-Einstellungen**

Option	Beschreibung
<b>USB Wake Support</b>	Wählen Sie das Kontrollkästchen, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird.
<b>Wake On LAN</b>	Wählen Sie aus der Dropdownliste eine Option aus, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird. Sie können einen Thin Client dazu bringen, aus dem ausgeschalteten Zustand über ein LAN-Signal oder ein Wireless-LAN-Signal hochgefahren zu werden.
<b>AC-Wiederherstellung</b>	Wählen Sie aus der Dropdownliste eine Option aus, um anzugeben, wie das System reagieren muss, wenn der Netzstrom wiederhergestellt wurde.

**Tabelle 219. Konfigurieren der Einstellungen für das automatische Einschalten**

Option	Beschreibung
<b>Automatische Einschaltung</b>	Wählen Sie aus der Dropdownliste die Tageszeit aus, zu der das System automatisch eingeschaltet werden soll

**Tabelle 220. Konfigurieren der Einstellungen der POST-Funktionsweise**

Option	Beschreibung
<b>Numlock-LED</b>	Aktivieren Sie das Kontrollkästchen, um die NumLock-LED-Anzeige anzuschalten, wenn das System neu gestartet wird.
<b>Tastaturfehler</b>	Wählen Sie das Kontrollkästchen, um mit der Tastatur in Zusammenhang stehende Fehler beim Neustarten des Systems anzuzeigen.
<b>Schnellstart</b>	Wählen Sie eine Option aus der Dropdownliste aus, um die Geschwindigkeit des Neustartvorgangs zu steigern.
<b>BIOS-POST-Zeit verlängern</b>	Wählen Sie aus der Dropdownliste eine Verzögerungszeit, um die Post-Statusmeldungen ansehen zu können.

**Tabelle 221. Konfigurieren des Neustart-Zeitplans**

Option	Beschreibung
<b>Neustartoption</b>	<p>Einige BIOS-Einstellungen machen einen Systemneustart erforderlich. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Sofort neu starten: Das System startet sofort neu.</li> <li>• Später neu starten: Wählen Sie <b>Neustart-Stunde</b> und <b>Neustart-<math>\langle 3 \rangle</math>Minute<math>\langle /3 \rangle</math></b> aus, um den Zeitpunkt für den Systemneustart festzulegen,</li> <li>• Keinen Neustart durchführen: Das System wird nicht neu gestartet.</li> </ul>

# Konfiguration der BIOS-Einstellungen für Wyse 5070 Thin-Client mit ThinLinux

Verwenden Sie die Seite für die **BIOS**-Einstellungen, um die BIOS-Einstellungen für den Wyse 5070 Thin Client mit ThinLinux zu konfigurieren.

**Tabelle 222. Konfigurieren der allgemeinen Einstellungen**

Option	Beschreibung
Gerätehinweise	Geben Sie die Gerätehinweise in das entsprechende Feld ein. Zum Beispiel das Ownership Tag der Property.

**Tabelle 223. Konfigurieren der Systemeinstellungen**

Option	Beschreibung
Audio aktivieren	Markieren Sie dieses Kontrollkästchen, um das Audiogerät zu aktivieren.
UEFI-Netzwerkstapel aktivieren	Markieren Sie dieses Kontrollkästchen, um den <b>UEFI-Netzwerkstapel</b> zu aktivieren. Für die aktivierten NICS sind die Netzwerkprotokolle installiert und die pre-OS- und early-OS-Netzwerkfunktionen sind verfügbar.
Integriertes NIC	<p>Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Diese Option steuert den integrierten LAN-Controller.</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> Das interne LAN ist deaktiviert und für das Betriebssystem nicht sichtbar, wenn es keine IP-Adresse besitzt.</li> <li>• <b>Aktiviert:</b> Das interne LAN ist aktiviert.</li> <li>• <b>Mit PXE aktiviert</b> – Das interne LAN ist aktiviert mit PXE-Start.</li> </ul> <p><b>ANMERKUNG:</b> Dell empfiehlt, keine Deaktivierung des integrierten NIC und des integrierten NIC 2 vorzunehmen.</p>
Paralleler Port	<p>Wählen Sie aus der Dropdownliste die Option aus, mit der bestimmt wird, wie die parallele Schnittstelle an der Docking-Station funktioniert.</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> Port ist deaktiviert.</li> <li>• <b>AT:</b> Port ist für IBM AT-Kompatibilität konfiguriert.</li> <li>• <b>PS2:</b> Port ist für IBM PS2-Kompatibilität konfiguriert.</li> <li>• <b>ECP:</b> Port ist für das ECP-Protokoll (Extended Capability Port) konfiguriert.</li> </ul> <p><b>ANMERKUNG:</b> Diese Option steht für das erweiterte Gehäuse zur Verfügung, wenn die Add-on-Karte installiert ist.</p>
Serielle Schnittstelle 1	<p>Wählen Sie aus der Dropdownliste die Option aus, mit der man ermittelt, wie die serielle Schnittstelle an der Docking-Station funktioniert. Diese Option ermöglicht es Ihnen, Ressourcenkonflikte zwischen Geräten zu verhindern, indem Sie die Adresse des Ports deaktivieren oder neu zuordnen.</p> <ul style="list-style-type: none"> <li>• <b>Deaktiviert:</b> Port ist deaktiviert.</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>• <b>COM1</b> – Der Port wird für die Adresse 3F8h mit IRQ 4 konfiguriert.</li> <li>• <b>COM2</b> – Der Port wird für die Adresse 2F8h mit IRQ 3 konfiguriert.</li> <li>• <b>COM3</b> – Der Port wird für die Adresse 3F8h mit IRQ 4 konfiguriert.</li> <li>• <b>COM4</b> – Der Port wird für die Adresse 2F8h mit IRQ 3 konfiguriert.</li> </ul>

**Tabelle 224. Konfigurieren der USB-Einstellungen**

Option	Beschreibung
<b>USB-Start-Unterstützung aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, um das USB-Startsetup zu aktivieren. Ermöglicht das Starten von jedem USB-Massenspeichergerätetyp.
<b>Vordere USB-Anschlüsse aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät am vorderseitigen USB-Anschluss aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, wird das Gerät vom Betriebssystem erkannt. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System das am vorderseitigen USB-Anschluss angeschlossene Gerät nicht erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>
<b>Hintere USB-Anschlüsse aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, damit das Gerät am rückseitigen USB-Anschluss aktiviert wird. Wenn Sie dieses Kontrollkästchen auswählen, wird das Gerät vom Betriebssystem erkannt. Wenn der USB-Anschluss jedoch deaktiviert ist, kann das System das am rückseitigen USB-Anschluss angeschlossene Gerät nicht erkennen.   <b>ANMERKUNG: Die USB-Tastatur und -Maus funktionieren im BIOS-Setup ungeachtet dieser Einstellung immer.</b>

**Tabelle 225. Konfigurieren der Sicherheitseinstellungen**

Option	Beschreibung
<b>UEFI-Kapsel-Firmwareaktualisierung aktivieren</b>	Wählen Sie das Kontrollkästchen aus, um das BIOS über die Aktualisierung der UEFI-Kapsel-Firmware zu aktualisieren.
<b>Sperre für Administrator-Setup aktivieren</b>	Aktivieren Sie dieses Kontrollkästchen, um Benutzer vom Aufrufen des Setups abzuhalten, wenn ein Administratorenkennwort festgelegt worden ist.

**Tabelle 226. Konfigurieren der Energieverwaltungs-Einstellungen**

Option	Beschreibung
<b>Wake On LAN</b>	Wählen Sie aus der Dropdownliste eine Option aus, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird. Sie können einen Thin Client dazu bringen, aus

Option	Beschreibung
	dem ausgeschalteten Zustand über ein LAN-Signal hochgefahren zu werden.
<b>AC-Wiederherstellung</b>	Wählen Sie aus der Dropdownliste eine Option aus, um anzugeben, wie das System funktionieren sollte, wenn der Netzstrom wiederhergestellt wurde.
<b>Unterstützung für Reaktivieren bei USB-Anschluss</b>	Wählen Sie das Kontrollkästchen, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird.

**Tabelle 227. Konfigurieren der Einstellungen der POST-Funktionsweise**

Option	Beschreibung
<b>Numlock-LED aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um die NumLock-LED-Anzeige anzuschalten, wenn das System neu gestartet wird.
<b>Enable Keyboard Error Detection (Tastaturfehlererkennung aktivieren)</b>	Aktivieren Sie das Kontrollkästchen, damit Tastaturfehlern beim Neustart im System angezeigt werden können.
<b>Schnellstart</b>	Wählen Sie eine Option aus der Dropdownliste aus, um die Geschwindigkeit des Neustartvorgangs zu steigern.
<b>BIOS-POST-Zeit verlängern</b>	Wählen Sie aus der Dropdownliste eine Verzögerungszeit, um die Post-Statusmeldungen ansehen zu können.

**Tabelle 228. Konfigurieren der WLAN-Einstellungen**

Option	Beschreibung
<b>WLAN/WiGig</b>	Wählen Sie dieses Kontrollkästchen zum Aktivieren der internen Wireless-Geräte.
<b>Bluetooth</b>	Markieren Sie dieses Kontrollkästchen, um Bluetooth-Geräte zu aktivieren.

**Tabelle 229. Konfigurieren des BIOS-Administratorkennworts**

Option	Beschreibung
<b>Administrator-Kennwort aktivieren</b>	Wählen Sie dieses Kontrollkästchen aus, um das BIOS-Administratorkennwort zu aktivieren. Wenn Sie dieses Kennwort ändern, werden die Änderungen sofort angewendet.
<b>Administrator-Kennwort</b>	Geben Sie ein neues BIOS-Administratorkennwort ein. Diese Option ist nur verfügbar, wenn Sie das Kontrollkästchen <b>Administrator-Kennwort aktivieren</b> auswählen.

**Tabelle 230. Konfigurieren der Einstellungen für das automatische Einschalten**

Option	Beschreibung
<b>Auto On Time (Automatisch pünktlich)</b>	Wählen Sie aus der Dropdownliste die Tageszeit aus, zu der das System automatisch eingeschaltet werden soll.

**Tabelle 231. Konfigurieren der Neustart-Zeitplaneinstellungen**

Option	Beschreibung
<b>Neustartoption</b>	<p>Einige BIOS-Einstellungen machen einen Systemneustart erforderlich. Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Sofort neu starten: Das System startet sofort neu.</li> <li>• Später neu starten: Wählen Sie <b>Neustart-Stunde</b> und <b>Neustart-<math>\langle 3 \rangle</math>Minute<math>\langle /3 \rangle</math></b> aus, um den Zeitpunkt für den Systemneustart festzulegen,</li> <li>• Nicht neu starten: Das System wird nicht neu gestartet.</li> </ul>

## Konfigurieren der globalen Browsereinstellungen

Auf dieser Seite können Sie die Webbrowser-Einstellungen von Google Chrome und Mozilla Firefox für Thin Clients mit ThinLinux 2.1 und höheren Versionen konfigurieren.

**Tabelle 232. Konfiguration von Mozilla Firefox-Browsereinstellungen**

Option	Beschreibung
<b>Lesezeichen ausblenden</b>	Wählen Sie diese Option, um das Lesezeichensymbol auszublenden.
<b>Suchleiste ausblenden</b>	Wählen Sie diese Option, um das Symbol der Suchleiste auszublenden.
<b>Verlauf ausblenden</b>	Wählen Sie diese Option, um das Symbol für Öffnen des Menüs und den Verlauf auszublenden.
<b>Browserdaten löschen</b>	Wählen Sie diese Option, um die Browserdaten wie Cache, Cookies, Sitzungsdaten usw. zu löschen.
<b>Proxy-Methode</b>	<p>Wählen Sie aus der Dropdown-Liste Ihre bevorzugte Proxy-Methode. Dies sind die möglichen Optionen:</p> <ul style="list-style-type: none"> <li>• Kein</li> <li>• AutoDetect</li> <li>• Manuell</li> <li>• Proxy-Konfiguration</li> <li>• System-Proxy</li> </ul> <p><b>ANMERKUNG:</b></p> <ul style="list-style-type: none"> <li>• Wenn Sie die Einstellungen konfigurieren und anwenden, werden Sie aufgefordert, den Firefox-Browser auf dem Thin Client zu schließen.</li> <li>• Um die alten Konfigurationen zu löschen, müssen Sie in der Dropdown-Liste <b>Proxy-Methode</b> die Option <b>Keine</b> auswählen und die Konfiguration übertragen.</li> </ul>
<b>Multi-Proxy-Einstellungen</b>	Verwenden Sie diese Option, um eine oder mehrere Proxy-Server-Einstellungen zu konfigurieren. Diese Option wird aktiviert, wenn Sie als Proxy-Methode <b>Manuell</b> auswählen.
<b>Kein Proxy</b>	Verwenden Sie diese Option, um die Ausschlussliste für Proxy-Einstellungen aufzurufen. Diese Option wird aktiviert, wenn Sie als Proxy-Methode <b>Manuell</b> auswählen.
<b>Socks-Version</b>	Verwenden Sie diese Option, um die SOCKS-Serveradresse einzugeben, um im Namen eines Clients eine TCP-Verbindung zu

Option	Beschreibung
	einem anderen Server herzustellen. Diese Option wird aktiviert, wenn Sie als Proxy-Methode <b>Manuell</b> auswählen.
<b>Proxy-Konfiguration-URL</b>	Verwenden Sie diese Option, um die URL der Proxy-Konfiguration einzugeben. Diese Option wird aktiviert, wenn Sie als Proxy-Methode <b>Proxy-Konfiguration</b> auswählen.


**Tabelle 233. Konfigurieren von Google Chrome-Einstellungen**

Option	Beschreibung
<b>Lesezeichen ausblenden</b>	Wählen Sie diese Option zum Ausblenden der Lesezeichen-Symbolleiste.
<b>Downloads ausblenden</b>	Wählen Sie diese Option zum Ausblenden der Option "Downloads".
<b>Verlauf ausblenden</b>	Wählen Sie diese Option zum Ausblenden der Option "Verlauf".
<b>Browserdaten löschen</b>	Wählen Sie diese Option, um die Browserdaten wie Cache, Cookies, Sitzungsdaten usw. zu löschen.

## Konfigurieren von Proxy-Einstellungen

Auf dieser Seite können Sie systemweite Proxy-Einstellungen für Thin Clients mit ThinLinux 2.1 und höheren Versionen konfigurieren.

**Tabelle 234. Konfigurieren systemweiter Proxy-Einstellungen**

Option	Beschreibung
<b>Proxy-Methode</b>	Wählen Sie aus dem Dropdown-Menü die Proxy-Methode aus, die Sie verwenden möchten. Die verfügbaren Proxy-Methoden sind: <ul style="list-style-type: none"> <li>• Kein</li> <li>• Manuell</li> <li>• Automatisch</li> </ul> <p> <b>ANMERKUNG:</b> Diese Einstellung wird auf Thin Clients mit ThinLinux Version 2.1 und höher unterstützt.</p>
<b>URL des automatischen Proxy</b>	Geben Sie die Konfigurations-URL ein. Diese Option wird aktiviert, wenn Sie als <b>Proxy-Methode Automatisch</b> auswählen.
<b>Multi-Proxy-Einstellungen</b>	Verwenden Sie diese Option, um eine oder mehrere Proxy-Server-Einstellungen zu konfigurieren. Diese Option wird aktiviert, wenn Sie als <b>Proxy-Methode Manuell</b> auswählen. Klicken Sie auf <b>Element hinzufügen</b> und konfigurieren Sie die folgenden Proxy-Protokolle: <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• FTP</li> <li>• Socks</li> </ul>

## Bearbeiten von Teradici-Richtlinieneinstellungen

Gehen Sie folgendermaßen vor, um die Teradici-Richtlinieneinstellungen zu bearbeiten:

- 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 **Teradici**.

Die Seite **Teradici** wird angezeigt. Die Teradici Thin Client-Richtlinieneinstellungen umfassen die folgenden Optionen:

- Zeitzone
- Sprache
- Unternehmenslogo
- Video
- Power (Stromverbrauch)
- Security (Sicherheit)
- Firmware-Upgrade
- Remote-Verbindung

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

## Konfigurieren von Zeitzoneneinstellungen

Verwenden Sie die Seite **Zeitzone** zum Konfigurieren der Zeitzoneneinstellungen für den Teradici Thin Client.

**Tabelle 235. Konfigurieren von Zeitzoneneinstellungen**

Option	Beschreibung
<b>NTP aktivieren</b>	Aktivieren Sie das Kontrollkästchen zum Aktivieren der Network Time Protocol- (NTP-)Funktion.
<b>NTP-Server</b>	Wählen Sie diese Option aus, um den NTP-Hostnamen einzugeben. Die Hostnamen müssen IP-Adressen oder FQDNs sein.
<b>Abfrageintervall</b>	Geben Sie das Abfrageintervall in Minuten, Stunden, Tagen oder Wochen ein. Das Abfrageintervall ist die maximale Zeitdauer, die zwischen dem Zeitpunkt, an dem der Router eine Anfrage sendet, und dem Zeitpunkt, an dem er eine Antwort vom Host erhält, vergehen darf.
<b>Zeitzone</b>	Wählen Sie aus der Dropdownliste die Zeitzone des Systems aus.
<b>Sommerzeit aktivieren</b>	Aktivieren Sie das Kontrollkästchen zum Aktivieren der Sommerzeit-Funktion.

## Konfigurieren von Spracheinstellungen

Verwenden Sie die Seite **Sprache** zum Konfigurieren der Spracheinstellungen.

**Tabelle 236. Konfigurieren von Spracheinstellungen**

Option	Beschreibung
<b>Sprache</b>	Wählen Sie aus der Dropdownliste „Sprache“ die Sprache für die Benutzeroberfläche des Objekt-Speichergeräts (OSD) aus.
<b>Keyboard Layout (Tastaturlayout)</b>	Wählen Sie aus der Dropdownliste „Tastaturlayout“ das Layout für das OSD aus.

# Konfigurieren von Firmenlogo-Einstellungen

Verwenden Sie die Seite **Firmenlogo** zum Konfigurieren der Firmenlogo-Einstellungen.

**Tabelle 237. Konfigurieren von Firmenlogo-Einstellungen**

Option	Beschreibung
<b>Logodatei</b>	<p>Wählen Sie aus der Dropdownliste die gewünschte Logodatei aus. Die Teradici-OSD-Logodateien auf der Seite <b>Datei-Repository-Bestand</b> werden geladen.</p> <p><b>ANMERKUNG:</b> Das Logo-Bild muss eine 24-bmp-Bitmap-Datei sein, die nicht größer als 256 x 24 Pixel sein sollte. Ein Bild mit abweichenden Eigenschaften wird nicht oder falsch angezeigt.</p>
<b>Logo für Ansichtsbanner verwenden</b>	<p>Aktivieren Sie das Kontrollkästchen für das Logo-Banner, das Sie anzeigen möchten.</p>

# Konfigurieren von Videoeinstellungen

Verwenden Sie die Seite **Video** zum Konfigurieren der Videoeinstellungen.

**Tabelle 238. Konfigurieren von Videoeinstellungen**

Option	Beschreibung
<b>Mindestens erforderliche Bildqualität</b>	<p>Ermöglicht das Ändern der Bildqualität und Bildwiederholrate bei begrenzter Netzwerkbandbreite. Einige Anwendungsfälle erfordern möglicherweise eine niedrigere Bildqualität bei höherer Bildwiederholrate, andere erfordern qualitativ hochwertige Bilder mit einer niedrigeren Bildwiederholrate. In Umgebungen mit einer begrenzten Netzwerkbandbreite wählen Sie <b>Reduziert</b> aus, um höhere Bildwiederholraten zu ermöglichen. Wählen Sie „Störungsfrei“, um eine höhere Bildqualität zu ermöglichen. Wenn die Netzwerkbandbreite nicht begrenzt ist, hält das PCoIP-System eine störungsfreie Qualität aufrecht, unabhängig von den Parametern für die mindestens erforderliche Bildqualität. Hinweis: Die anfängliche maximal zulässige Bildqualität muss größer oder gleich der mindestens erforderlichen Bildqualität sein.</p>
<b>Maximal zulässige Bildqualität</b>	<p>Wählen Sie „Reduziert“ zur Reduzierung der Netzwerkbandbreitenspitzen, die durch Änderungen des Bildschirminhalts verursacht werden. Hierdurch werden Bilder mit geringerer Bildqualität erzeugt. Wählen Sie „Störungsfrei“, um Bilder mit höherer Bildqualität zu erzeugen. Hierbei werden auch höhere Bandbreitenspitzen erzeugt. Dieser Parameter schränkt die anfängliche Qualität auf dem ersten Bildschirmbild bei Änderungen des Bildschirminhalts ein. Unveränderte Bereiche des Bildes werden unabhängig von diesem Parameter in einem verlustfreien Zustand aufgebaut. Hinweis: Die anfängliche maximal zulässige Bildqualität</p>

Option	Beschreibung
	muss größer oder gleich der mindestens erforderlichen Bildqualität sein.
<b>Lokalen Cursor aktivieren</b>	Wenn diese Option aktiviert ist, zeigt der Tera2PCoIP Zero-Client immer den lokalen Cursor an. Wenn diese Option deaktiviert ist, wird der lokale Cursor nur dann angezeigt, wenn der Host dies anfordert oder eine lokale Maus angeschlossen wird.

## Konfigurieren der Energieeinstellungen

Verwenden Sie die Seite **Energie** zum Konfigurieren der Energieeinstellungen.

**Tabelle 239. Konfigurieren der Energieeinstellungen**

Option	Beschreibung
<b>Zeitüberschreitung für OSD-Bildschirmschoner</b>	Hierbei handelt es sich um die Zeitspanne der Inaktivität auf dem Gerät. Sie können die Zeit in Sekunden eingeben. Nach dem Eingeben der Zeit versetzt das Gerät die angeschlossenen Bildschirme in den Energiesparmodus. Der Bereich geht von 10 bis 9999. Geben Sie die Zeit mit „0“ ein, um die Option zu deaktivieren.  <span>❗</span> <b>ANMERKUNG: Diese Funktion ist nur dann anwendbar, wenn das Gerät nicht in einer Sitzung ist.</b>
<b>Zeitüberschreitung zum Anhalten der Anzeige</b>	Hierbei handelt es sich um die Zeitspanne der Inaktivität auf dem Gerät. Sie können die Zeit in Sekunden eingeben. Nach dem Eingeben der Zeit versetzt das Gerät die angeschlossenen Bildschirme in den Energiesparmodus. Der Bereich geht von 10 bis 14400. Geben Sie die Zeit mit „0“ ein, um die Option zu deaktivieren.  <span>❗</span> <b>ANMERKUNG: Diese Funktion ist nur dann anwendbar, wenn das Gerät in einer Sitzung ist.</b>

## Konfigurieren der Sicherheitseinstellungen

Verwenden Sie die Seite **Sicherheit** zum Konfigurieren der Sicherheitseinstellungen.

**Tabelle 240. Hochladen eines Zertifikats**

Option	Beschreibung
<b>Zertifikate</b>	Aktivieren Sie das erforderliche Kontrollkästchen, um das Zertifikat hochzuladen. Deaktivieren Sie das Kontrollkästchen zum Löschen eines hochgeladenen Zertifikats. Die Liste der auf der Seite <b>Datei-Repository-Bestand</b> hochgeladenen Zertifikate wird angezeigt. Die Zertifikate werden nach dem Neustart des Geräts gelöscht. Sie können nur <b>.pem</b> -Dateien hochladen.

**Tabelle 241. USB-Geräteautorisierung**

Option	Beschreibung
<b>Autorisierte/nicht autorisierte Geräte nach Klasse</b>	Wählen Sie aus der Dropdownliste <b>Status</b> und <b>Geräteklasse</b> die gewünschte Option aus. Basierend auf der Klasse können Sie ein USB-Gerät autorisieren oder seine Autorisierung aufheben. Klicken Sie auf die Option <b>Klasse hinzufügen</b> zum Hinzufügen von weiteren Klassen. Klicken Sie auf das Symbol – zum Entfernen einer Klasse.

**Tabelle 242. Erweiterte Konfiguration**

Option	Beschreibung
<b>Administrative Webschnittstelle aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um die Schnittstelle der Verwaltungskonsole zu aktivieren. Falls diese Funktion aktiviert ist, kann die PCoIP-Verwaltungskonsole nicht auf den Tera2 PCoIP Zero-Client zugreifen oder diesen verwalten.
<b>Wake-on-LAN aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird. Sie können einen Thin Client dazu bringen, aus dem ausgeschalteten Zustand über ein LAN-Signal hochgefahren zu werden.
<b>Einschalten nach Stromausfall aktivieren</b>	Aktivieren Sie das Kontrollkästchen, um zuzulassen, dass der Thin Client aus dem ausgeschalteten Zustand hochgefahren wird, wenn die Stromversorgung aktiviert wird.
<b>Benutzername speichern</b>	Aktivieren Sie das Kontrollkästchen, um den zuletzt eingegebenen Benutzernamen automatisch auszufüllen.
<b>Sicherheitseinstellungen</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Die verfügbaren Optionen sind: <ul style="list-style-type: none"> <li>· Niedrig</li> <li>· Mittel</li> <li>· Hoch</li> </ul>

**Tabelle 243. Administratorkennwort**

Option	Beschreibung
<b>Administrator Password</b>	Geben Sie ein neues Administratorkennwort für die administrative Webschnittstelle (AWI) und die lokale OSD-Schnittstelle ein.

## Upgrade der Firmware-Einstellungen

Verwenden Sie die Seite **Firmware-Upgrade** zum Upgraden der Firmware-Einstellungen.

**Tabelle 244. Upgrade der Firmware-Einstellungen**

Option	Beschreibung
<b>Live-Upgrade aktivieren</b>	Wählen Sie diese Option aus, um den Live-Upgrade-Vorgang zu aktivieren. Diese Funktion erlaubt es Ihnen, die Firmware herunterzuladen und sofort nach dem Herunterladen anzuwenden. Das System startet automatisch neu und die Änderungen an <b>Live-Upgrade aktivieren</b> werden angewendet. Wenn Sie diese Funktion

Option	Beschreibung
	deaktivieren, wird die Firmware heruntergeladen, jedoch nicht installiert. Das System wartet bis zum nächsten Neustart, um die Firmware anzuwenden.
<b>Automatische Firmware-Bereitstellung</b>	Die Liste der auf der Seite „Datei-Repository-Bestand“ hochgeladenen Firmware-Dateien wird geladen. Wählen Sie in der Dropdownliste die Firmware-Datei zur Aktualisierung des Thin Client aus. Die Sicherheitsstufe muss auf <b>Umgebung mit hoher Sicherheit</b> festgelegt werden.

## Konfigurieren von Remote-Verbindungseinstellungen

Verwenden Sie die Seite **Remote-Verbindung** zum Konfigurieren der Remote-Verbindungseinstellungen.

**Tabelle 245. Remote-Verbindung**

Option	Beschreibung
<b>Verbindungsart für Sitzung</b>	Wählen Sie in der Dropdownliste die Verbindungsart aus. Die verfügbaren Verbindungsarten sind: <ul style="list-style-type: none"> <li>· View Connection-Server</li> <li>· PCoIP-Verbindungsserver</li> </ul> Basierend auf der ausgewählten Verbindungsart ändern sich die Konfigurationsoptionen.
<b>Modus</b>	Wählen Sie in der Dropdownliste den Sitzungstyp aus. Die verfügbaren Sitzungstypen sind: <ul style="list-style-type: none"> <li>· Einfach</li> <li>· Auto-Anmeldung</li> <li>· Kiosk</li> <li>· Imprivata OneSign</li> </ul>
<b>Hostname oder IP-Adresse</b>	Geben Sie den DNS-Namen oder die IP-Adresse an. Diese Option ist verfügbar, wenn die Verbindungsart <b>View Connection-Server</b> ist und die Sitzungstypen <b>Einfach</b> , <b>Auto-Anmeldung</b> und <b>Kiosk</b> lauten.
<b>Server-URI</b>	Geben Sie den Uniform Resource Identifier (URI) für den <b>PCoIP-Verbindungsmanager</b> ein. Die Adresse muss das folgende Format aufweisen: <b>https://[hostname]][IP Address]</b> Diese Option ist verfügbar, wenn die Verbindungsart <b>PCoIP-Verbindungsserver</b> ist und die Sitzungstypen <b>Einfach</b> oder <b>Auto-Anmeldung</b> lauten.
<b>Anmeldebenutzername</b>	Geben Sie den Benutzernamen des Clients an. Der Benutzername darf maximal 128 Zeichen enthalten. Diese Option ist verfügbar, wenn die Verbindungsarten <b>View Connection-Server</b> oder <b>PCoIP-Verbindungsserver</b> sind und der Sitzungstyp <b>Auto-Anmeldung</b> lautet.
<b>Anmeldekennwort</b>	Geben Sie das Kennwort für den Client ein. Das Kennwort darf aus maximal 128 Zeichen bestehen. Diese Option ist verfügbar, wenn

Option	Beschreibung
	die Verbindungsarten <b>View Connection-Server</b> oder <b>PCoIP-Verbindungsserver</b> sind und der Sitzungstyp <b>Auto-Anmeldung</b> lautet.
<b>Anmeldedomänenname</b>	Geben Sie den Domainnamen des Thin Client ein. Der Domainname darf maximal 256 Zeichen enthalten. Diese Option ist verfügbar, wenn die Verbindungsarten <b>View Connection-Server</b> oder <b>PCoIP-Verbindungsserver</b> sind und der Sitzungstyp <b>Auto-Anmeldung</b> lautet.
<b>Typ des Benutzernamens</b>	Wählen Sie aus der Dropdownliste den Typ des Benutzernamens aus. Der Benutzername muss mit dem Gerätenamen im View Connection-Server übereinstimmen. Diese Option ist verfügbar, wenn die Verbindungsart <b>View Connection-Server</b> und der Sitzungstyp <b>Kiosk</b> ist.
<b>Kennwort</b>	Geben Sie das Kennwort für den Schutz der virtuellen Kiosk-Maschine an. Das Kennwort muss mit dem Gerätekenwort im View Connection-Server übereinstimmen. Diese Option ist verfügbar, wenn die Verbindungsart <b>View Connection-Server</b> und der Sitzungstyp <b>Kiosk</b> ist.
<b>Bootstrap URL</b>	Geben Sie die Bootstrap-URL ein, um den ersten OneSign-Server in einer Bereitstellung mit OneSign-Authentifizierung zu finden. Diese Option ist verfügbar, wenn der Verbindungstyp <b>View Connection-Server</b> und der Sitzungstyp <b>Imprivata OneSign</b> ist.

**Tabelle 246. Erweiterte Optionen**

Option	Beschreibung
<b>Sichere Verbindung (SSL) verwenden</b>	Wählen Sie diese Option aus, um die SSL-Verbindung zu verwenden. Diese Option ist verfügbar, wenn die Verbindungsart <b>View Connection-Server</b> ist und die Sitzungstypen <b>Einfach</b> , <b>Auto-Anmeldung</b> und <b>Kiosk</b> lauten.
<b>Beim Starten immer mit diesem Server verbinden</b>	Wählen Sie diese Option aus, um automatisch eine Verbindung zu dem Server herzustellen. Diese Option ist verfügbar, wenn die Verbindungsart <b>View Connection-Server</b> ist und die Sitzungstypen <b>Einfach</b> , <b>Auto-Anmeldung</b> und <b>Kiosk</b> lauten.
<b>Bei nur einem Desktop automatisch starten</b>	Wählen Sie diese Option aus und geben Sie die Anmeldeinformationen für eine Verbindung zu einem bereitgestellten Desktop oder einer Anwendung ein. Diese Option ist verfügbar, wenn die Verbindungsart <b>View Connection-Server</b> ist und die Sitzungstypen <b>Einfach</b> , <b>Auto-Anmeldung</b> und <b>Kiosk</b> lauten.
<b>OneSign Pool Name Mode (Modus für OneSign-Poolname)</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option. Diese Option ist verfügbar, wenn der Verbindungstyp <b>View Connection-Server</b> und der Sitzungstyp <b>Imprivata OneSign</b> ist.
<b>Pool Name to Select (Poolnamen auswählen)</b>	Geben Sie den Poolnamen ein. Wenn die Liste den eingegebenen Poolnamen enthält, startet der Client sofort einer Sitzung mit diesem Pool. Diese Option ist verfügbar, wenn der Verbindungstyp <b>View Connection-Server</b> und der Sitzungstyp <b>Imprivata OneSign</b> ist.
<b>Verifizierung der OneSign-Appliance</b>	Wählen Sie in der Dropdownliste den Typ der Überprüfung für das Zertifikat aus, das vom OneSign-Applianceserver bereitgestellt wird.

Option	Beschreibung
	Diese Option ist verfügbar, wenn der Verbindungstyp <b>View Connection-Server</b> und der Sitzungstyp <b>Imprivata OneSign</b> ist.
<b>An View-Adresse weiterleiten</b>	Geben Sie die Adresse ein, die verwendet werden soll, wenn der OneSign-Server nicht erreichbar ist. Die Adresse muss das folgende Format aufweisen: <b>https://[hostname][IP Address]</b>  Diese Option ist verfügbar, wenn der Verbindungstyp <b>View Connection-Server</b> und der Sitzungstyp <b>Imprivata OneSign</b> ist.
<b>Zertifikatsprüfmodus</b>	Wählen Sie in der Dropdownliste die Ebene der Überprüfung für das Zertifikat aus, das vom Verbindungsserver bereitgestellt wird. Diese Option ist verfügbar, wenn der Verbindungstyp <b>PCoIP-Verbindungsserver</b> ist.
<b>Modus für Zertifikatsüberprüfung sperren</b>	Wählen Sie diese Option aus, wenn erforderlich. Diese Option ist verfügbar, wenn der Verbindungstyp <b>PCoIP-Verbindungsserver</b> ist.
<b>Enable Session Disconnect Hotkey (Hotkey zum Trennen von Sitzungen aktivieren)</b>	Markieren Sie das Kontrollkästchen, um diese Funktion zu aktivieren. Sie können die Hotkey-Tastenfolge <b>Ctrl+Alt+F12</b> zur Anzeige des Bildschirms <b>Zero-Client-Systemsteuerung</b> drücken. Sie können die aktuelle Sitzung auf der Workstation trennen oder die Workstation ausschalten. Diese Option ist verfügbar, wenn der Verbindungstyp <b>PCoIP-Verbindungsserver</b> ist.

Tabelle 247. Verfügbare Broker-Server

Option	Beschreibung
<b>Servertyp</b>	Wählen Sie in der Dropdownliste den Servertyp aus. Die verfügbaren Verbindungsarten sind: <ul style="list-style-type: none"> <li>View Connection-Server</li> <li>PCoIP-Verbindungsserver</li> </ul>
<b>Cache-Modus</b>	Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
<b>Broker-Server</b>	Klicken Sie auf die Option <b>Server hinzufügen</b> zum Hinzufügen der Broker-Verbindung.

## Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen

Gehen Sie zum Bearbeiten der Wyse Software Thin Client-Richtlinieneinstellungen folgendermaßen vor:

- 1 Klicken Sie auf **Gruppen und Konfigurationen**.  
Die Seite **Gruppen und Konfigurationen** wird angezeigt.
- 2 Klicken Sie auf die Dropdownliste **Richtlinien bearbeiten**.
- 3 Klicken Sie auf **Wyse Software Thin Client**.  
Die Seite **Wyse Software Thin Client** wird angezeigt. Die Wyse Software Thin Client-Richtlinieneinstellungen umfassen die folgenden Optionen:
  - Systempersonalisierung
  - Desktoperlebnis
  - Netzwerk
  - Sicherheit und Sperrmodus

- Andere Einstellungen
  - Citrix Remote-Verbindungen
  - VMware Remote-Verbindungen
  - RDP Remote-Verbindungen
  - Browser-Remote-Verbindungen
  - Geräteinfo
  - Wyse Easy Setup (2.0+)
  - VNC-Einstellungen
  - Domäneneinstellungen
- 4 Klicken Sie nach der Konfiguration der Richtlinienereinstellungen auf **Speichern und veröffentlichen**.

## Konfigurieren der Systempersonalisierung

Verwenden Sie diese Seite zum Konfigurieren der Thin Client-Anzeigeeinstellungen, wie z. B. Auflösung, Farbtiefe, Dualmonitor, Zeitzone, Maus und Audiooptionen für Wyse-Software-Geräte.

**Tabelle 248. Konfigurieren von Anzeigooptionen**

Option	Beschreibung
<b>Dualmonitor aktivieren</b>	Wählen Sie diese Option aus, um die Dualmonitor-Funktion zu aktivieren.
<b>Monitorauflösung (primär)</b>	Wählen Sie diese Option aus, um die Auflösung Ihres Monitors einzustellen. Wählen Sie aus dem Dropdownmenü die geeignete Auflösung aus:
<b>Anzeigenkennung (primär)</b>	Wählen Sie diese Option aus, um eine Anzeigenkennung für Ihren Monitor einzugeben. Wählen Sie aus dem Dropdownmenü eine geeignete Monitoridentifizierungsnummer.
<b>Monitordrehung (primär)</b>	Wählen Sie diese Option aus, um eine Ausrichtung für den Monitor einzustellen. Wählen Sie im Dropdownmenü nach Bedarf eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>· Querformat</li> <li>· Hochformat</li> <li>· Querformat umgedreht</li> <li>· Hochformat umgedreht</li> </ul>

**Tabelle 249. Konfigurieren von Tastaturoptionen**

Option	Beschreibung
<b>Sprache</b>	Wählen Sie diese Option, um ein oder mehrere Eingabesprachen für die Tastatur festzulegen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Tastatur-Eingabesprache aus.
<b>Tastaturlayout</b>	Wählen Sie diese Option aus, um ein entsprechendes Tastaturlayout einzustellen. Wählen Sie aus dem Dropdownmenü Ihr bevorzugtes Tastaturlayout.
<b>Blinkfrequenz</b>	Wählen Sie diese Option aus, um die Geschwindigkeit einzustellen, mit der der Cursor (Einfügemarke) blinkt, um den Cursor mehr oder weniger sichtbar zu machen, je nach Ihren Anforderungen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Cursorblinkrate aus.
<b>Tastatureinstellungen</b>	Wählen Sie diese Option zum Einstellen der Tastaturschnellasten.

Option	Beschreibung
<b>Tastatur-Wiederholverzögerung</b>	<p>Wählen Sie diese Option aus, um die Zeit festzulegen, die eine Taste gedrückt bleiben kann, ohne dass der Buchstabe als Eingabe wiederholt wird. Wählen Sie im Dropdownmenü nach Bedarf eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>· Kurz</li> <li>· Mittelkurz</li> <li>· Mittellang</li> <li>· Lang</li> </ul>
<b>Tastatur-Wiederholrate</b>	<p>Wählen Sie diese Option, um die Wiederholrate für die Tastatur einzustellen. Diese gibt die Geschwindigkeit an, mit der die Tasteneingabe beim Drücken und Halten der Taste auf der Tastatur wiederholt wird.</p>
<b>Menüzugriff</b>	<p>Wählen Sie diese Option aus, um die Menüzugriffstasten auf der Tastatur zu aktivieren.</p>
<b>Tastaturlayout „MS Gina“</b>	<p>Wählen Sie diese Option zum Anzeigen des Bildschirms <b>Tastaturlayout</b> auf dem Windows Anmeldebildschirm anzuzeigen. Das Tastaturlayout „MS Gina“ ermöglicht das Auswählen der gewünschten Sprache und des gewünschten Tastaturlayouts auf dem Anmeldebildschirm des Windows Geräts. Beispiel:</p> <p>Falls die Windows-Anmeldeinformationen nicht in englischer Sprache sind und die Tastatur des Windows-Systems eine englische ist. Sie können die Anmeldeinformationen nicht eingeben, da keine Option zum Ändern oder Auswählen der Sprache und des Tastaturlayouts auf dem Windows-Anmeldebildschirm vorhanden ist.</p> <p>Sie können die gewünschten Sprachen konfigurieren und Sprachen und das Tastaturlayout mithilfe des <b>Tastaturlayouts „MS Gina“</b> vom Wyse Management Suite-Server ersetzen. Wenn Sie die Sprache oder Tastatureinstellungen anwenden, wird das Tastaturlayout „MS Gina“ auf dem Windows-Anmeldebildschirm angezeigt.</p> <p>Sie können die gewünschte Sprache und das gewünschte Tastaturlayout auf dem Windows-Anmeldebildschirm ändern oder auswählen.</p> <p><b>!</b> <b>ANMERKUNG: Der Windows Anmeldebildschirm wird angezeigt, wenn die automatische Anmeldung deaktiviert ist. Zum Anwenden der Einstellungen des Tastaturlayouts „MS Gina“ vom Wyse Management Suite-Server müssen Sie die Option „Schreibfilter“ deaktivieren und aktivieren. Das Windows-System wird zweimal neu gestartet.</b></p>

**Tabelle 250. Konfigurieren der Mauseinstellungen**

Option	Beschreibung
<b>Mausgeschwindigkeit</b>	<p>Wählen Sie diese Option aus, um die Geschwindigkeit des Mauszeigers beim Bewegen der Maus anzugeben.</p>
<b>Linkshänder-Maus</b>	<p>Wählen Sie diese Option aus, um die linke und rechte Maustaste zu vertauschen.</p>

**Tabelle 251. Grundlegende Mausoptionen konfigurieren**

Option	Beschreibung
<b>KlickEinrasten</b>	Wählen Sie diese Option aus, um den Mauszeiger ohne Gedrückthalten der Maustaste zu markieren oder zu ziehen. Wählen Sie zum Einstellen der Option <b>Klick-Einrasten-Zeit</b> aus dem Dropdownmenü die gewünschte Zeit für die die Maustaste gedrückt gehalten werden muss, bevor das Klicken gesperrt wird.
<b>Doppelklickgeschwindigkeit</b>	Wählen Sie diese Option, um das Zeitintervall zwischen zwei aufeinanderfolgenden Mausclicks festzulegen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.

**Tabelle 252. Konfigurieren der Mauszeiger-Option**

Option	Beschreibung
<b>Mauszeiger finden</b>	Wählen Sie diese Option aus, wenn Sie den Mauszeiger finden möchten, wenn er nicht in Bewegung ist.  <b>ANMERKUNG:</b> Sie können die <code>strg</code> -Taste auf der Tastatur drücken, um den Mauszeiger zu finden, wenn er nicht in Bewegung ist.
<b>Mauszeiger ausblenden</b>	Wählen Sie diese Option zum Ausblenden des Mauszeigers, wenn er nicht in Bewegung ist.  <b>ANMERKUNG:</b> Um den Mauszeiger zu finden, wenn er nicht in Bewegung ist, drücken Sie die Taste <code>strg</code> .
<b>Zeigerpfadlänge</b>	Wählen Sie diese Option zum Definieren der Länge des Zeigerpfads, wenn der Mauszeiger bewegt wird.
<b>Zur Standardschaltfläche springen</b>	Wählen Sie diese Option aus, um in Dialogfeldern automatisch zur Standardschaltfläche zu springen.

**Tabelle 253. Mausvertikale**

Option	Beschreibung
<b>Scrollzeilen</b>	Wählen Sie diese Option aus, um die Anzahl der gleichzeitig gescrollten Zeilen beim vertikalen Scrollen zu definieren.

**Tabelle 254. Zeitzone konfigurieren**

Option	Beschreibung
<b>Zeitserver (NTP-Server)</b>	Wählen Sie diese Option zum Anzeigen der Zeitserver zum Aktivieren der lokalen Zeitsynchronisierung. Geben Sie die NTP-Server jeweils getrennt durch ein Komma ein.

**Tabelle 255. Konfigurieren von Zeitzonenoptionen**

Option	Beschreibung
<b>Name der Zeitzone</b>	Wählen Sie diese Option zum Einstellen der Zeitzone auf Ihrem Gerät. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Zeitzone.

**Tabelle 256. Konfigurieren von Audioeinstellungen**

Option	Beschreibung
<b>Audio stumm schalten</b>	Wählen Sie diese Option aus, um den Ton Ihres Geräts stummzuschalten.
<b>Audiolautstärke</b>	Wählen Sie diese Option aus, um die Lautstärke Ihres Geräts anzupassen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Lautstärkeoption.
<b>Mikrofon stumm schalten</b>	Wählen Sie diese Option aus, um das Mikrofon stummzuschalten.
<b>Mikrofonlautstärke</b>	Wählen Sie diese Option aus, um die Lautstärke des Mikrofons einzustellen. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Lautstärkeoption.

## Desktop-Erfahrung konfigurieren

Verwenden Sie diese Seite zum Konfigurieren der Thin Client Einstellungen, wie z. B. Desktop-Hintergrundbild und Desktopfarbe für Wyse Software-Geräte.

**Tabelle 257. Desktop-Erfahrung konfigurieren**

Option	Beschreibung
<b>Desktophintergrund</b>	<p>Wählen Sie diese Option aus, um ein Hintergrundbild für Ihren Desktop festzulegen.</p> <p>Nach Aktivierung der Option Desktop-Hintergrundbild gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> <li>Wählen Sie aus der Dropdownliste <b>Hintergrundbild-Datei</b> ein Hintergrundbild für Ihren Desktop aus.</li> </ul> <p><b>i ANMERKUNG:</b> Wählen Sie nur ein Hintergrundbild aus der Liste der Hintergrundbilder, die in das Datei-Repository hochgeladen wurden.</p> <ul style="list-style-type: none"> <li>Wählen Sie aus der Dropdownliste <b>Hintergrundbild-Layout</b> eines der folgenden Layouts für Ihr Desktop-Hintergrundbild: <ul style="list-style-type: none"> <li>Zentriert</li> <li>Nebeneinander</li> <li>Strecken</li> <li>Füllen</li> </ul> </li> </ul>
<b>Desktopfarbe</b>	Wählen Sie diese Option aus, um eine Hintergrundfarbe für den lokalen Desktop festzulegen.

# Konfigurieren der Netzwerkeinstellungen

Verwenden Sie diese Seite für das Konfigurieren der Netzwerkeinstellungen der Wyse Software-Geräte.

**Tabelle 258. Konfigurieren der Netzwerkeinstellungen**

Option	Beschreibung
<b>WLAN-Status</b>	<p>Wählen Sie diese Option aus, um den Status "drahtloser Funkempfänger" zu aktivieren.</p> <p><b>ANMERKUNG:</b> Diese Option ist ähnlich zum Ein- oder Auszuschalten des Geräts.</p>
<b>Windows Wireless-Profil</b>	<p>Wählen Sie diese Option aus, um ein Windows Wireless-Profil festzulegen. Wählen Sie aus dem Dropdownmenü Ihr bevorzugtes Windows Wireless-Profil aus.</p> <p><b>ANMERKUNG:</b> Wählen Sie nur ein Profil aus der Liste der Wireless-Profile, die in das Datei-Repository hochgeladen wurden.</p>

# Konfigurieren der Sicherheits- und Sperrmoduseinstellungen

Verwenden Sie diese Seite für die Konfiguration der Sicherheits- und Sperrmoduseinstellungen.

**Tabelle 259. Sicherheit und Sperrmodus**

Option	Beschreibung
<b>Zertifikate installieren</b>	Wählen Sie diese Option zum Anzeigen der Zertifikate, die in das Datei-Repository hochgeladen wurden.
<b>Zugriff auf USB-Speichergerät deaktivieren</b>	Wählen Sie diese Option zum Aktivieren oder Deaktivieren des Zugriffs auf USB-Massenspeichergeräte für Nicht-Administratorbenutzer.
<b>Druck deaktivieren</b>	Wählen Sie diese Option zum Aktivieren oder Deaktivieren der Druck-Funktion (Screenshot) für Nicht-Administratorbenutzer.
<b>Task-Manager deaktivieren</b>	Wählen Sie diese Option zum Aktivieren oder Deaktivieren des Zugriffs auf den Task-Manager für Nicht-Administratorbenutzer.

# Andere Einstellungen konfigurieren

Verwenden Sie diese Seite zum Konfigurieren der Thin Client Einstellungen, wie z. B. Strom, freigegebene Laufwerke und Uhreinstellungen für Wyse Software-Geräte.

**Tabelle 260. Konfigurieren des Gerätemodus**

Option	Beschreibung
<b>Anwendungsmodus</b>	Wählen Sie diese Option zum Einstellen eines geeigneten Modus für das Gerät aus. Die Option „Gerätemodus“ startet die Anwendung in einem Kioskmodus und ohne Zugriff auf den Desktop oder andere Anwendungen. Sie können den Gerätemodus mithilfe der

Option	Beschreibung
	<p>konfigurierten Tasten aufheben. Zum Beispiel: Strg + Umschalttaste + A. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Aus</li> <li>• Generisch</li> <li>• VMware View</li> <li>• Citrix</li> <li>• Internet Explorer</li> <li>• RDP</li> </ul>
<b>Gerätemodus beenden</b>	Wählen Sie diese Option aus, um den Gerätemodus zu beenden, indem Sie eine Tastenkombination benutzen.

**Tabelle 261. Energieeinstellungen**

Option	Beschreibung
<b>Energieplan des Geräts</b>	<p>Wählen Sie diese Option, um einen Energiesparplan für Ihr Gerät zu wählen. Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Ausgeglichen</li> <li>• Energiesparmodus</li> </ul>

**Tabelle 262. Energieeinstellungen im Akkubetrieb**

Option	Beschreibung
<b>Ruhezustandsplan für das Gerät (im Akkubetrieb)</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der das Gerät in den Ruhemodus versetzt wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Anzeige abdunkeln (im Akkubetrieb)</b>	Wählen Sie diese Option aus, um die Zeit festzulegen, nach der die Anzeige abgeblendet wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Anzeige ausschalten (im Akkubetrieb)</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der die Anzeige ausgeschaltet wird. Wählen Sie eine Verzögerungszeit aus der Dropdownliste aus.

**Tabelle 263. Energieeinstellungen beim Anschluss an Stromversorgung**

Option	Beschreibung
<b>Ruhezustandsplan für das Gerät (an Stromversorgung angeschlossen)</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der das Gerät in den Ruhemodus versetzt wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Anzeige abdunkeln (an Stromversorgung angeschlossen)</b>	Wählen Sie diese Option aus, um die Zeit festzulegen, nach der die Anzeige abgeblendet wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.
<b>Anzeige ausschalten (an Stromversorgung angeschlossen)</b>	Wählen Sie diese Option aus, um die Zeit einzustellen, nach der die Anzeige ausgeschaltet wird. Wählen Sie aus dem Dropdownmenü die Verzögerungszeit aus.

**Tabelle 264. Konfigurieren freigegebener Geräte**

Option	Beschreibung
<b>Freigegebenes Laufwerk</b>	<p>Wählen Sie diese Option zum Hinzufügen eines freigegebenen Laufwerks an Ihr Gerät. Klicken Sie auf <b>Freigegebenes Gerät hinzufügen</b>. Geben Sie den Freigabennamen, den Pfad des Remote-Laufwerks, den Benutzernamen und das Kennwort für das freigegebene Laufwerk ein.</p> <p><b>ANMERKUNG:</b> Zum Löschen eines freigegebenen Laufwerks aus der Liste wählen Sie das freigegebene Laufwerk, das Sie entfernen möchten, und klicken Sie auf <b>Entfernen</b>.</p>

**Tabelle 265. Uhreinstellungen**

Option	Beschreibung
<b>Uhr1</b>	<p>Wählen Sie diese Option aus, um Uhr 1 Ihres Geräts zu konfigurieren.</p> <p>Nachdem Sie Uhr 1 aktivieren, legen Sie den <b>Anzeigenamen</b> für die Uhr fest. Wählen Sie aus dem Dropdownmenü die <b>Zeitzone</b> für Uhr 1.</p>
<b>Uhr2</b>	<p>Wählen Sie diese Option aus, um Uhr 2 Ihres Geräts zu konfigurieren.</p> <p>Nachdem Sie die Uhr 2 aktivieren, legen Sie den <b>Anzeigenamen</b> für die Uhr fest. Wählen Sie aus dem Dropdownmenü die <b>Zeitzone</b> für Uhr 2.</p>

## Konfigurieren von Remote-Verbindungseinstellungen – Citrix

Auf dieser Seite können Sie konfigurieren, auf welche Citrix Remote-Verbindungen auf dem Wyse Software Thin Client zugegriffen werden kann.

**Tabelle 266. Grundlegende Optionen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um einen Namen für die Verbindungsidentifikation festzulegen.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option aus, um das automatische Starten der Sitzung nachdem Sie sich angemeldet haben zu aktivieren.
<b>Verbindungstyp</b>	<p>Wählen Sie diese Option aus, um einen Verbindungstyp festzulegen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Veröffentlichte Anwendungen (XenApp)</li> <li>• Serververbindung (XenDesktop)</li> <li>• Gateway</li> <li>• Storefront</li> </ul>
<b>Citrix Server-FQDN oder -IP-Adresse</b>	Wählen Sie diese Option aus, um die Citrix-Server aufzulisten. Geben Sie die Liste der ICA-Browser für die Verbindung durch Kommas getrennt ein.

Option	Beschreibung
<b>Veröffentlichte Anwendungen</b>	Wählen Sie diese Option zur Angabe einer veröffentlichten Anwendung, die Sie starten möchten.
<b>Single Sign On</b>	Wählen Sie diese Option zur Aktivierung der Funktion "Einmaliges Anmelden" für die Verbindung aus. Wenn Sie die "Einmalige Anmeldung" aktivieren, verwenden Sie Ihre Windows-Anmeldeinformationen für die Verbindung mit dem Citrix-Server.
<b>Benutzername</b>	Wählen Sie diese Option aus, um einen Benutzernamen für die Citrix-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Kennwort</b>	Wählen Sie diese Option aus, um ein Kennwort für die Citrix-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Domainname</b>	Wählen Sie diese Option aus, um einen Domainnamen für die Citrix-Verbindung zu definieren.
<b>Fenstergröße</b>	Wählen Sie diese Option zur Angabe der Fenstergröße für die Citrix-Verbindung. Wählen Sie aus dem Dropdownmenü die Fenstergröße aus.
<b>Bildschirm-Farbtiefe</b>	<p>Wählen Sie diese Option zum Definieren der Bildschirm-Farbtiefe der Citrix-Verbindung.</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Bessere Geschwindigkeit 16 Bit</li> <li>• Bessere Darstellung 32 Bit</li> </ul>
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, um automatisch die Verbindung wiederherzustellen, wenn die Verbindung abbricht.
<b>Audioqualität</b>	<p>Wählen Sie diese Option, um die Tonqualität für die Citrix-Verbindung zu wählen. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Standardaudioeinstellung des Benutzers</li> <li>• High Definition</li> <li>• Für Sprache optimiert</li> <li>• Niedrige Bandbreite</li> <li>• Aus</li> </ul>
<b>Passthrough für Tastenkombinationen des Benutzers</b>	<p>Wählen Sie diese Option, um anzugeben, auf welches Fenster die Tastenkombinationen des Windows-Benutzers angewendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Standard-Passthrough für Tastenkombinationen des Benutzers</li> <li>• Auf dem lokalen Desktop</li> <li>• Auf dem Remotedesktop</li> <li>• Nur auf Vollbild-Desktops</li> </ul>
<b>Speichernamen</b>	Geben Sie den Speichernamen des Citrix Servers oder der StoreFront ein.
<b>Authentifizierungsmethoden</b>	<p>Mit dieser Option wird der allgemeine Authentifizierungstyp aktiviert. Wählen Sie im Dropdownmenü eine beliebige der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• Eingabeaufforderung für Anmeldeinformationen</li> <li>• Authentifizierung von Benutzername und Kennwort</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>· Smartcard-Authentifizierung</li> <li>· Einmaliges Anmelden (Domain-Passthrough-Authentifizierung)</li> </ul>

**ANMERKUNG:**

- Nachfolgend sind die Voraussetzungen aufgeführt, unter denen End-to-End-Passthrough-Authentifizierung aktiviert wird, wenn Sie als Authentifizierungsmethode einmaliges Anmelden auswählen:
  - Einmaliges Anmelden für den Citrix-Empfänger muss auf dem Gerät aktiviert sein.
  - Das Zielgerät muss der Domäne hinzugefügt werden.
  - Der Domänenbenutzer muss sich am Gerät anmelden.
- Nachfolgend sind die Voraussetzungen aufgeführt, unter denen End-to-End-Passthrough-Authentifizierung aktiviert wird, wenn Sie als Authentifizierungsmethode Smart-Card-Authentifizierung auswählen:
  - Einmaliges Anmelden für den Citrix-Empfänger muss auf dem Gerät aktiviert sein.
  - Das Zielgerät muss der Domäne hinzugefügt werden. Das Zielgerät muss der Domäne hinzugefügt werden.
  - Der Domänenbenutzer muss sich mit der Smart Card am Gerät anmelden.

Weitere Informationen finden Sie im Artikel *Configure domain pass-through authentication* (Domänen-Passthrough-Authentifizierung konfigurieren) unter [docs.citrix.com](https://docs.citrix.com).

**Tabelle 267. Anwendungsanzeige**

Option	Beschreibung
<b>Desktopanzeige</b>	Wählen Sie diese Option zum Anzeigen der Citrix-Verbindung auf Ihrem Desktop. Wenn Sie diese Option aktivieren, geben Sie den <b>Namen des Desktopordners</b> für die Verbindung ein.
<b>Startmenüanzeige</b>	Wählen Sie diese Option, um die Startmenüanzeige auf dem Verbindungsdesktop zu aktivieren. Nachdem Sie diese Option aktiviert haben, geben Sie den <b>Ordner der Startmenüanzeige</b> für die Verbindung ein.
<b>Taskleistenanzeige</b>	Durch Auswahl dieser Option wird die Citrix-Verbindung im Infobereich angezeigt.

**Tabelle 268. Serveroptionen**

Option	Beschreibung
<b>Anmeldemethode</b>	Wählen Sie diese Option zur Auswahl einer Anmeldemethode für Ihre Citrix-Verbindung. <ul style="list-style-type: none"> <li>· Standard-Anmeldemethode</li> <li>· Geforderte Anmeldemethode</li> </ul>

**Tabelle 269. Erweiterte Einstellungen**

Option	Beschreibung
<b>Vollbildschirm-Popup deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der Vollbildschirm-Pop-up-Warnung.
<b>Anmeldung – Verbindung zu aktiven und getrennten Sitzungen herstellen</b>	Wählen Sie diese Option aus, um nach dem Anmelden eine Verbindung zu den aktiven und getrennten Sitzungen herzustellen.
<b>Menü – Verbindung zu aktiven und getrennten Sitzungen herstellen</b>	Wählen Sie diese Option aus, um eine Verbindung zu aktiven und getrennten Sitzungen herzustellen.
<b>Über Menü erneut verbinden</b>	Wählen Sie diese Option aus, um sich über das Client-Menü erneut mit vorhandenen Sitzungen zu verbinden.

**Tabelle 270. Flash-Umleitung**

Option	Beschreibung
<b>Flash-Remoting verwenden</b>	Wählen Sie diese Option aus, um die Flash-Inhalte auf dem Client-Gerät anstatt auf dem Remote-Server darzustellen.
<b>Serverseitigen Inhaltsabruf aktivieren</b>	Wählen Sie diese Option aus, um Inhalte vom Server herunterzuladen und anschließend an das Benutzergerät zu senden.
<b>Server-HTTP-Cookies verwenden</b>	Wählen Sie diese Option zum Synchronisieren der clientseitigen HTTP-Cookies mit den serverseitigen.
<b>URL-Umschreibungsregeln für clientseitigen Inhaltsabruf</b>	<p>Wählen Sie diese Option aus, um Regeln zum Umleiten von Benutzergeräten an andere Server für den clientseitigen Abruf hinzuzufügen. Klicken Sie auf <b>Element hinzufügen</b> und geben Sie den Namen der Inhaltsregel und den Wert der Inhaltsregel an.</p> <p><b>ANMERKUNG:</b> Zum Löschen eines Elements aus der Liste wählen Sie das Element, das Sie entfernen möchten, und klicken Sie auf <b>Entfernen</b>.</p>

## Konfigurieren von Remote-Verbindungseinstellungen – VMware

Auf dieser Seite können Sie konfigurieren, auf welche VMware Remote-Verbindungen auf dem Wyse Software Thin Client zugegriffen werden kann.

**Tabelle 271. Konfigurieren von Remote-Verbindungseinstellungen – VMware**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um den Namen für die Identifizierung der Verbindung zu definieren.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option aus, um das automatische Starten der Verbindung nachdem Sie sich angemeldet haben zu aktivieren.
<b>VMware Serveradresse</b>	Wählen Sie diese Option zur Eingabe der Serveradresse der VMware-Verbindung.
<b>Protokoll</b>	<p>Wählen Sie diese Option aus, um das Protokoll für die VMware-Verbindung zu wählen. Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>• PCOIP</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>· RDP</li> <li>· Blast</li> </ul>
<b>Als aktueller Benutzer anmelden</b>	Wählen Sie diese Option zur Aktivierung der Funktion "Einmaliges Anmelden" für die Verbindung aus. Wenn Sie die Option <b>Als aktueller Benutzer anmelden</b> aktivieren, verwenden Sie Ihre Windows-Anmeldeinformationen für die Verbindung mit dem VMware-Server.
<b>Benutzername</b>	Wählen Sie diese Option aus, um einen Benutzernamen für die VMware-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Kennwort</b>	Wählen Sie diese Option aus, um ein Kennwort für die VMware-Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Domainname</b>	Wählen Sie diese Option aus, um einen Domainnamen für die VMware-Verbindung zu definieren.
<b>Sicherheitsmodus</b>	Wählen Sie diese Option zur Angabe der Client-Konnektivität, wenn Sie keine sichere Verbindung zum Server gewährleisten können.
<b>Vollbildschirm-Modus</b>	Wählen Sie diese Option, um das VMware-Verbindungsfenster im Vollbildschirm-Modus auszuführen. Wenn Sie den Vollbildschirm-Modus nicht auswählen, wählen Sie aus dem Dropdownmenü die <b>Fenstergröße</b> .
<b>Dropdown-Menüleiste für Vollbildschirm anzeigen</b>	Durch Auswahl dieser Option wird das Dropdownmenü <b>Vollbildschirm-Modus</b> für Ihre Verbindung angezeigt.
<b>Diesen Desktop automatisch starten</b>	Wählen Sie diese Option zur Angabe eines veröffentlichten Desktops zum Starten nach dem erfolgreichen Verbindungsaufbau.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, um sich automatisch wiederzuverbinden, wenn die Verbindung getrennt wird.
<b>Broker</b>	Wählen Sie diese Option aus, um den Hostnamen oder die IP-Adresse des <b>View Connection</b> Brokers zu definieren.
<b>Brokerverlauf</b>	Wählen Sie diese Option aus, um den zuvor verwendeten Hostnamen oder die IP-Adresse des <b>View Connection</b> Brokers zu definieren.

## Konfigurieren von Remote-Verbindungseinstellungen – RDP

Auf dieser Seite können Sie konfigurieren, auf welche RDP-Remote-Verbindungen auf dem Wyse Software Thin Client zugegriffen werden kann.

**Tabelle 272. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um den Namen für die Identifizierung der Verbindung zu definieren.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option aus, um das automatische Starten der Verbindung nachdem Sie sich angemeldet haben zu aktivieren.
<b>Serveradresse</b>	Wählen Sie diese Option zur Eingabe der Serveradresse der Verbindung.

Option	Beschreibung
<b>Single Sign On</b>	Wählen Sie diese Option zur Aktivierung der Funktion "Einmaliges Anmelden" für die Verbindung aus. Wenn Sie die Option <b>Als aktueller Benutzer anmelden</b> aktivieren, verwenden Sie Ihre Windows-Anmeldeinformationen für die Verbindung mit dem Server.
<b>Benutzername</b>	Wählen Sie diese Option aus, um einen Benutzernamen für die Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Kennwort</b>	Wählen Sie diese Option aus, um ein Kennwort für die Verbindung zu definieren, wenn "Einmaliges Anmelden" deaktiviert ist.
<b>Domainname</b>	Wählen Sie diese Option aus, um einen Domainnamen für die Verbindung zu definieren.
<b>Automatisch neu verbinden</b>	Wählen Sie diese Option aus, um das automatische Wiederverbinden zu aktivieren, wenn die Verbindung getrennt wird.

**Tabelle 273. Konfigurieren von RD-Gateway-Einstellungen**

Option	Beschreibung
<b>RD-Gateway-Einstellungen verwenden</b>	<p>Wählen Sie diese Option zum Konfigurieren der Einstellungen für das RD-Gateway. Nachdem Sie die Option aktivieren, geben Sie den <b>RD-Servernamen</b> für das Gateway ein. Geben Sie die Anmeldeinformationen zur Prüfung der Verbindung mit dem RD-Gateway an.</p> <p>Wählen Sie aus dem Dropdownmenü <b>Anmeldemethode für RD-Gateway</b> eine der folgenden Optionen:</p> <ul style="list-style-type: none"> <li>• Nach Kennwort für NTLM fragen</li> <li>• Smart Card</li> <li>• Spätere Auswahl zulassen</li> </ul> <p>Wählen Sie aus dem Dropdownmenü <b>Nutzungsmethode des RD-Gateways</b> eine der folgenden Möglichkeiten zur Nutzung eines Remote-Desktop-Servers:</p> <ul style="list-style-type: none"> <li>• RD-Gateway-Server nicht verwenden – alle IP-Adressen</li> <li>• RD-Gateway-Servereinstellungen verwenden</li> <li>• RD-Gateway-Servereinstellungen nur für nicht lokale IP-Adressen verwenden</li> <li>• Standardeinstellungen verwenden</li> <li>• Nur lokale IP-Adressen</li> </ul>
<b>KDC-Proxy des Remotedesktop-Gateways</b>	Wählen Sie diese Option zum Konfigurieren der Einstellungen für den KDC-Proxy. Nachdem Sie die Option aktivieren, geben Sie den <b>Namen des KDC-Proxys</b> für den Server an.

**Tabelle 274. Konfigurieren der Anzeigeeinstellungen**

Option	Beschreibung
<b>Vollbildschirm-Modus</b>	Wählen Sie diese Option, um das Verbindungsfenster im Vollbildschirm-Modus auszuführen.

Option	Beschreibung
	Nachdem der Vollbildschirm-Modus aktiviert ist, wählen Sie aus dem Dropdownmenü die Fenstergröße aus.
<b>Verbindungsleiste anzeigen</b>	Wählen Sie diese Option, um die Verbindungsleiste im Vollbildschirm-Modus anzuzeigen.
<b>Multimonitor-Unterstützung</b>	Wählen Sie diese Option aus, um die Multimonitor-Funktion zu aktivieren.
<b>Bildschirm-Farbtiefe (in Bits)</b>	Wählen Sie diese Option zum Definieren der Bildschirm-Farbtiefe der Verbindung. <ul style="list-style-type: none"> <li>· RDP 15 Bit High Color</li> <li>· RDP 16 Bit High Color</li> <li>· RDP 24 Bit True Color</li> <li>· RDP 32 Bit höchste Qualität</li> </ul>

**Tabelle 275. Konfigurieren anderer Einstellungen – Lokal und Parameter**

Option	Beschreibung
<b>Remote-Audiowiedergabe</b>	Wählen Sie diese Option, um die Audiowiedergabequalität für die Remoteverbindung zu wählen.
<b>Remote-Audioaufzeichnung aktivieren</b>	Wählen Sie diese Option aus, um die Tonaufzeichnung im Remote-Zugriff zu ermöglichen.
<b>Windows Tasten anwenden</b>	Wählen Sie diese Option, um die Windows-Tasten anzuwenden. Wählen Sie aus dem Dropdownmenü Ihre bevorzugte Option.
<b>Das folgende Programm bei Verbindung starten</b>	Wählen Sie diese Option zum Starten des ausgewählten Programms, sobald das System verbunden ist. Nachdem Sie die Option aktivieren, geben Sie den <b>Programmpfad und Dateinamen</b> an und geben Sie die Einzelheiten zum Ordner im Feld <b>In folgendem Ordner beginnen</b> ein.
<b>Nach Anmeldeinformationen fragen</b>	Wählen Sie diese Option aus, um die Anmeldeinformationen einzugeben.
<b>Sicherheitsschicht verhandeln</b>	Wählen Sie diese Option aus, um die sicherste Ebene zu verwenden, die der Client unterstützt.
<b>Komprimierung aktivieren</b>	Wählen Sie diese Option aus, um die Dateien zur Reduzierung der Größe der Dateien und zur Reduzierung der Zeit, die das Herunterladen der Dateien in Anspruch nimmt, automatisch zu komprimieren.
<b>Videowiedergabe aktivieren</b>	Wählen Sie diese Option aus, um den Ton des Remote-Computers in einer Remote-Sitzung umzuleiten und eine höhere Benutzerfreundlichkeit bei der Videowiedergabe zu bieten.
<b>Neuverbindung von Workspace aktivieren</b>	Wählen Sie diese Option aus, um die Verbindung mit dem Arbeitsbereich wiederherzustellen.

**Tabelle 276. Lokale Ressourcen konfigurieren**

Option	Beschreibung
<b>Zwischenablage umleiten</b>	Wählen Sie diese Option für die Verwendung der lokalen Zwischenablage des Geräts in der Remoteverbindung aus.
<b>COM-Ports umleiten</b>	Wählen Sie diese Option für die Verwendung des lokalen COM-Ports (seriell) des Geräts in der Remoteverbindung aus.
<b>DirectX umleiten</b>	Wählen Sie diese Option aus, um DirectX auf dem Client-Computer umzuleiten und damit die Option in der Remoteverbindung verfügbar ist.
<b>Laufwerke umleiten</b>	Wählen Sie diese Option für die Verwendung der lokalen Laufwerke des Geräts in der Remoteverbindung aus.
<b>POS-Geräte umleiten</b>	Wählen Sie diese Option aus, um Point-of-Service-Geräte, wie z. B. Barcodeleser und magnetische Leser des Geräts in der Remoteverbindung zu verwenden.
<b>Alle Drucker weiterleiten</b>	Wählen Sie diese Option für die Verwendung des lokalen Druckers des Geräts in der Remoteverbindung.
<b>Smart Card umleiten</b>	Wählen Sie diese Option für die Verwendung der lokalen Smart Cards des Geräts in der Remoteverbindung.

**Tabelle 277. Konfigurieren anderer Einstellungen – Erlebnis**

Option	Beschreibung
<b>Verbindungsgeschwindigkeit zur Optimierung der Leistung</b>	Wählen Sie diese Option aus, um die Verbindungsgeschwindigkeit der Leistung gemäß zu optimieren.
<b>Desktophintergrund</b>	Wählen Sie diese Option für die Aktivierung des Desktophintergrunds für die Verbindung aus.
<b>Visuelle Stile</b>	Wählen Sie diese Option für die Aktivierung der visuellen Stile für die Verbindung aus.
<b>Schriftartglättung</b>	Wählen Sie diese Option für die Aktivierung der Schriftartenglättung für die Verbindung aus.
<b>Persistentes Bitmap-Caching</b>	Wählen Sie diese Option aus, um persistentes Bitmap-Caching für die Verbindung zu aktivieren.
<b>Desktopzusammensetzung</b>	Wählen Sie diese Option für die Aktivierung der Desktopzusammensetzung für die Verbindung aus.
<b>Cursoreinstellung deaktivieren</b>	Wählen Sie diese Option zum Deaktivieren der Cursoreinstellung für die Verbindung aus.
<b>Fensterinhalt beim Ziehen anzeigen</b>	Wählen Sie diese Option aus, um den Fensterinhalt beim Verschieben des Fensters anzuzeigen.
<b>Menü- und Fensteranimation</b>	Wählen Sie diese Option aus, um das Menü und die Fensteranimation für die Verbindung zu aktivieren.
<b>Weiterleitung des Servernamens verwenden</b>	Wählen Sie diese Option aus, um die Verwendung der Weiterleitung des Servernamens zu verwenden.
<b>Wenn Serverauthentifizierung fehlschlägt</b>	Wählen Sie diese Option aus, um die Maßnahme festzulegen, die ergriffen werden soll, wenn die Serverauthentifizierung fehlschlägt. <ul style="list-style-type: none"> <li>• Verbinden ohne Warnmeldung</li> <li>• Nicht verbinden</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>Warnen</li> </ul>

## Konfigurieren von Remote-Verbindungseinstellungen – Browser

Auf dieser Seite können Sie konfigurieren, auf welchen Remote-Verbindungsbrowser auf dem Wyse Software Thin Client zugegriffen werden kann.

**Tabelle 278. Konfigurieren von Grundeinstellungen**

Option	Beschreibung
<b>Verbindungsname</b>	Wählen Sie diese Option aus, um einen Namen für die Identifizierung der Verbindung zu definieren.
<b>Verbindung bei Anmeldung automatisch starten</b>	Wählen Sie diese Option aus, um das automatische Starten der Verbindung nachdem Sie sich angemeldet haben zu aktivieren.
<b>URL</b>	Wählen Sie diese Option zur Angabe der Standard-URL für den Browser aus.
<b>Sicherheitsstufe der Internetzone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer in der Internetzone festzulegen.
<b>Sicherheitsstufe der lokalen Zone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer in der lokalen Zone festzulegen.
<b>Sicherheitsstufe in der vertrauenswürdigen Zone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer auf vertrauenswürdigen Sites festzulegen.
<b>Sicherheitsstufe in der eingeschränkten Zone</b>	Wählen Sie diese Option aus, um die Sicherheitseinstellungen für Internet Explorer auf eingeschränkten Sites festzulegen.

**Tabelle 279. Einstellungen für IE-Favoriten (Internet Explorer) und vertrauenswürdige Sites konfigurieren**

Option	Beschreibung
<b>IE-Favoriten</b>	<p>Wählen Sie diese Option zum Hinzufügen Ihres Favoriten und vertrauenswürdigen Sites. Führen Sie folgende Schritte durch, um Ihre Favoriten und vertrauenswürdigen Sites hinzuzufügen:</p> <ul style="list-style-type: none"> <li>Klicken Sie auf <b>Site hinzufügen</b> und geben Sie den Namen des Ordners, die URL und eine Beschreibung ein.</li> <li>Klicken Sie auf <b>Verknüpfung erstellen</b>, um eine Verknüpfung für die Site zu erstellen.</li> <li>Klicken Sie auf <b>Entfernen</b> zum Löschen einer Site aus der Liste.</li> </ul> <p><b>ANMERKUNG:</b> Die URL muss mit https:// beginnen, wenn das Kontrollkästchen <b>Vertrauenswürdige Sites</b> ausgewählt wurde.</p>
<b>Serverüberprüfung (https:) für alle Sites der Zone erforderlich machen</b>	Wählen Sie diese Option zum Aktivieren einer Serverüberprüfung für alle Sites in der Zone aus.

**Tabelle 280. Internet Explorer – IE-Proxy-Einstellungen konfigurieren**

Option	Beschreibung
Proxy aktivieren	Wählen Sie diese Option aus, um den Proxy für den Browser zu konfigurieren.

**Tabelle 281. Konfigurieren von Firewall-Einstellungen**

Option	Beschreibung
Domain-Firewall	Wählen Sie diese Option aus, um die Domain-Firewall zu aktivieren.
Private Firewall	Wählen Sie diese Option aus, um die Private Firewall zu aktivieren.
Öffentliche Firewall	Wählen Sie diese Option aus, um die Öffentliche Firewall zu aktivieren.

**Tabelle 282. Aero-Einstellungen konfigurieren (gültig für Windows Embedded Standard 7)**

Option	Beschreibung
Aero	Wählen Sie diese Option für die Aktivierung der Funktion "Aero" für den Browser.  <div style="border-left: 1px solid black; padding-left: 10px;"> <p><b>ANMERKUNG:</b> Diese Funktion steht nur auf Windows Embedded Standard 7 zur Verfügung.</p> </div>

## Geräteinformationen konfigurieren

Verwenden Sie die Seite **Geräteinformationen**, um die Gerätedetails anzuzeigen.

**Tabelle 283. Geräteinformationen konfigurieren**

Option	Beschreibung
Standort	Geben Sie den Gerätestandort ein.
Kontakt	Geben Sie die Kontaktdaten des Geräts ein.
Benutzerdefiniert 1 bis 3	Geben Sie benutzerdefinierte Werte ein.

## Konfigurieren von Wyse Easy Setup-Versionseinstellungen

Die Seite **Wyse Easy Setup (2.0+)** dient zur Konfiguration der Wyse Easy Setup-Einstellungen für die Systemsteuerung und die Benutzeroberfläche.

**Tabelle 284. Konfigurieren des Systems**

Option	Beschreibung
<b>Ton</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Audiooptionen in der Systemsteuerung zu erhalten.
<b>Region &amp; Sprache</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Optionen für Region und Sprache in der Systemsteuerung zu erhalten.
<b>Datum &amp; Uhrzeit</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Optionen für Datum und Uhrzeit in der Systemsteuerung zu erhalten.
<b>Anzeige</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Anzeigeeoptionen in der Systemsteuerung zu erhalten.
<b>Netzwerk</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Netzwerkoptionen in der Systemsteuerung des lokalen Systems zu erhalten.
<b>Erleichterter Zugriff</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Optionen für erleichterten Zugriff in der Systemsteuerung zu erhalten.

**Tabelle 285. Konfigurieren von Peripheriegeräten**

Option	Beschreibung
<b>Maus</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Mausoptionen in der Systemsteuerung zu erhalten.
<b>Tastatur</b>	Aktivieren Sie dieses Kontrollkästchen, um Zugriff auf die Tastaturoptionen in der Systemsteuerung zu erhalten.

**Tabelle 286. Konfigurieren des Kioskmodus**

Option	Beschreibung
<b>Kioskmodus</b>	Aktivieren Sie dieses Kontrollkästchen, um den standardmäßigen Windows-Desktop durch Wyse Easy Setup-Desktop, Wyse Easy Setup Remote-Verbindungen und Wyse Easy Setup-Anwendungen zu ersetzen.
<b>Anwendungen</b>	Geben Sie die Einzelheiten zum Registrieren einer neuen Anwendung ein.
<b>Aktion beim Beenden der Anwendung</b>	Wählen Sie aus der Dropdownliste Aktion beim Beenden der Anwendung eine beliebige der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• Herunterfahren beim Beenden</li> <li>• Neu starten beim Beenden</li> <li>• Logout beim Beenden</li> <li>• Persistent beim Beenden</li> </ul> <p>Diese Einstellung gilt, wenn Sie mindestens eine der Remote-Verbindungen konfiguriert haben.</p>
<b>Anwendungszustand – Wiederholungsversuche</b>	Geben Sie in der Wyse Easy Setup-Shell an, wie oft versucht werden soll, die Anwendung zu öffnen.

Option	Beschreibung
Anwendungszustand – Wiederholungsintervall	Geben Sie das Zeitintervall für zwei aufeinanderfolgende Versuche zum Öffnen der Anwendung in der Wyse Easy Setup-Shell an.

Tabelle 287. Personalisierung konfigurieren

Option	Beschreibung
Hintergrund	Wählen Sie aus der Dropdownliste die gewünschte Grafik aus. Hinweis: Bevor Sie diesen Schritt durchführen, müssen Sie die Grafiken in das Datei-Repository hochladen.
Logo	Wählen Sie aus der Dropdownliste die Logo-Dateien aus, die in <b>Apps &amp; Daten &gt; Datei-Repository &gt; Bestand</b> hochgeladen werden.

Tabelle 288. Konfigurieren der Taskleiste

Option	Beschreibung
Datum & Uhrzeit	Wählen Sie diese Option zur Einstellung der Option für Datum und Uhrzeit auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
Ton	Wählen Sie diese Option zur Einstellung von Tonparametern auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
Netzwerk	Wählen Sie diese Option zur Ansicht von Netzwerkoptionen auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
Bildschirmtastatur	Wählen Sie diese Option zur Ansicht der Bildschirmtastatur auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.

Tabelle 289. Konfigurieren des Startmenüs

Option	Beschreibung
Abschaltung zulassen	Wählen Sie diese Option zum Herunterfahren des Systems auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
Neustart zulassen	Wählen Sie diese Option für den Systemneustart auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
Abmeldung zulassen	Wählen Sie diese Option für die Systemabmeldung auf der Wyse Easy Setup-Shell oder dem benutzerdefinierten Desktop.
Startmenü anzeigen	Ermöglicht den Zugriff auf das <b>Startmenü</b> in der Wyse Easy Setup-Benutzeroberfläche.
Hilfe aktivieren	Ermöglicht den Zugriff auf die <b>Hilfe</b> -Option in der Wyse Easy Setup-Benutzeroberfläche.

## Konfigurieren der VNC-Einstellungen

Verwenden Sie diese Seite zum Konfigurieren der VNC-Einstellungen.

**Tabelle 290. Konfigurieren der VNC-Einstellungen**

Option	Beschreibung
<b>VNC aktivieren</b>	Wählen Sie diese Option aus, um den VNC-Server zu aktivieren.
<b>VNC-Benutzeraufforderung</b>	Wenn Sie diese Option auswählen, müssen Sie VNC-Shadowing annehmen oder ablehnen.
<b>Erforderliches Kennwort für VNC-Benutzer</b>	Wählen Sie diese Option aus, um das VNC-Kennwort festzulegen.
<b>Primäres VNC-Kennwort</b>	Wählen Sie diese Option aus, um das VNC-Kennwort zu ändern. Geben Sie das neue Kennwort mit bis zu acht Zeichen ein.
<b>VNC-Kennwort für Modus "Nur anzeigen"</b>	Geben Sie das primäre Kennwort ein. Sie können das Kennwort nicht ändern.

## Konfigurieren von Domäneneinstellungen

Lesen Sie die Anweisungen auf dem Bildschirm, um das Wyse Software Thin Client-Gerät zur Active Directory-Domain des Unternehmens hinzuzufügen.

**Tabelle 291. Konfigurieren von Domäneneinstellungen**

Option	Beschreibung
<b>Domäne oder Arbeitsgruppe</b>	Wählen Sie diese Option aus, um die Domain auszuwählen. Wählen Sie aus der Dropdownliste Ihre bevorzugte Option.
<b>Name der Domäne oder Arbeitsgruppe</b>	Geben Sie den FQDN der Domain an.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein. Das Konto sollte über die Option <b>Zu Domain hinzufügen</b> verfügen.
<b>Kennwort</b>	Geben Sie das Kennwort ein.
<b>Konto-OE</b>	Geben Sie den Speicherort der Organisationseinheit ein, an dem das Computerobjekt erstellt werden soll.
<b>Automatische Anmeldung</b>	Aktivieren Sie das Kontrollkästchen zur Anzeige des Windows-Anmeldebildschirms.

# Verwalten von Geräten

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

Sie können die Geräteliste nach folgenden Kriterien sortieren:

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

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

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

Themen:

- [Methoden zum Registrieren Geräten bei Wyse Management Suite](#)
- [Suche nach einem Gerät unter Verwendung von Filtern](#)
- [Aktuellen Filter speichern](#)
- [Abfragen des Gerätestatus](#)
- [Sperren der Geräte](#)
- [Neustart der Geräte](#)
- [Deregistrierung der Geräte](#)
- [Wiederherstellen der Standardeinstellungen](#)
- [Ändern einer Gruppenzuweisung](#)
- [Senden von Nachrichten an Geräte](#)
- [Aktivieren der Geräte](#)
- [Anzeigen von Gerätedetails](#)
- [Gerätezusammenfassung verwalten](#)
- [Anzeigen von Systeminformationen](#)
- [Anzeigen von Geräteereignissen](#)
- [Anzeigen installierter Anwendungen](#)
- [Umbenennen des Thin Client](#)
- [Konfigurieren von Remote Shadowing-Verbindung](#)
- [Herunterfahren von Geräten](#)

- Tagging von Geräten
- Compliance-Status des Geräts
- Pull für Windows Embedded Standard oder ThinLinux-Abbild ausführen
- Aktualisieren von ThinLinux 1.x auf 2.1 und neuere Versionen
- Anfordern einer Protokolldatei
- Beheben von Störungen 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 Sie für eine private Cloud einen Thin Client durch die Angabe der Wyse Management Suite-URL und den Gruppentoken (optional) für die Gruppe, in der Sie dieses Gerät registrieren möchten. Geräte werden in der nicht verwalteten Gruppe registriert, wenn kein Gruppentoken angegeben wurde.

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

So registrieren Sie ThinOS Geräte manuell:

- 1 Klicken Sie auf dem Desktopmenü auf **System-Setup Zentrale Konfiguration**.  
Das Fenster **Zentrale-Konfiguration** wird angezeigt.
- 2 Klicken Sie auf die Registerkarte **WDA**. Der WDA-Dienst wird automatisch ausgeführt, sobald der Client-Startprozess abgeschlossen ist.  
**WMS** ist standardmäßig ausgewählt.
- 3 Wählen Sie das Kontrollkästchen **Wyse Management Suite aktivieren** zum Aktivieren der Wyse Management Suite aus.
- 4 Geben Sie den für die gewünschte Gruppe von Ihrem Administrator konfigurierten **Gruppenregistrierungsschlüssel** ein.
- 5 Wählen Sie die Option **Erweiterte WMS-Einstellungen aktivieren** aus und geben Sie die Details für den WMS-Server oder MQTT-Server ein.
- 6 Aktivieren oder deaktivieren Sie die CA-Validierung abhängig von Ihrem Lizenztyp. Public Cloud: Wählen Sie das Kontrollkästchen **CA-Validierung aktivieren** aus. Private Cloud: Wählen Sie das Kontrollkästchen **CA-Validierung aktivieren** aus, wenn Sie Zertifikate von einer bekannten Zertifizierungsstelle in Ihren Wyse Management Suite-Server importiert haben.  
Um die CA-Validierungsoption in der Private Cloud zu aktivieren, müssen Sie dasselbe selbstsignierte Zertifikat auch auf dem ThinOS Gerät installieren. Wenn Sie das selbstsignierte Zertifikat nicht auf dem ThinOS Gerät installiert haben, wählen Sie nicht das Kontrollkästchen **CA-Validierung aktivieren** aus. Sie können das Zertifikat mithilfe der Wyse Management Suite nach der Registrierung auf dem Gerät installieren und anschließend die CA-Validierungsoption aktivieren.

### ① ANMERKUNG:

Nehmen Sie an der Public-Cloud-Version von Wyse Management Suite im Rechenzentrum in den USA keine Änderungen an den Standarddetails des WMS-Servers und MQTT-Servers vor. Verwenden Sie für die Public-Cloud-Version von Wyse Management Suite im Rechenzentrum in Europa Folgendes:

- CCM-Server – [eu1.wysemanagementsuite.com](http://eu1.wysemanagementsuite.com)
- MQTT-Server – [eu1-pns.wysemanagementsuite.com:1883](http://eu1-pns.wysemanagementsuite.com:1883)

7 Klicken Sie auf **Schlüssel validieren**, um das Setup zu überprüfen. Das Gerät startet automatisch neu, nachdem der Schlüssel validiert wurde.

### ① 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-Konsole registriert.

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

### Vorbedingungen

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

### Schritte

- 1 Öffnen Sie die Anwendung **Wyse Geräte-Agent**.  
Das Fenster **Wyse Geräte-Agent** wird angezeigt.
- 2 Geben Sie die Geräteregistrierungsinformationen ein.
- 3 Wählen Sie in der Dropdown-Liste **Verwaltungsserver** die Option **Wyse Management Suite** aus.
- 4 Geben Sie die Serveradresse und die Portnummer in die jeweiligen Felder ein.
- 5 Geben Sie das Gruppentoken ein. Für einen einzelnen Mandanten ist die Eingabe eines Gruppentokens ein optionaler Schritt.
- 6 Klicken Sie auf **Registrieren**.  
Nachdem die Registrierung abgeschlossen ist, wird die Meldung **An Wyse Management Suite registriert** angezeigt.

## Registrieren von Linux Thin Clients über Wyse Geräte-Agent


### ① ANMERKUNG: Erstellen einer Gruppe ist eine Voraussetzung für die Registrierung von Thin Client bei der Wyse Management Suite. Weitere Informationen finden Sie unter [Hinzufügen einer Gruppe](#).

- 1 Öffnen Sie die Anwendung **Wyse Geräte-Agent** (WDA).  
Das Fenster **Wyse Geräte-Agent** wird angezeigt.
- 2 Geben Sie die Geräteregistrierungsinformationen ein.
- 3 In der Registerkarte **Wyse Management Suite** geben Sie die Serveradresse der Wyse Management Suite ein.
- 4 Geben Sie das Gruppentoken ein.  
  

### ① ANMERKUNG: Das Gruppentoken, das im Feld Gruppentoken eingegeben wird, wird nicht als Klartext angezeigt.
- 5 Klicken Sie auf **Registrieren**.  
Nachdem die Registrierung abgeschlossen ist, wird die Meldung **An Wyse Management Suite registriert** angezeigt.

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

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

- 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.
- 4 Geben Sie das Gruppentoken ein. Für einen einzelnen Mandanten ist die Eingabe eines Gruppentokens ein optionaler Schritt.  
 **ANMERKUNG: Das Gruppentoken, das im Feld Gruppentoken eingegeben wird, wird nicht als Klartext angezeigt.**
- 5 Klicken Sie auf **Registrieren**.

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

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

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

**WMSEnable**=yes\no

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

**GroupRegistrationKey**=GroupToken present in WMS Server

**CAValidation**=True/False

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

**WMSEnable**=yes

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

**GroupRegistrationKey**=defa-defadefa

**CAValidation**=True

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

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

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

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

**WMSEnable**=yes\no

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

**GroupRegistrationKey**=GroupToken present in WMS Server

**CAValidation**=True/False

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

**WMSEnable**=yes

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

**GroupRegistrationKey**=defa-defadefa

**CAValidation**=True

- 2 Speichern Sie die wlx.ini-Datei im Ordner „wyse\wlx“.
- 3 Gehen Sie zu **Einstellungen** und wechseln Sie auf dem ThinLinux Thin Client zum Administrator.
- 4 Gehen Sie zu **Verwaltung > INI**.
- 5 Geben Sie die FTP-Server-URL ein.
- 6 Klicken Sie auf **Speichern** und starten Sie den Thin Client neu.
- 7 Gehen Sie zu **Verwaltung > Wyse Geräte-Agent**.

In der Registerkarte „Wyse Geräte-Agent“ stehen die Wyse Verwaltungsserverdetails in dem entsprechenden Feld und der Client-Eintrag auf der Seite „Geräte“ des Wyse Verwaltungsservers zur Verfügung.

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

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

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

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

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

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

- 2 Legen Sie die wnos.ini-Datei im wnos-Ordner eines beliebigen FTP-Pfads ab.
- 3 Gehen Sie zu **Zentrale Konfiguration** auf dem ThinOS-Gerät.

- 4 Geben Sie in der Registerkarte **Allgemein** den FTP-Pfad bei Dateiservern oder den Pfad zum übergeordneten Ordner an.
- 5 Geben Sie die FTP-Anmeldeinformationen an, falls erforderlich. Wenn der FTP keine Anmeldeinformationen erfordert, können Benutzername und Kennwort anonym sein.
- 6 Klicken Sie auf **OK** und starten Sie dann den Thin Client neu.
- 7 Gehen Sie zu **Zentrale Konfiguration** auf dem ThinOS-Gerät.

In der Registerkarte **Wyse Geräte-Agent** stehen die Wyse Verwaltungsserverdetails in dem entsprechenden Feld und der Client-Eintrag auf der Seite „Geräte“ des Wyse Verwaltungsservers zur Verfügung.

## Registrieren von ThinLinux Thin Clients über Wyse Geräte-Agent

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

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

## Registering devices by using DHCP option tags

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

### ANMERKUNG:

Ausführliche Informationen zum Hinzufügen von DHCP-Option-Tags auf dem Windows Server finden Sie unter [Erstellen und Konfigurieren von DHCP-Options-Tags](#).

**Tabelle 292. Registrieren von Geräten mithilfe von DHCP-Options-Tags**

Options-Tag	Beschreibung
<b>Name</b> – WMS <b>Datentyp</b> – Zeichenfolge <b>Code</b> – 165 <b>Beschreibung</b> – WMS-Server-FQDN	Dieses Tag verweist auf die Wyse Management Suite-Server-URL. Beispiel: <b>wmserver.acme.com:443</b> , wobei <b>wmserver.acme.com</b> der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist. Links zum Registrieren Ihrer Geräte in der Wyse Management Suite in einer öffentlichen Cloud finden Sie unter <a href="#">Erste Schritte mit der Wyse Management Suite in einer öffentlichen Cloud</a> .
<b>Name</b> – MQTT <b>Datentyp</b> – Zeichenfolge <b>Code</b> – 166 <b>Beschreibung</b> – MQTT-Server	Dieses Tag leitet das Gerät zum Wyse Management Suite-Pushbenachrichtigungsserver (PNS) weiter. Bei einer Installation in einer privaten Cloud wird das Gerät an den MQTT-Dienst auf dem Wyse Management Suite-Server weitergeleitet. Beispiel: <b>wmservername.domain.com:1883</b> .  Zum Registrieren Ihrer Geräte in der öffentlichen Cloud der Wyse Management Suite sollte das Gerät auf die PNS-(MQTT-)Server in der öffentlichen Cloud verweisen. Beispiel:  US1:us1-pns.wysemanagementsuite.com  EU1:eu1-pns.wysemanagementsuite.com

Options-Tag	Beschreibung
<p><b>Name</b> – CA-Validation</p> <p><b>Datentyp</b> – Zeichenfolge</p> <p><b>Code</b> – 167</p> <p><b>Beschreibung</b> – Zertifizierungsstellenprüfung</p>	<p>Sie können die Option „CA-Validierung“ aktivieren oder deaktivieren, wenn Sie Ihre Geräte mit der Wyse Management Suite in der privaten Cloud registrieren. Standardmäßig ist die CA-Validierung in der öffentlichen Cloud aktiviert. Sie können die CA-Validierung auch in der öffentlichen Cloud deaktivieren.</p> <p>Geben Sie <b>Wahr</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server von einer bekannten Zertifizierungsstelle importiert haben.</p> <p>Geben Sie <b>Falsch</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server nicht von einer bekannten Zertifizierungsstelle importiert haben.</p>
<p><b>Name</b> – GroupToken</p> <p><b>Datentyp</b> – Zeichenfolge</p> <p><b>Code</b> – 199</p> <p><b>Beschreibung</b> – Gruppentoken</p>	<p>Dieser Tag ist erforderlich, um ThinOS-Geräte in der Wyse Management Suite in einer öffentlichen oder privaten Cloud zu registrieren.</p> <p>Dieser Tag ist optional zum Registrieren des Windows Embedded Standard oder von ThinLinux-Geräten in der Wyse Management Suite in einer privaten Cloud. Wenn der Tag nicht verfügbar ist, werden die Geräte während der Installation vor Ort automatisch in der unverwalteten Gruppe registriert.</p>

Weitere Informationen zu den Sicherheitsumgebungen für Kunden finden Sie unter [Wyse-Geräte-Agent](#).

## Geräte mit DNS-SRV-Eintrag registrieren

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

- Windows Embedded Systems – 13.0 oder spätere Versionen
- Thin Linux – 2.0.24 oder spätere Versionen
- ThinOS – 8.4 Firmware oder spätere Versionen

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

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

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

**Tabelle 293. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags**

URL/Tag	Beschreibung
<p><b>Eintragsname</b> – _WMS_MGMT</p> <p><b>Eintrags-FQDN</b> – _WMS_MGMT._tcp.&lt;Domänenname&gt;</p> <p><b>Eintragstyp</b> – SRV</p>	<p>Dieser Eintrag verweist auf die Wyse Management Suite Server-URL. Beispiel: <b>wmserver.acme.com:443</b>, wobei <b>wmserver.acme.com</b> der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist. Links zum Registrieren Ihrer Geräte in der Wyse Management Suite in einer öffentlichen Cloud finden Sie unter <a href="#">Erste Schritte mit der Wyse Management Suite in einer öffentlichen Cloud</a>.</p> <p><b>ANMERKUNG:</b> Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird.</p>
<p><b>Eintragsname</b> – _WMS_MQTT</p> <p><b>Eintrags-FQDN</b> – _WMS_MQTT._tcp.&lt;Domänenname&gt;</p>	<p>Dieser Eintrag leitet das Gerät zum Wyse Management Suite-Pushbenachrichtigungsserver (PNS) weiter. Bei einer Installation in einer privaten Cloud wird das Gerät an den MQTT-Dienst auf dem</p>

URL/Tag	Beschreibung
<b>Eintragstyp</b> – SRV	<p>Wyse Management Suite-Server weitergeleitet. Beispiel:  <b>wmsservername.domain.com:1883.</b></p> <p><b>ANMERKUNG: MQTT ist bei der neuesten Version der Wyse Management Suite optional.</b></p> <p>Zum Registrieren Ihrer Geräte in der öffentlichen Cloud der Wyse Management Suite sollte das Gerät auf die PNS-(MQTT-)Server in der öffentlichen Cloud verweisen. Beispiel:</p> <p>US1 –<a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>EU1 –<a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p>
<b>Eintragsname</b> – _WMS_GROUPTOKEN <b>Eintrags-FQDN</b> – _WMS_GROUPTOKEN.<Domain> <b>Eintragstyp</b> – TEXT	<p>Dieser Datensatz ist erforderlich, um ThinOS-Geräte in der Wyse Management Suite in einer öffentlichen oder privaten Cloud zu registrieren.</p> <p>Dieser Datensatz ist optional zum Registrieren des Windows Embedded Standard oder von ThinLinux-Geräten in der Wyse Management Suite in einer privaten Cloud. Wenn der Eintrag nicht verfügbar ist, werden die Geräte während der Installation vor Ort automatisch in der unverwalteten Gruppe registriert.</p> <p><b>ANMERKUNG: Das Gruppentoken ist optional für die neueste Version von Wyse Management Suite in einer privaten Cloud.</b></p>
<b>Eintragsname</b> – _WMS_CAVALIDATION <b>Eintrags-FQDN</b> – _WMS_CAVALIDATION.<Domain> <b>Eintragstyp</b> – TEXT	<p>Sie können die Option „CA-Validierung“ aktivieren oder deaktivieren, wenn Sie Ihre Geräte mit der Wyse Management Suite in der privaten Cloud registrieren. Standardmäßig ist die CA-Validierung in der öffentlichen Cloud aktiviert. Sie können die CA-Validierung auch in der öffentlichen Cloud deaktivieren.</p> <p>Geben Sie <b>Wahr</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server von einer bekannten Zertifizierungsstelle importiert haben.</p> <p>Geben Sie <b>Falsch</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server nicht von einer bekannten Zertifizierungsstelle importiert haben.</p> <p><b>ANMERKUNG: CA Validation ist bei der neuesten Version der Wyse Management Suite optional.</b></p>

Weitere Informationen zu den Sicherheitsumgebungen für Kunden finden Sie unter [Wyse-Geräte-Agent](#).

## Suche nach einem Gerät unter Verwendung von Filtern

So suchen Sie ein Gerät mithilfe von Filtern:

- 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
  - 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.
- 6 Wählen Sie aus der Dropdownliste **OS-Version** eine OS-Version.
- 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.

## Aktuellen Filter speichern

Nach der Auswahl Ihrer benötigten Filteroptionen können Sie die Filter als Gruppe speichern. Gehen Sie folgendermaßen vor, um die aktuellen Filter zu speichern:

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

## Abfragen des Gerätestatus

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

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

# Sperrn der Geräte

Um das registrierte Gerät zu sperren, gehen Sie wie folgt vor:

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

# Neustart der Geräte

Um das registrierte Gerät neu zu starten, gehen Sie wie folgt vor:

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

# Deregistrierung der Geräte

Um das registrierte Gerät zu deregistrieren, gehen Sie wie folgt vor:

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

## ① ANMERKUNG:

- Die Option „Aufhebung der Registrierung erzwingen“ kann verwendet werden, um das Gerät zu entfernen, wenn keine Kommunikation zwischen dem Server und dem Client besteht. Das Gerät wird in den nicht verwalteten Zustand versetzt und lässt sich aus dem Servereintrag entfernen.
- Die Aktionen „Registrierung aufheben“ und „Aufhebung der Registrierung erzwingen“ können auch über die WES WDA UI durchgeführt werden kann.

# Wiederherstellen der Standardeinstellungen

So setzen Sie Ihr ThinOS-basiertes Gerät auf die werksseitigen Standardeinstellungen zurück:

- 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

Zum Ändern einer Gruppenzuweisung gehen Sie wie folgt vor:

- 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 Nachrichten an Geräte

Um Nachrichten an Geräte zu senden, gehen Sie wie folgt vor:

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

## Aktivieren der Geräte

Wenn ein Gerät ausgeschaltet ist oder sich im Energiesparmodus befindet und Sie das Gerät aktivieren möchten, gehen Sie wie folgt vor:

- 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 von Gerätedetails

Um Gerätedetails anzuzeigen, führen Sie die folgenden Schritte aus:

- 1 Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
- 2 Wenden Sie die Filter an, um das bevorzugte Gerät zu finden. Weitere Informationen finden Sie unter [Suche nach einem Gerät mithilfe von Filtern](#).  
Die Liste bevorzugter Geräte wird angezeigt.

- 3 Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.

## Gerätezusammenfassung verwalten

So können Sie Informationen zu Anmerkungen, Gruppenzuordnung, Warnungen und Gerätekonfiguration anzeigen und verwalten.

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

## Anzeigen von Systeminformationen

Um die Systeminformationen anzuzeigen, gehen Sie folgendermaßen vor:

- 1 Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
- 2 Wenden Sie die Filter an, um das bevorzugte Gerät zu finden. Weitere Informationen finden Sie unter [Suche nach einem Gerät mithilfe von Filtern](#).  
Die Liste bevorzugter Geräte wird angezeigt.
- 3 Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
- 4 Klicken Sie auf **Systeminfo**.  
Die folgenden Systeminformationen werden angezeigt:

## Anzeigen von Geräteereignissen

So können Sie Informationen zu den zu einem Gerät gehörigen Systemereignissen anzeigen:

- 1 Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
- 2 Wenden Sie die Filter an, um das bevorzugte Gerät zu finden. Weitere Informationen finden Sie unter [Suche nach einem Gerät mithilfe von Filtern](#).  
Die Liste bevorzugter Geräte wird angezeigt.
- 3 Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
- 4 Klicken Sie auf der Seite **Gerätedetails** auf die Registerkarte **Ereignisse**.  
Die Ereignisse auf dem Gerät werden angezeigt.

# Anzeigen installierter Anwendungen

So zeigen Sie die installierten Anwendungen auf dem Gerät an:

- 1 Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
- 2 Wenden Sie die Filter an, um das bevorzugte Gerät zu finden. Weitere Informationen finden Sie unter [Suche nach einem Gerät mithilfe von Filtern](#).  
Die Liste bevorzugter Geräte wird angezeigt.
- 3 Klicken Sie auf eines der angezeigten Geräte.  
Die Seite **Gerätedetails** wird angezeigt.
- 4 Klicken Sie auf die Registerkarte **installierte Apps**.  
Der Liste der installierten Anwendungen auf dem Gerät wird angezeigt.  
Diese Option ist für Windows Embedded Standard-, Linux- und ThinLinux-Geräte verfügbar. Die folgenden Attribute werden auf der Seite angezeigt:
  - Name
  - Herausgeber
  - Version
  - Installiert auf

## ANMERKUNG:

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

# Umbenennen des Thin Client

Verwenden Sie diese Seite zum Ändern des Hostnamens von Thin Clients, die auf Windows Embedded Standard, ThinLinux und ThinOS Betriebssystemen ausgeführt werden. Um den Host-Namen zu ändern, gehen Sie folgendermaßen vor:

- 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 Embedded 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.

### Alert

You are about to send a Change Host Name command to the selected device.  
Please enter a new host name for the selected device.

The device needs to be restarted for the new hostname to take effect. Please restart now or specify a future time.

Reboot:  Time:  :

Do you wish to proceed?

---

Abbildung 5. Warnung

**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 Shadowing-Verbindung

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

**ANMERKUNG:** Das Wyse Management Suite-Portal unterstützt maximal fünf Remote Shadowing-Sitzungen pro Mandant.

- 1 Klicken Sie auf der Seite **Geräte** auf das Gerät.
- 2 Wählen Sie aus der Dropdownliste **Mehr Optionen** die Option **Remote-Spiegelung (VNC)**.

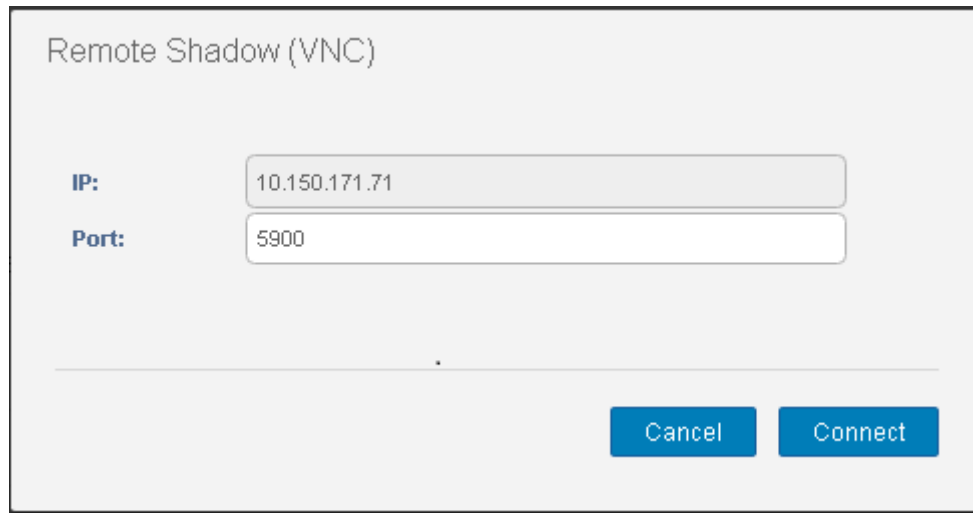


Abbildung 6. Remote-Spiegelung (VNC)

Die IP-Adresse und die Port-Nummer des Ziel-Thin Clients wird im Dialogfeld **Remote-Spiegelung (VNC)** angezeigt.

**ANMERKUNG:** Die Standardportnummer ist 5900.

- 3 Ändern Sie die Portnummer des Ziel-Thin Clients. (optional)
- 4 Klicken Sie auf **Verbinden**, um eine Remote-Sitzung mit dem Ziel-Thin Client zu initiieren.

## Herunterfahren von Geräten

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

- 1 Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
- 2 Wenden Sie die Filter an, um das bevorzugte Gerät zu finden. Weitere Informationen finden Sie unter [Suche nach einem Gerät mithilfe von Filtern](#).  
Die Liste bevorzugter Geräte wird angezeigt.
- 3 Klicken Sie in der Dropdown-Liste **Weitere Optionen** auf **Jetzt herunterfahren**.  
Der Remote-Befehl zum Abschalten des Geräts wird an das ausgewählte Gerät gesendet. Das Gerät antwortet auf den Server und der Befehl wird erfolgreich ausgeführt.

**ANMERKUNG:** Die Option **Jetzt herunterfahren** ist für Thin Clients unter Linux nicht aktiviert.

## Tagging von Geräten

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

- 1 Klicken Sie auf **Geräte**.  
Es wird die Seite **Gerät** angezeigt.
- 2 Wenden Sie die Filter an, um das bevorzugte Gerät zu finden. Weitere Informationen finden Sie unter [Suche nach einem Gerät mithilfe von Filtern](#).  
Die Liste bevorzugter Geräte wird angezeigt.
- 3 Wählen Sie ein oder mehrere Geräte aus. Klicken Sie in der Dropdownliste **Weitere Optionen** auf **Gerät mit Tag versehen**.  
Das Fenster **Geräte-Tag einrichten** wird angezeigt.
- 4 Geben Sie den bevorzugten Tag-Namen ein.
- 5 Klicken Sie auf **Tag einrichten**.

# Compliance-Status des Geräts

Standardmäßig werden die folgenden Farben als Gerätestatus angezeigt:

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

Der Standardwert kann von 1 bis 99 Tage geändert werden.

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

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

## Pull für Windows Embedded Standard oder ThinLinux-Abbild ausführen

Verwenden Sie die Wyse Management Suite, um einen Pull für ein Betriebssystem oder das BIOS von einem Thin Client auszuführen.

**ANMERKUNG:** Sie können ThinLinux von 1.x auf 2.x aktualisieren.

### 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 1.4 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.

Zum Ausführen der Windows Embedded Standard oder ThinLinux Image-Pull-Vorgangs:

- 1 Wechseln Sie zur Geräteseite **Windows Embedded Standard** oder **ThinLinux**.
- 2 Wählen Sie die Option **OS-Abbild abrufen** aus der Dropdownliste **Weitere Maßnahmen** aus.
- 3 Geben Sie folgende Informationen ein bzw. wählen Sie sie aus:
  - **Namen des Images:** Geben Sie einen Namen für das Abbild an. Zum Ersetzen des Abbilds mit einem ähnlichen Namen und Bilddateien, die nicht erfolgreich abgeschlossen wurden, klicken Sie auf **Name überschreiben**.
  - **Datei-Repository:** Wählen Sie aus der Dropdownliste das Datei-Repository aus, in das das Abbild hochgeladen werden soll. Es gibt zwei Arten von Datei-Repositories:
    - Lokales Repository
    - Wyse Management Suite Remote-Repository
  - **Pull-Typ:** Wählen Sie entweder **Standard** oder **Erweitert** basierend darauf, welchen Pull-Typ Sie benötigen.
    - Wenn der Pull-Typ **Standard** ausgewählt ist, werden die folgenden Optionen angezeigt:
      - Komprimieren
      - OS
      - BIOS
      - Wiederherstellung – Für ThinLinux 2.x
    - Wenn der Pull-Typ **Erweitert** ausgewählt ist, wird eine Dropdownliste für die Auswahl der Vorlagen angezeigt. Wählen Sie eine Vorlage aus, die standardmäßig verfügbar ist.

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

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

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

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

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

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

## 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

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

Um das ThinLinux 2.x-Abbild vorzubereiten, gehen Sie wie folgt vor:

- 1 Rufen Sie die Website [www.dell.com/support](http://www.dell.com/support) auf.
- 2 Klicken Sie auf **Produkt-Support**, geben Sie die **Service-Tag-Nummer** Ihres Thin Clients ein, und drücken Sie dann die **Eingabetaste**.

**ANMERKUNG:** Wenn Sie über keine Service-Tag-Nummer verfügen, suchen Sie manuell nach Ihrem Thin Client-Modell.

- 3 Klicken Sie auf **Treiber und Downloads**.
- 4 Wählen Sie in der Dropdown-Liste **Betriebssystem** die Option **ThinLinux**.
- 5 Laden Sie die Add-ons **merlin\_nonpxe-4.0.1-0 0.04.amd64.deb** und **wda\_3.4.6-05\_amd64.tar** herunter.
- 6 Kopieren Sie das heruntergeladene Add-on zu `<Laufwerk C>/wms/localrepo/repository/thinClientsApps/`.
- 7 Gehen Sie auf dem Thin Client mit ThinLinux 2.x zu **Einstellungen > Verwaltung > Wyse-Geräte-Agent**.
- 8 Registrieren Sie das Gerät auf dem Wyse Management Suite-Server.
- 9 Schließen Sie das Fenster **Einstellungen**.

**ANMERKUNG:** Wenn das Fenster "Einstellungen" nicht geschlossen wird, wird der Fehler Profil gesperrt angezeigt, nachdem Sie das Abbild bereitgestellt haben.

- 10 Melden Sie sich bei der Wyse Management Suite-Konsole an.
- 11 Erstellen Sie die Anwendungsrichtlinie für die Add-ons **merlin\_nonpxe-4.0.1-0 0.04.amd64.deb** und **wda\_3.4.6-05\_amd64.tar** und stellen Sie sie bereit.
- 12 Starten Sie den Thin Client neu.
- 13 Melden Sie sich beim Wyse Management Suite-Server an.
- 14 Navigieren Sie zur Seite "Gerät" und stellen Sie sicher, dass die Merlin- und WDA-Versionen aktualisiert werden.
- 15 Klicken Sie auf das registrierte Gerät und navigieren Sie zu **Weitere Maßnahmen > OS-Abbild abrufen**.  
Das Fenster **OS-Abbild abrufen** wird angezeigt.
- 16 Geben Sie den Namen des Abbilds ein.
- 17 Wählen Sie in der Dropdown-Liste "Datei-Repository" das Datei-Repository aus.
- 18 Wählen Sie die Pull-Operation aus, die Sie durchführen möchten.
  - **Standard:** Aktivieren Sie das Kontrollkästchen **OS + Wiederherstellung** und rufen Sie das Abbild ab (komprimiert/unkomprimiert).
  - **Erweitert:** Wählen Sie die Vorlage **Compress\_OS\_Recovery\_Commandsxml/uncompress\_OS\_Recovery\_CommandsXml** und rufen Sie das Abbild ab.

## 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 1.4 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

Um ThinLinux mit der Wyse Management Suite zu aktualisieren, führen Sie die folgenden Schritte aus:

- 1 Rufen Sie die Website [www.dell.com/support](http://www.dell.com/support) auf.
- 2 Klicken Sie auf **Produkt-Support**, geben Sie die **Service-Tag-Nummer** Ihres Thin Clients ein, und drücken Sie dann die **Eingabetaste**.  
**ANMERKUNG:** Wenn Sie über keine Service-Tag-Nummer verfügen, suchen Sie manuell nach Ihrem Thin Client-Modell.
- 3 Klicken Sie auf **Treiber und Downloads**.
- 4 Wählen Sie in der Dropdown-Liste **Betriebssystem** die Option **ThinLinux**.
- 5 Blättern Sie auf der Seite nach unten und gehen Sie wie folgt vor:
  - Laden Sie die Add-ons **Platform\_util-1.0.26-0.3.x86\_64.rpm**, **wda-2.1.23-00.01.x86\_64.rpm** und **merlin-nonpxe\_3.7.7-00.05\_amd64.deb** herunter.
  - Laden Sie die neueste **2.1.0.01\_3040\_16GB\_merlin.exe** oder **2.2.0.00\_3040\_merlin\_16GB.exe** ThinLinux Version 2.x Image-Datei herunter ( ).
- 6 Navigieren Sie auf dem Thin Client zu **Einstellungen > Verwaltung > Wyse-Geräte-Agent**.
- 7 Registrieren Sie das Gerät auf dem Wyse Management Suite-Server.
- 8 Melden Sie sich bei der Wyse Management Suite-Konsole an.
- 9 Erstellen Sie eine Anwendungsrichtlinie für **Platform\_util-1.0.26-0.3.x86\_64.rpm**, **wda-2.1.23-00.01.x86\_64.rpm** und **merlin-nonpxe\_3.7.7-00.05\_amd64.deb** und stellen Sie sie bereit.
- 10 Starten Sie den Thin Client neu.
- 11 Melden Sie sich beim Wyse Management Suite-Server an.
- 12 Kopieren Sie das heruntergeladene Abbild (Datei **2.2.0.00\_3040\_merlin\_16GB.exe**) nach **Laufwerk C>/wms/localrepo/repository/osimages/zipped/**.  
**ANMERKUNG:** Das Abbild im komprimierten Ordner wird in einen gültigen Ordner extrahiert. Der Extrahierungsvorgang kann 10–15 Minuten dauern.
- 13 Melden Sie sich bei der Wyse Management Suite-Konsole an.
- 14 Rufen Sie **Anwendungen und Daten > OS-Abbild-Repository > WES/ThinLinux** auf und überprüfen Sie, ob das ThinLinux-Abbild verfügbar ist.
- 15 Navigieren Sie zu **Apps und Daten > OS-Abbildrichtlinien (WES/ThinLinux)** und klicken Sie auf **Richtlinie hinzufügen**.
- 16 Konfigurieren Sie im Fenster "Richtlinie hinzufügen" die folgenden Optionen:
  - OS-Typ: ThinLinux
  - OS-Subfilter: ThinLinux (ThinLinux)
  - Regel: Nur Upgrade/Diese Version erzwingen  
**ANMERKUNG:** Wählen Sie das abgerufene/neue Abbild, das beim Erstellen der Richtlinie in das Repository kopiert wurde.
- 17 Aktualisieren Sie die anderen erforderlichen Felder nach Bedarf, und klicken Sie auf **Speichern**.
- 18 Planen Sie den Job.
- 19 Klicken Sie auf dem Client auf **Jetzt aktualisieren**, um das Abbild zu aktualisieren.

# Anfordern einer Protokolldatei

Um ein Geräteprotokoll von Windows Embedded Standard-, ThinOS- und ThinLinux-Geräten anzufordern, führen Sie die folgenden Schritte aus:

- 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.

The screenshot shows the 'Device Details' page in the Wyse Management Suite. At the top, there are buttons for 'Query', 'Restart', and 'Unregister', along with a 'More Actions' dropdown menu. The main content area is divided into two columns. The left column contains a device image and a list of details: Compliance Status (green dot), Device Name (WIE10Device1), Device Type (Thin Client (Wyse 5020 thin client)), OS Version (Win 10 Enterprise 2015 LTSP), Last Logged In User (WIE10Device1\Admin), Configuration Group (test11), and Agent Version (12.1.1.25). The right column contains: Serial Number, Mac Address, IP Address, Connection Type (Ethernet), and Last Check-in (1 minute ago). Below the details is a navigation bar with tabs: Summary, System Info, Events, Installed Apps (23), Device Log (1), and Troubleshooting. The 'Device Log' tab is selected and has a circled '1' above it. Below the navigation bar, there is a 'Request Log File' button with a circled '2' above it. Below the button, it says 'Current log updated at: 6 days ago' and 'To download log file, click here.' Below this text is a circled '3'.

Abbildung 7. Pull für Protokolldatei

## ① ANMERKUNG:

- Das Gerät muss aktiviert sein, um einen Pull für eine Protokolldatei auszuführen.
- Das ThinOS-Gerät lädt die Systemprotokolle hoch.
- Der Windows Embedded Standard lädt Protokolle des Wyse Geräte-Agenten und der Windows-Ereignisanzeige hoch.
- Linux oder ThinLinux lädt Protokolle des Wyse Geräte-Agenten und Systemprotokolle hoch.
- Linux oder ThinLinux lädt die Protokolldatei im `tar`-Format hoch; wenn Sie das Extrahieren der Dateien auf einem Windows-System vornehmen, dann benötigen Sie 7zip oder eine äquivalente Datei.

# Beheben von Störungen auf Ihrem Gerät

Zum Anzeigen und Verwalten der Informationen zur Behebung von Störungen, führen Sie die folgenden Schritte aus:

- 1 Klicken Sie auf der Seite **Gerätedetails** auf die Registerkarte **Fehlerbehebung**.
- 2 Klicken Sie auf **Screenshot anfordern**.  
Sie können den Screenshot des Thin Client mit oder ohne Zustimmung des Clients erstellen. Wenn das Kontrollkästchen **Zustimmung des Benutzers erforderlich machen** ausgewählt ist, wird auf dem Client eine Meldung angezeigt. Diese Option gilt nur für Windows Embedded Standard-, Linux- und ThinLinux-Geräte.
- 3 Klicken Sie auf **Prozessliste anfordern**, um die Liste der ausgeführten Verfahren auf dem Thin Client anzufordern.
- 4 Klicken Sie auf **Dienstliste anfordern**, um die Liste der ausgeführten Dienste auf dem Thin Client anzufordern.
- 5 Klicken Sie auf **Überwachung starten** für den Zugriff auf die Konsole Leistungsmetrik.

Auf der Konsole **Leistungsmetrik** werden die folgenden Details angezeigt:

- Durchschnittliche CPU-Last in der letzten Minute.
- Durchschnittliche Speichernutzung in der letzten Minute

# Anwendungen und Daten

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

- 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. Weitere Informationen finden Sie unter [Verwalten von Jobs](#).

Themen:

- [Anwendungsrichtlinie](#)
- [Abbildrichtlinie](#)
- [Datei-Repository verwalten](#)

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

### Wichtige Hinweise für Windows-basierte Geräte:

- Unterstützt die Installation für Windows-basierte Anwendungen mit der Erweiterung .msi, .exe, .msu, .msp.

Eine Anwendung mit einer anderen Erweiterung wird heruntergeladen auf `%systemdrive%\wyse\WDA` Ex: "C:\wyse\WDA

- Für die Bereitstellung von EXE-Anwendungen unter Verwendung der Wyse Management Suite befolgen Sie die Methode der automatischen Installation. Sie müssen gegebenenfalls die entsprechenden Parameter für die automatische Installation eingeben. Zum Beispiel **VMware-Horizon-Client-4.6.1-6748947.exe /silent /install /norestart**
- Unterstützt Skriptbereitstellungen mit Dateierweiterungen .bat, .cmd, .ps1, .vbs.

Ein Skript mit anderer Erweiterung wird heruntergeladen auf `%systemdrive%\wyse\WDA` Ex: "C:\wyse\WDA.

- Skripte, die unter Verwendung der Wyse Management Suite bereitgestellt werden, sollten nicht-interaktiv sein, das heißt, dass während der Installation keine Benutzermaßnahme erforderlich ist.
- Wenn in der erweiterten Anwendungsrichtlinie ein Skript/eine EXE-Datei vorhanden ist, die einen anderen Wert als 0 zurückgibt, wird dies als Fehler betrachtet.
- Wenn in der erweiterten Anwendungsrichtlinie die Vorinstallation fehlschlägt, wird die Anwendungsinstallation nicht fortgesetzt.
- Skripte/EXE-Dateien, die unter Verwendung der Standardanwendung bereitgestellt werden, sind erfolgreich, und der Fehlercode wird im Jobstatus aktualisiert.

- Für Anwendungen mit der Erweiterung msi/msu/msp werden Standardfehlercodes berichtet. Wenn eine Anwendung „REBOOT\_REQUIRED“ zurückgibt, wird das Gerät einmal zusätzlich neu gestartet.

#### Wichtige Hinweise für Linux-Geräte:

- Unterstützt die Installation für Linux-basierte Anwendungen mit der Erweiterung .bin, .deb für ThinLinux 2.0 und .rpm für Thin Linux 1.0.
- Unterstützt Skriptbereitstellungen für ThinLinux-Geräte mit der Erweiterung .sh.
- Wenn in der Standard- oder erweiterten Anwendungsrichtlinie ein Skript/eine deb./rpm.-Datei vorhanden ist, das bzw. die einen anderen Wert als 0 zurückgibt, wird dies als Fehler betrachtet.
- Wenn in der erweiterten Anwendungsrichtlinie die Vorinstallation fehlschlägt, wird die Anwendungsinstallation nicht fortgesetzt.

## Konfigurieren einer Thin-Client-Anwendungsbestandsaufnahme

Gehen Sie zum Konfigurieren des Thin Client-Bestands folgendermaßen vor:

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

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

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

## Konfigurieren der Wyse Software Thin-Client-Anwendungsbestandsaufnahme

Gehen Sie zum Konfigurieren des Wyse Software Thin Client-Bestands folgendermaßen vor:

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

# Erstellen und Bereitstellen von Standardanwendungsrichtlinie für Thin Clients

So stellen Sie Thin Clients eine Standardanwendungsrichtlinie zur Verfügung:

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

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

- 3 Klicken Sie auf **Apps & Daten**.

Die Seite **Apps & Daten** wird angezeigt.

- 4 Klicken Sie in den **App-Richtlinien** auf **Thin Client**.
- 5 Klicken Sie auf **Richtlinie hinzufügen**.

Das Fenster **Standard-App-Richtlinie hinzufügen** wird angezeigt.

- 6 Geben Sie den **Richtliniennamen** ein.
- 7 Wählen Sie eine **Gruppe** aus der Dropdownliste aus.
- 8 Wählen Sie die **Aufgabe** aus der Dropdownliste aus.
- 9 Wählen Sie in der Dropdownliste den **Betriebssystemtyp** aus.
- 10 Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
- 11 Wählen Sie eine **Anwendung** aus der Dropdownliste aus.

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

- 12 Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
- 13 Die Zeitüberschreitung zeigt eine Meldung auf dem Client an, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt. Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client angezeigt werden soll.
- 14 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).
- 15 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**

- 16 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.

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

## Erstellen und Bereitstellen einer erweiterten Anwendungsrichtlinie auf Thin Clients

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

- 1 Kopieren Sie die Anwendung und die Skripte vor/nach der Installation (falls erforderlich) zur Bereitstellung auf den Thin Clients. Speichern Sie die Anwendung und die Skripte vor/nach der Installation im Ordner **thinClientApps** im lokalen Repository oder dem Wyse Management Suite-Repository.
- 2 Gehen Sie zu **Apps&DatenAppInventory** und wählen Sie **Thin Client** um zu überprüfen, ob die Anwendung registriert ist.
- 3 Klicken Sie auf **Thin Client** unter **App-Richtlinien**.
- 4 Klicken Sie auf **Erweiterte Richtlinie hinzufügen**. Die Seite **Erweiterte App-Richtlinie hinzufügen** wird angezeigt.
- 5 So erstellen Sie einen Zeitplan für eine Anwendungsrichtlinie:
  - a Geben Sie den **Richtliniennamen** ein.
  - b Wählen Sie eine **Gruppe** aus der Dropdownliste aus.
  - c Aktivieren Sie das Kontrollkästchen **Untergruppen**, um die Richtlinie auf Untergruppen anzuwenden.
  - d Wählen Sie die **Aufgabe** aus der Dropdownliste aus.
  - e Wählen Sie in der Dropdownliste den **Betriebssystemtyp** aus.
  - f Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
  - g Klicken Sie auf **App hinzufügen** und wählen Sie einen oder mehrere Anwendungen unter **Apps**. Für jede Anwendung können Sie ein Skript vor und nach der Installation unter **Vorinstallation**, **Nachinstallation** und **Installations-Parameter** wählen. Wenn Sie möchten, dass das System nach der erfolgreichen Installation der Anwendung neu starten soll, wählen Sie **Neustart**. Klicken Sie auf **App hinzufügen** und wiederholen Sie den Schritt zum Hinzufügen mehrerer Anwendungen.

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

**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.

- h Wenn Sie diese Richtlinie auf einem bestimmten Betriebssystem oder einer bestimmten Plattform bereitstellen möchten, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter**.
- i Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client im Feld **Zeitüberschreitung (1–999 Min.)** angezeigt werden soll. Die Zeitüberschreitung zeigt eine Meldung auf dem Client an, die Ihnen Zeit zum Speichern der Änderungen verschafft, bevor die Installation beginnt.
- j Damit eine Verzögerung bei der Ausführung der Richtlinie ermöglicht wird, markieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Dropdownmenüs aktiviert:

- Wählen Sie aus 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).
- k 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
- l Aktivieren Sie das Kontrollkästchen **Überprüfung des Schreibfilters überspringen**, um die Schreibfiltervorgänge zu überspringen. Diese Option gilt für Geräte mit Windows Embedded Standard-Betriebssystem und Wyse Software Thin-Client-Geräte.
- m 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.
- 6 Klicken Sie auf **Speichern**. Eine Nachricht wird angezeigt, um es Administratoren zu ermöglichen, diese Richtlinie für Geräte basierend auf der Gruppe zu planen. Wählen Sie **Ja**, um die Anwendungsrichtlinie sofort oder zu einem auf der Seite **App-Richtlinienjob** geplanten Datum und Uhrzeit auszuführen.
- Der Anwendungsrichtlinienjob kann ausgeführt werden:
- a **Sofort** – Der Server führt den Job sofort aus.
  - b **Gemäß Zeitzone des Geräts** – Der Server erstellt einen Job gemäß der Zeitzone für jedes Gerät und plant den Job mit dem ausgewählten Datum/Uhrzeit in der Zeitzone des Geräts.
  - c **Gemäß ausgewählter Zeitzone** – Der Server erstellt einen Job, der an dem Datum und zu der Uhrzeit der angegebenen Zeitzone geplant sein muss.
- 7 Klicken Sie auf **Vorschau** und "Zeitplan festlegen" auf der nächsten Seite, um den Job zu erstellen.
- 8 Sie können den Status des Jobs auf der Seite **Jobs** überprüfen.

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

So stellen Sie eine Standardanwendungsrichtlinie für Wyse Software Thin Clients bereit:

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

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

- 3 Klicken Sie auf **Apps & Daten**.

Die Seite **Apps & Daten** wird angezeigt.

- 4 Klicken Sie in den **App-Richtlinien** auf **Wyse Software Thin Client**.
- 5 Klicken Sie auf **Richtlinie hinzufügen**.

Das Fenster **Standard-App-Richtlinie hinzufügen** wird angezeigt.

- 6 Geben Sie den **Richtliniennamen** ein.
- 7 Wählen Sie eine **Gruppe** aus der Dropdownliste aus.
- 8 Wählen Sie die **Aufgabe** aus der Dropdownliste aus.

- 9 Wählen Sie in der Dropdownliste den **Betriebssystemtyp** aus.
  - 10 Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
  - 11 Wählen Sie eine **Anwendung** aus der Dropdownliste aus.
  - 12 Um diese Richtlinie für ein bestimmtes Betriebssystem oder eine Plattform bereitzustellen, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter** aus.
  - 13 Zeitüberschreitung zeigt eine Meldung auf dem Client an, die Ihnen vor der Installation Zeit zum Speichern der Änderungen verschafft. Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client angezeigt werden soll.
  - 14 Damit eine Verzögerung bei der Ausführung der Richtlinie ermöglicht wird, markieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Dropdownmenüs aktiviert:
    - Wählen Sie aus 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).
  - 15 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`
- 16 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.
  - 17 Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen.  
Eine Meldung wird angezeigt, um den Administrator das Planen dieser Richtlinie auf Geräten basierend auf der Gruppe zu gewähren.
  - 18 Wählen Sie **Ja** aus, um einen Job auf derselben Seite zu planen.
  - 19 Der Anwendungsrichtlinienjob kann ausgeführt werden:
    - a **Sofort** – Der Server führt den Job sofort aus.
    - b **Nach Zeitzone des Geräts** – Der Server erstellt einen Job für jede Gerätezeitzone und plant den Job für das ausgewählte Datum bzw. die Uhrzeit der Zeitzone des Geräts.
    - c **Nach ausgewählter Zeitzone** – Der Server erstellt einen Job zur Durchführung an dem Datum bzw. der Uhrzeit der zugewiesenen Zeitzone.
  - 20 Klicken Sie zum Erstellen eines Jobs auf **Vorschau** und Zeitpläne werden auf der nächsten Seite angezeigt.
  - 21 Sie können den Status des Jobs durch Navigation zur Seite **Jobs** überprüfen.

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

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

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

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

- 3 Klicken Sie auf **Apps & Daten**.

Die Seite **Apps & Daten** wird angezeigt.

- 4 Klicken Sie auf **Wyse Software Thin Clients** in **App-Richtlinien**.
- 5 Klicken Sie auf **Erweiterte Richtlinie hinzufügen**. Die Seite **Erweiterte App-Richtlinie hinzufügen** wird angezeigt.
- 6 So erstellen Sie einen Zeitplan für eine Anwendungsrichtlinie:
  - a Geben Sie den **Richtliniennamen** ein.
  - b Wählen Sie eine **Gruppe** aus der Dropdownliste aus.
  - c Aktivieren Sie das Kontrollkästchen **Untergruppen**, um die Richtlinie auf Untergruppen anzuwenden.
  - d Wählen Sie die **Aufgabe** aus der Dropdownliste aus.
  - e Wählen Sie in der Dropdownliste den **Betriebssystemtyp** aus.
  - f Aktivieren Sie das Kontrollkästchen **Dateien nach Erweiterungen filtern**, um die Anwendungen zu filtern.
  - g Klicken Sie auf **App hinzufügen** und wählen Sie einen oder mehrere Anwendungen unter **Apps**. Für jede Anwendung können Sie ein Skript vor und nach der Installation unter **Vorinstallation**, **Nachinstallation** und **Installations-Parameter** wählen. Wenn Sie möchten, dass das System nach der erfolgreichen Installation der Anwendung neu starten soll, wählen Sie **Neustart**. Klicken Sie auf **App hinzufügen** und wiederholen Sie den Schritt zum Hinzufügen mehrerer Anwendungen.

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

- h Wenn Sie diese Richtlinie auf einem bestimmten Betriebssystem oder einer bestimmten Plattform bereitstellen möchten, wählen Sie entweder **OS-Subtypfilter** oder **Plattformfilter**.
- i Geben Sie die Anzahl der Minuten an, die das Meldungsdialogfeld auf dem Client im Feld **Zeitüberschreitung (1–999 Min.)** angezeigt werden soll. Zeitüberschreitung zeigt eine Meldung auf dem Client an, die Ihnen vor der Installation Zeit zum Speichern der Änderungen verschafft.
- j Damit eine Verzögerung bei der Ausführung der Richtlinie ermöglicht wird, markieren Sie das Kontrollkästchen **Verzögerung bei der Richtlinienausführung zulassen**. Wenn diese Option ausgewählt ist, werden die folgenden Dropdownmenüs aktiviert:
  - Wählen Sie aus 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).
- k 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**
- l Aktivieren Sie das Kontrollkästchen **Überprüfung des Schreibfilters überspringen**, um die Schreibfiltervorgänge zu überspringen. Diese Option gilt für Geräte mit Windows Embedded Standard-Betriebssystem.
- m 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.
- 7 Klicken Sie auf **Speichern**. Eine Nachricht wird angezeigt, um es Administratoren zu ermöglichen, diese Richtlinie für Geräte basierend auf der Gruppe zu planen. Wählen Sie **Ja**, um die Anwendungsrichtlinie sofort oder zu einem auf der Seite **App-Richtlinienjob** geplanten Datum und Uhrzeit auszuführen.

Der Anwendungsrichtlinienjob kann ausgeführt werden:

- a **Sofort** – Der Server führt den Job sofort aus.
  - b **Nach Zeitzone des Geräts** – Der Server erstellt einen Job für jede Gerätezeitzone und plant den Job für das ausgewählte Datum bzw. die Uhrzeit der Zeitzone des Geräts.
  - c **Gemäß ausgewählter Zeitzone** – Der Server erstellt einen Job, der an dem Datum und zu der Uhrzeit der angegebenen Zeitzone geplant sein muss.
- 8 Klicken Sie auf **Vorschau** und "Zeitplan festlegen" auf der nächsten Seite, um den Job zu erstellen.

9 Sie können den Status des Jobs durch Navigation zur Seite **Jobs** überprüfen.

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

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

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

Informationen zur Bereitstellung einer Richtlinie finden Sie unter [Erstellen und Bereitstellen einer Standardanwendungsrichtlinie für Thin Clients](#) und [Erstellen und Bereitstellen einer Standardanwendungsrichtlinie für Wyse Software Thin Clients](#).

## Abbildrichtlinie

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

- Hinzufügen der Windows Embedded Standard-Betriebssystem- und ThinLinux-Abbilder zum Repository
- Hinzufügen von ThinOS-Firmware zum Repository
- Hinzufügen von Teradici-Firmware zum Repository
- Erstellen von Windows Embedded Standard- und ThinLinux-Abbildrichtlinien.

## Hinzufügen von Windows Embedded Standard-Betriebssystem- und ThinLinux-Abbildern zum Bestand

Vorbedingungen

- Wenn Sie die Wyse Management Suite mit Cloudbereitstellung verwenden, rufen Sie **Portalverwaltung > Konsoleinstellungen > Datei-Repository** auf. Klicken Sie auf **Version 1.4 herunterladen**, um die Datei **WMS\_Repo.exe** herunterzuladen, und installieren Sie das Wyse Management Suite-Repository-Installationsprogramm. Weitere Informationen finden Sie unter [Zugriff auf das Datei-Repository](#).
- Wenn Sie die Wyse Management Suite mit Bereitstellung vor Ort verwenden, wird das lokale Repository während der Installation der Wyse Management Suite installiert.

So fügen Sie ein Abbild zum Repository-Ordner auf Ihrem System hinzu:

- 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

So fügen Sie ein Betriebssystemabbild zum ThinOS-Firmware-Repository hinzu:

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

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

## Hinzufügen von ThinOS-Paketdatei zu Repository

Um eine Paketdatei zum ThinOS-Repository hinzuzufügen, gehen Sie wie folgt vor:

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

**ANMERKUNG:**

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

## Hinzufügen von ThinOS-BIOS-Datei zu Repository

Um eine BIOS-Datei zum ThinOS-Repository hinzuzufügen, gehen Sie wie folgt vor:

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

7 Klicken Sie auf **Hochladen**.

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

## Hinzufügen von Teradici-Firmware zum Repository

So fügen Sie ein Betriebssystemabbild zum Teradici-Firmware-Repository hinzu:

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

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

## Erstellen von Windows Embedded Standard- und ThinLinux-Abbildrichtlinien

Zum Konfigurieren von Windows Embedded Standard- und ThinLinux-Abbildrichtlinien gehen Sie wie folgt vor:

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

# Datei-Repository verwalten

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

Gehen Sie folgendermaßen vor, um eine neue Datei hinzuzufügen:

- 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

Zum Hinzufügen eines Hintergrundbilds zu Wyse Management Suite-Repositorys führen Sie folgendes aus:

- 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 zeigen Sie darauf.
- 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 Wählen Sie eine Richtliniengruppe aus.
- 2 Klicken Sie auf **Richtlinien bearbeiten** und wählen Sie **WES**.

- 3 Wählen Sie **Desktoperlebnis** und klicken Sie auf **Dieses Element konfigurieren**.
- 4 Wählen Sie **Desktop-Hintergrundbild** aus.
- 5 Wählen Sie aus der Dropdownliste die Hintergrundbild-Datei.
- 6 Klicken Sie auf **Speichern und Veröffentlichen**.

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

# Verwalten von Regeln

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

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

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 einer Regel](#)
- [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**. Zum Bearbeiten einer Registrierungsregel gehen Sie wie folgt vor:

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

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

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

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

- 6 Klicken Sie auf **Speichern**.

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

Zum Erstellen von Regeln für die automatische Zuweisung nicht verwalteter Geräte gehen Sie wie folgt vor:

**ANMERKUNG:** Stellen Sie sicher, dass Sie über die Pro Lizenzversion der Wyse Management Suite verfügen.

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

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

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

Zum Bearbeiten von Regeln für die automatische Zuweisung nicht verwalteter Geräte gehen Sie wie folgt vor:

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

## Deaktivieren und Löschen einer Regel

Zum Deaktivieren von Regeln und Löschen deaktivierter Regeln für die automatische Zuweisung nicht verwalteter Geräte gehen Sie wie folgt vor:

- 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 löschen**.  
Die Regel wird gelöscht.

## Speichern der Regelreihenfolge

Wenn mehrere Regeln vorhanden sind, können Sie die Reihenfolge ändern, in der eine Regel auf die Geräte angewendet wird. Zum Ändern der Reihenfolge einer Regel, führen Sie die folgenden Schritte aus:

- 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**.

## Hinzufügen einer Regel für Warnmeldungen

So fügen Sie eine Regel für Warnmeldungen hinzu:

- 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

Zum Bearbeiten einer Regel für Warnmeldungen gehen Sie wie folgt vor:

- 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 Verwaltungskonsolle planen und verwalten.

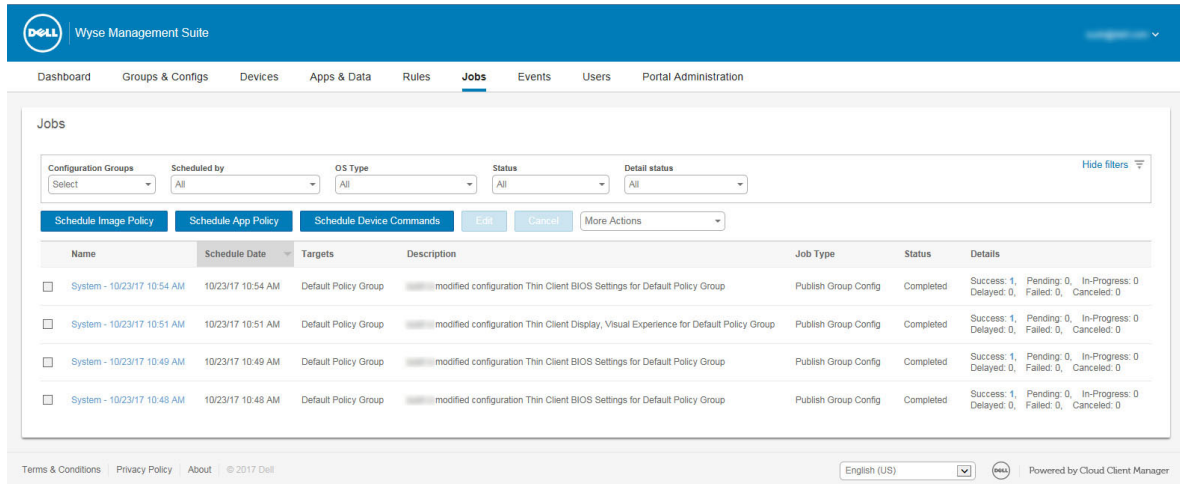


Abbildung 8. Jobs

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. Dies sind die möglichen Optionen:
  - Admin
    - App-Richtlinie
    - Abbildrichtlinie
    - Gerätebefehle
  - System
    - Gruppenkonfiguration veröffentlichen
    - Andere
- **Betriebssystemtyp** – Wählen Sie das Betriebssystem aus dem Dropdownmenü. Dies sind die möglichen Optionen:
  - ThinOS
  - WES
  - Linux
  - Thin Linux
  - Wyse Software Thin Client
- **Status** – Wählen Sie aus dem Dropdownmenü den Status des Jobs aus. Dies sind die möglichen Optionen:
  - Geplant
  - Wird ausgeführt/In Verarbeitung
  - Abgeschlossen
  - Abgebrochen

- Fehlgeschlagen
- **Detailstatus** – Wählen Sie aus dem Dropdownmenü den Status im Detail. Dies sind die möglichen Optionen:
  - 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

Themen:

- [BIOS-Administratorkennwort synchronisieren](#)
- [Suchen eines geplanten Jobs mithilfe von Filtern](#)
- [Planen der Abbildrichtlinie](#)
- [Planen einer Anwendungsrichtlinie](#)
- [Planen des Gerätebefehlsjobs](#)

## BIOS-Administratorkennwort synchronisieren

Wählen Sie aus dem Dropdownmenü **Weitere Maßnahmen** die Option **BIOS-Administratorkennwort synchronisieren**. So synchronisieren Sie das BIOS-Administratorkennwort:

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

## Suchen eines geplanten Jobs mithilfe von Filtern

In diesem Abschnitt wird beschrieben, wie Sie geplante Jobs in der Verwaltungskonsolle suchen und verwalten. So suchen Sie einen geplanten Job mithilfe von Filtern:

- 1 Klicken Sie auf **Jobs**.  
Die Seite **Jobs** wird angezeigt.
- 2 Wählen Sie aus der Dropdownliste **Konfigurationsgruppen** entweder die Standardrichtliniengruppe oder die Gruppen, die durch einen Administrator hinzugefügt wurden.
- 3 Wählen Sie aus der Dropdownliste **Geplant von** den Planer aus, der die Planungsaktivität ausführt.  
Dies sind die möglichen Optionen:
  - Admin
    - App-Richtlinie
    - Abbildrichtlinie
    - Gerätebefehle
  - System
    - Gruppenkonfiguration veröffentlichen

- Andere
- 4 Wählen Sie aus der Dropdownliste **Betriebssystemtyp** das Betriebssystem aus.  
Dies sind die möglichen Optionen:
    - ThinOS
    - WES
    - Linux
    - Thin Linux
    - Wyse Software Thin Client
  - 5 Wählen Sie aus der Dropdownliste **Status** den Status des Jobs aus.  
Dies sind die möglichen Optionen:
    - Geplant
    - Wird ausgeführt/In Verarbeitung
    - Abgeschlossen
    - Abgebrochen
    - Fehlgeschlagen
  - 6 Wählen Sie aus der Dropdownliste **Detailstatus** den Status im Detail aus.  
Dies sind die möglichen Optionen:
    - 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 [Sync BIOS Admin Password](#).

## Planen der Abbildrichtlinie

Die Abbildrichtlinie ist kein wiederkehrender Job. Jeder Befehl ist spezifisch für ein Gerät. So erstellen Sie einen Zeitplan für eine Abbildrichtlinie:

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

## Planen einer Anwendungsrichtlinie

Die Anwendungsrichtlinie ist kein wiederkehrender Job. Jeder Befehl ist spezifisch für ein Gerät. So erstellen Sie einen Zeitplan für eine Anwendungsrichtlinie:

- 1 Klicken Sie auf der Seite **Jobs** auf die Option **Anwendungsrichtlinie planen**.  
Der Bildschirm **App-Richtlinienjob** wird angezeigt.
- 2 Wählen Sie eine Richtlinie aus der Dropdownliste aus.

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

## Planen des Gerätebefehljobs

Führen Sie die folgenden Schritte aus, um einen Gerätebefehljob zu planen:

- 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. Dies sind die möglichen Optionen:
  - Neustart
  - Wake on LAN (Reaktivieren von LAN)
  - Herunterfahren
  - Abfrage

Gerätebefehle sind wiederkehrende Jobs. An ausgewählten Wochentagen und zu einem bestimmten Zeitpunkt werden die Befehle an die ausgewählten Geräte gesendet.

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

# Verwalten von Ereignissen

In diesem Abschnitt wird beschrieben, wie Sie alle Ereignisse und Warnungen im Verwaltungssystem mithilfe der Verwaltungskonsolle anzeigen können. Darüber hinaus enthält er Anweisungen zum Anzeigen der Überprüfungsereignisse und Warnungen zu Systemüberwachungszwecken.

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

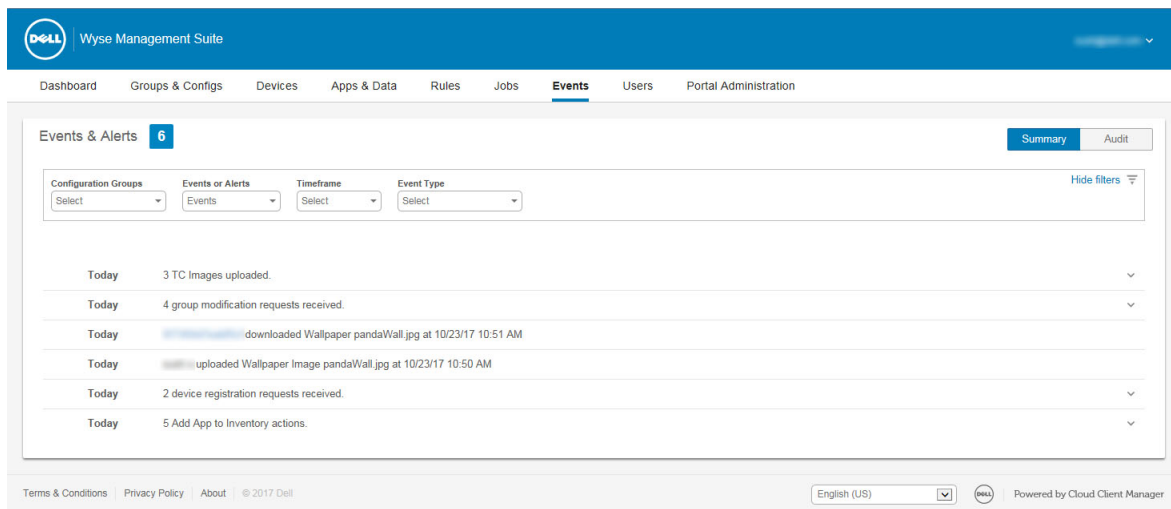


Abbildung 9. Ereignisse

## Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern

So suchen Sie ein Ereignis oder eine Warnung mithilfe von Filtern:

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

- Diese Woche
  - Benutzerdefiniert
- 5 Wählen Sie von der Dropdownliste **Ereignistyp** eines der folgenden Betriebssysteme aus:  
Alle Ereignisse werden in bestimmte Gruppen klassifiziert. Die verfügbaren Optionen im Dropdownmenü sind:
- Zugriff
  - Registrierung
  - Konfiguration
  - Remote-Befehle
  - Verwaltung
  - Konformität

## Suchen eines Ereignisses oder einer Warnung mithilfe von Filtern

So suchen Sie ein Ereignis oder eine Warnung mithilfe von Filtern:

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

# Überwachungsprotokoll anzeigen

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

- 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.

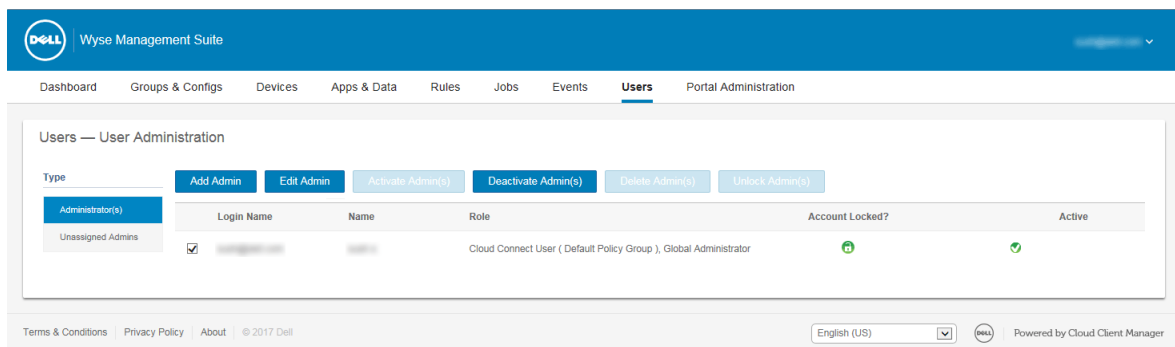
# Verwalten von Benutzern

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.
  - Ein Betrachter hat Nur-Lese-Zugriff auf alle Daten und kann Berechtigungen zugewiesen bekommen, um spezifische Echtzeitbefehle auszuführen, wie z. B. Herunterfahren und Neu starten.

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

- Administrator hinzufügen
- Administrator bearbeiten
- Administrator(en) aktivieren
- Administrator(en) deaktivieren
- Administrator(en) löschen
- Administrator(en) entsperren



**Abbildung 10. Administratorkennwort**

- **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

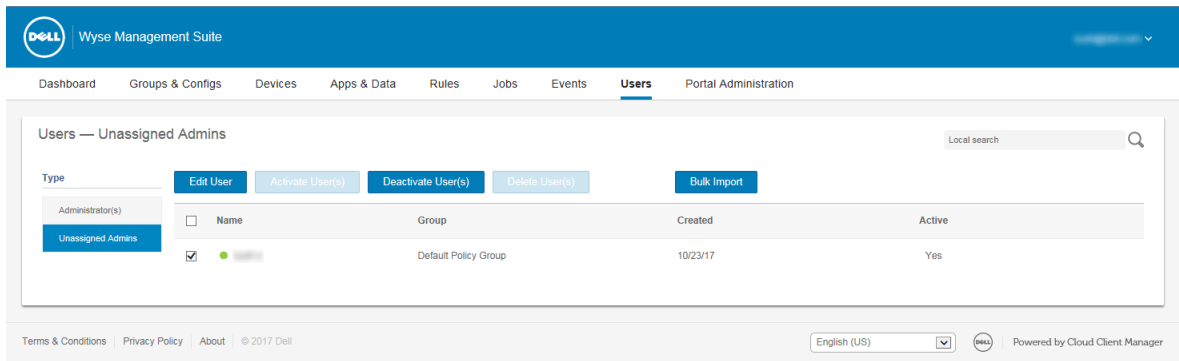


Abbildung 11. Nicht zugewiesene Administratoren

**ANMERKUNG:** Zum Importieren von Benutzern aus der CSV-Datei, klicken Sie auf Massenimport.

Themen:

- [Hinzufügen eines neuen Administratorprofils](#)
- [Bearbeiten eines Administratorprofils](#)
- [Deaktivieren eines Administratorprofils](#)
- [Löschen eines Administratorprofils](#)
- [Bearbeiten eines Benutzerprofils](#)
- [Importieren der CSV-Datei](#)

## Hinzufügen eines neuen Administratorprofils

Gehen Sie folgendermaßen vor, um ein neues Administratorprofil hinzuzufügen:

- 1 Klicken Sie auf **Benutzer**.
- 2 Klicken Sie auf **Administrator(en)**.
- 3 Klicken Sie auf **Administrator hinzufügen**.  
Das Fenster **Neuer Administrator-Benutzer** wird angezeigt.
- 4 Geben Sie Ihre E-Mail-ID und den Benutzernamen in die entsprechenden Felder ein.
- 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:
    - 1 Wählen Sie im Abschnitt **Rollen** aus der Dropdown-Liste **Rolle** 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

2 Führen Sie im Abschnitt **Kennwort** die folgenden Schritte aus:

- a Geben Sie das benutzerdefinierte Kennwort ein.
- b Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche **Zufälliges Kennwort generieren**.

7 Klicken Sie auf **Speichern**.

## Bearbeiten eines Administratorprofils

So bearbeiten Sie ein Administratorprofil:

1 Klicken Sie auf **Benutzer**.

2 Klicken Sie auf **Administrator(en)**.

3 Klicken Sie auf **Administrator bearbeiten**.

Das Fenster **Administratorbenutzer bearbeiten** wird angezeigt.

4 Geben Sie Ihre E-Mail-ID und den Benutzernamen in die entsprechenden Felder ein.

**ANMERKUNG:** Beim Aktualisieren des Anmeldenamens, sind Sie gezwungen, sich von der Konsole abzumelden. Melden Sie sich bei der Konsole unter Verwendung des aktualisierten Konto-Anmeldenamens an.

5 Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie auf die Registerkarte **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:

1 Wählen Sie im Abschnitt **Rollen** aus der Dropdown-Liste **Rolle** die Option **Administratorrolle**.

2 Führen Sie im Abschnitt **Kennwort** die folgenden Schritte aus:

- a Geben Sie das benutzerdefinierte Kennwort ein.
- b Zur Generierung eines zufälligen Kennworts, wählen Sie die Optionsschaltfläche **Zufälliges Kennwort generieren**.

6 Klicken Sie auf **Speichern**.

## 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. So deaktivieren Sie einen Administratorbenutzer:

1 Klicken Sie auf **Benutzer**.

2 Klicken Sie auf **Administrator(en)**.

3 Wählen Sie in der Liste einen Benutzer aus und klicken Sie auf **Administrator(en) deaktivieren**.

Es wird ein Benachrichtigungsfenster angezeigt.

- 4 Klicken Sie auf **OK**.


## Löschen eines Administratorprofils

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

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

## Bearbeiten eines Benutzerprofils

So bearbeiten Sie ein Benutzerprofil:

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

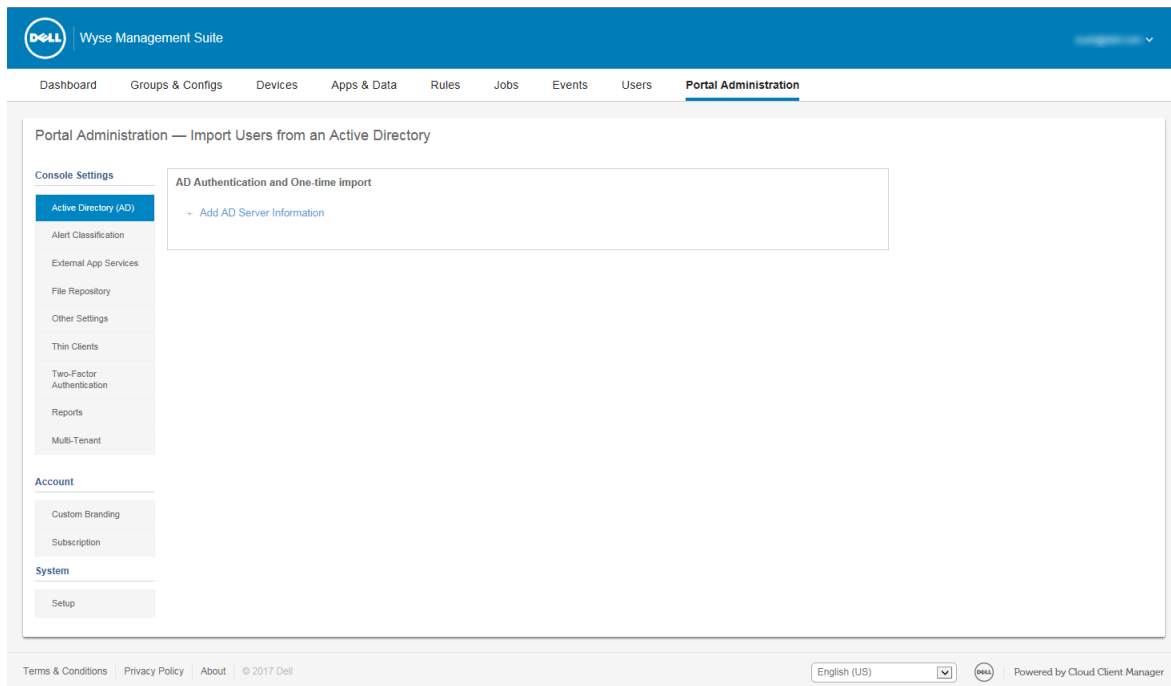
## Importieren der CSV-Datei

Zum Importieren von Benutzern aus der CSV-Datei gehen Sie wie folgt vor:

- 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**.

# Portalverwaltung

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



**Abbildung 12. Portaladministrator**

Themen:

- Hinzufügen der Active Directory-Serverinformationen
- Importieren von Benutzern in die öffentliche Cloud über Active Directory
- Warnungsklassifizierungen
- Erstellen eines API-Kontos (Application Programming Interface)
- Zugriff auf Datei-Repository
- Andere Einstellungen konfigurieren
- Verwalten von Teradici-Konfigurationen
- Aktivieren der Zweifaktor-Authentifizierung
- Generieren von Berichten
- Aktivieren von Multi-Tenant Konten
- Aktivieren von benutzerdefiniertem Branding
- Verwalten des Lizenzabonnements
- Verwalten des System-Setup

# Hinzufügen der Active Directory-Serverinformationen

Zum Importieren von Active Directory-Benutzern in die private Cloud der Wyse Management Suite gehen Sie wie folgt vor:

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

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

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

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

- 8 Klicken Sie auf **Anmelden**.
- 9 Klicken Sie auf der Seite **Benutzergruppe** auf **Gruppenname** und geben Sie den Gruppennamen ein.
- 10 Im Feld **Suche** geben Sie den Gruppennamen ein, den Sie auswählen möchten.
- 11 Wählen Sie eine Gruppe aus.  
Die ausgewählte Gruppe wird in den rechten Fensterbereich auf der Seite verschoben.
- 12 Klicken Sie auf **Weiter**.
- 13 Klicken Sie auf **Benutzer importieren**

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

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

- 14 Zum Zuweisen unterschiedlicher Rollen oder Berechtigungen wählen Sie einen Benutzer aus und klicken Sie auf **Benutzer bearbeiten**.  
Nach der Zuweisung der Rollen zum Active Directory-Benutzer, werden sie auf die Registerkarte **Administratoren** auf der Seite **Benutzer** verschoben.

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

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

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

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

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

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

- 1 Importieren Sie das AD-Domänen-Server-Stammzertifikat mit dem Schlüssel-Tool manuell in den Java-Schlüsselspeicher. Zum Beispiel: `<C:\Program Files\DELL\WMS\jdk1.8.0_152\jre\bin>keytool.exe -importcert -alias "WIN-O358EA52H8H" -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 öffentlichen Cloud konfigurieren

So konfigurieren Sie die Active Directory-Verbunddienste (ADFS) in einer öffentlichen Cloud:

- 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 **Informationensymbol (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 **Informationensymbol (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.

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

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

- 5 Klicken Sie auf **Speichern**.
- 6 Nach dem Speichern der Metadatendatei klicken Sie auf **Konfiguration aktualisieren**.

**ANMERKUNG:**

- Mandanten können sich durch die Verwendung ihrer AD-Anmeldeinformationen, die in ihren ADFS konfiguriert sind, an- und abmelden. Sie müssen sicherstellen, dass die AD-Benutzer auf den Wyse Management Suite-Server importiert wurden. Klicken Sie auf der Anmeldeseite auf **Anmelden** und geben Sie Ihre Domänenanmeldeinformationen ein. Sie müssen die E-Mail-Adresse Ihres AD-Benutzers eingeben und sich anmelden.
- Weitere Informationen zur ADFS Dokumentation finden Sie unter [Technet.microsoft.com/en-us/windowsserver/dd448613](https://technet.microsoft.com/en-us/windowsserver/dd448613).
- Nachdem die ADFS-Testverbindung erfolgreich war, importieren Sie die Benutzer über den im Remote-Repository vorhandenen AD Connector.
- Um einen Benutzer in die öffentliche Cloud zu importieren, muss ein Remote-Repository installiert sein.

# Importieren von Benutzern in die öffentliche Cloud über Active Directory

- 1 Informationen zum Herunterladen und Installieren des Datei-Repositorys finden Sie unter [Zugriff auf Datei-Repository](#). Das Repository muss unter Verwendung des Firmennetzwerks installiert werden und muss Zugriff auf den AD-Server haben, um Benutzer abzurufen.
- 2 Registrieren Sie das Repository in der öffentlichen Cloud. Nach der Registrierung befolgen Sie die Schritte in der UI zum Importieren der Benutzer in die öffentliche Cloud der Wyse Management Suite. Sie können die Rollen des AD-Benutzers nach dem Import in die öffentliche Cloud der Wyse Management Suite bearbeiten.
- 3 Informationen zur Einrichtung von ADFS in der öffentlichen Cloud finden Sie unter [Funktion „Active Directory-Verbunddienste“ in einer öffentlichen Cloud konfigurieren](#).

## Warnungsklassifizierungen

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

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

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

- Warnung über Gerätezustand
- Gerät nicht eingecheckt

## Erstellen eines API-Kontos (Application Programming Interface)

In diesem Bereich können Sie gesicherte API-Konten (Application Programming Interface) erstellen. Dieser Dienst bietet die Möglichkeit zur Erstellung spezieller Konten.

Zum Konfigurieren des externen Anwendungsdiensts führen Sie die folgenden Schritte aus:

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

## Zugriff auf Datei-Repository

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

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

der Installation registrieren Sie das Wyse Management Suite-Repository am Wyse Management Suite-Verwaltungsserver durch Angabe der erforderlichen Informationen.

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

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

#### **ANMERKUNG:**

- Die **Image Pull**-Vorlagen werden nicht automatisch in anderen Repositorys repliziert. Sie müssen diese Dateien manuell kopieren.
- Die Funktion zur Dateireplikation wird nur von Repositorys der Wyse Management Suite 1.4 und späteren Versionen unterstützt.
- Sie können kein selbst signiertes Zertifikat des Remote-Repositorys in den Wyse Management Suite-Server importieren. Wenn die CA-Validierung für das Remote-Repository aktiviert ist, schlägt die Replikation von Dateien aus dem Remote-Repository in das lokale Repository fehl.

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

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

#### **ANMERKUNG:**

- a Wenn die CA-Validierung des Wyse Management Suite Servers aktiviert ist, sollte das Zertifikat im Client vorhanden sein. Alle Vorgänge, wie z. B., Apps und Daten, Bildabruf, sind erfolgreich. Wenn das Zertifikat nicht im Client vorhanden ist, bietet der Wyse Management Suite Server eine generische Audit-Ereignisbenachrichtigung **Validierung der Zertifizierungsstelle fehlgeschlagen** auf der Seite **Ereignisse**. Alle Vorgänge, wie z. B., Apps und Daten, Bildabruf, waren nicht erfolgreich.
- b Wenn die CA-Validierung von Wyse ManagementSuite 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**.

## Andere Einstellungen konfigurieren

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

- **Lizenzablaufwarnung auf Dashboardseite verwerfen** – Markieren Sie dieses Kontrollkästchen zum Deaktivieren der Anzeige der Lizenzablaufwarnung auf der Seite **Dashboard**.

- **Optionen für Advanced Dell Wyse Cloud Connect auf Seite zur Konfiguration der Android Einstellungsrichtlinie aktivieren (Hinweis: nur professionelle Ebene)** – Wählen Sie diese Option zum Aktivieren der erweiterten Dell Wyse Cloud Connect-Optionen auf der Richtlinienkonfigurationsseite für Android-Einstellungen.
- **Taktintervall** – Geben Sie die Zeit ein. Das Gerät sendet alle 60 bis 360 Minuten ein Taktsignal.
- **Check-in-Intervall** – Geben die Zeit ein. Das Gerät sendet ein vollständiges Überprüfungssignal alle 8 bis 24 Stunden.
- **Konformitätswarnung "Nicht eingecheckt"** – Geben Sie die Anzahl an Tagen an, bevor ein Gerät eine **Konformitätswarnung "Nicht eingecheckt"** auslöst. Der Bereich liegt zwischen 1 und 99.
- **Zeitüberschreitung WMS-Konsole**: Geben Sie die Leerlaufzeit in Minuten ein, nach der der Benutzer von der Konsole abgemeldet wird. Diese Einstellung kann von jedem globalen Administrator konfiguriert werden. Der Standardwert beträgt 30 Minuten.

## Verwalten von Teradici-Konfigurationen

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

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

## Aktivieren der Zweifaktor-Authentifizierung

Sie müssen mindestens zwei aktive globale Administratorbenutzer im System haben.

Erstellen Sie zwei oder mehrere globale Administratoren vor dem Fortfahren mit der Aufgabe. So aktivieren Sie die Zwei-Faktor-Authentifizierung:

- 1 Melden Sie sich am Wyse Management Suite-Portal an und klicken Sie auf die Registerkarte **Portaladministrator**.
- 2 Klicken Sie auf **Zweifaktor-Authentifizierung** unter **Konsoleneinstellungen**.
- 3 Sie müssen das Kontrollkästchen zum Aktivieren der Zwei-Faktor-Authentifizierung auswählen.

**ANMERKUNG:** Administratoren müssen den zweiten Authentifizierungsfaktor über Einmal-Passcodes für die Anmeldung am Management Portal überprüfen.

- 4 Sie erhalten einen Einmal-Passcode an Ihre E-Mail-Adresse. Geben Sie den Einmal-Passcode zum Überprüfen ein.

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

## Generieren von Berichten

Gehen Sie folgendermaßen vor, um Berichte zu generieren:

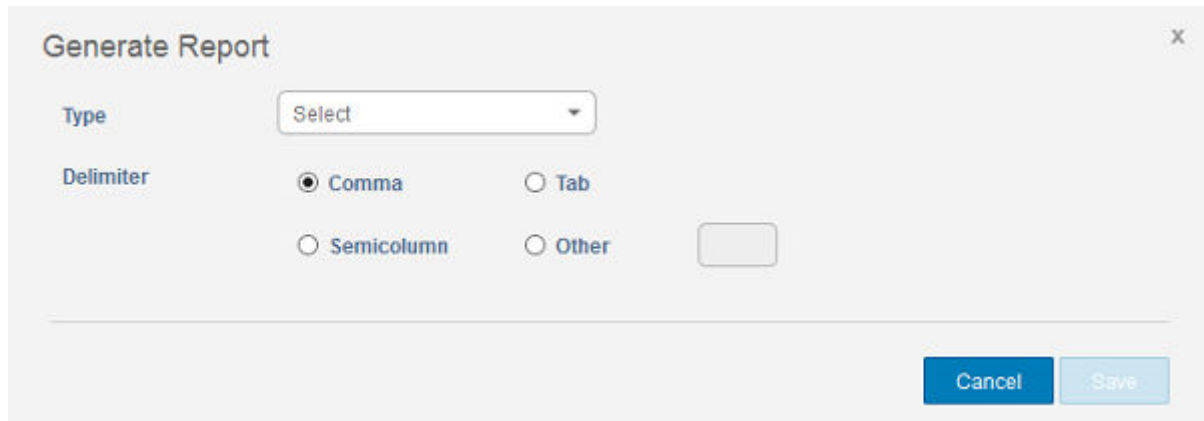


Abbildung 13. Bericht generieren

- 1 Gehen Sie zu **Portaladministrator > Berichte**.
- 2 Klicken Sie auf die Option **Bericht generieren**.  
Das Fenster **Bericht generieren** wird angezeigt.
- 3 Wählen Sie aus der Dropdownliste **Typ** den Berichtstyp aus.

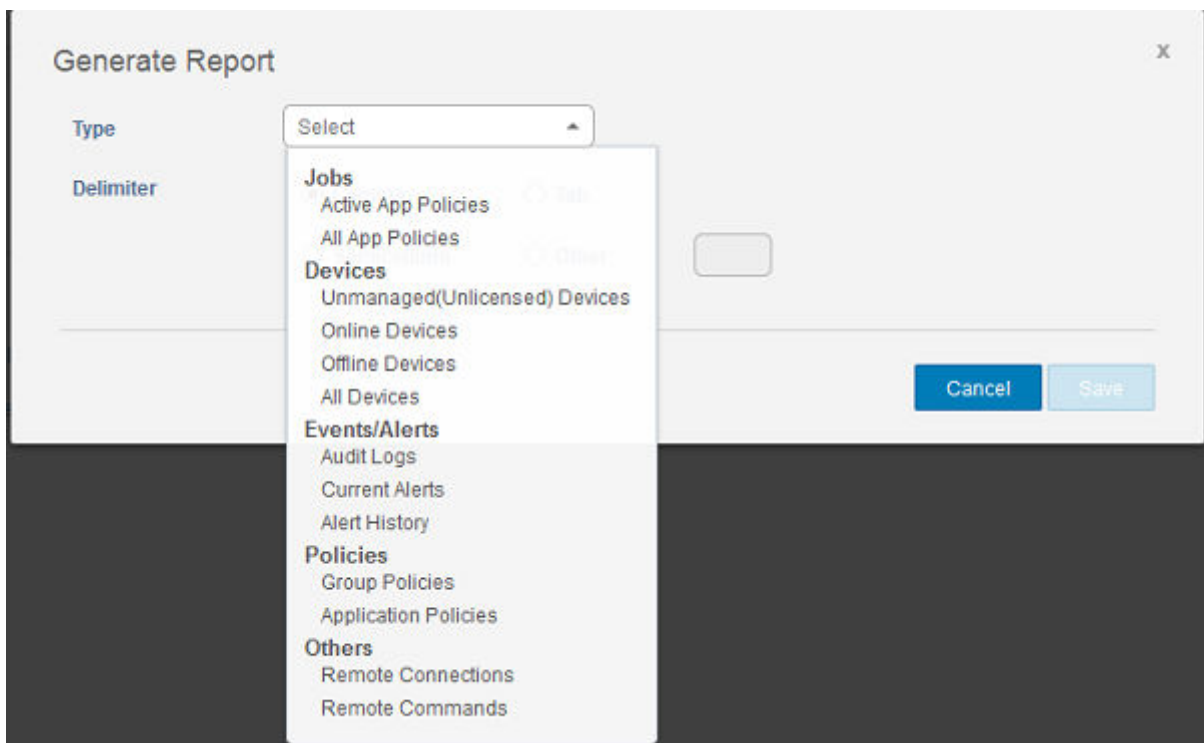


Abbildung 14. Berichtstypen

- 4 Wählen Sie aus der Dropdownliste **Gruppe** die Gruppe aus.
- 5 Wählen Sie das Trennzeichen aus.
- 6 Klicken Sie auf **Speichern**.

## Aktivieren von Multi-Tenant Konten

Dieser Abschnitt ermöglicht das Erstellen einer weiteren Organisation. Sie können die Organisationen unabhängig voneinander verwalten. Jedes Konto muss einen eigenen Lizenzschlüssel haben und kann einen eigenen Satz von Administratorkonten, Richtlinien,

Betriebssystemabbildern, Anwendungen, Regeln, Warnmeldungen usw. einrichten. Der übergeordnete Operator erstellt diese Organisationen.

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

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

## Aktivieren von benutzerdefiniertem Branding

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:

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

 **ANMERKUNG:** Sie dürfen die Bilder nur als **.ico-Dateien** speichern.

- 8 Klicken Sie auf **Einstellungen speichern**.

## Verwalten des Lizenzabonnements

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

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

- **Registrierte Thin Client-Geräte**
- **Serverinformationen**
- **Lizenz importieren (Private Cloud)**
- **Lizenz für private Cloud exportieren (Öffentliche Cloud)**

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

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

- 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 privaten Cloud-Konsole der Wyse Management Suite

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

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

# Thin Client-Lizenzzuweisung

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

- 1 Melden Sie sich bei der öffentlichen Cloud-Konsole der Wyse Management Suite an.
- 2 Gehen Sie zu **Portalverwaltung > Konten > Abonnement**.
- 3 Geben Sie die Anzahl der Thin Client Plätze an.

**ANMERKUNG:** Die Thin Client Arbeitsplätze sollten in der öffentlichen Cloud verwaltet werden können. Die eingegebene Anzahl der Thin Client Arbeitsplätze darf nicht höher sein als die in der Option Verwaltbar angezeigte Anzahl.

4 Klicken Sie auf **Exportieren**.

**ANMERKUNG:** Die Anzahl der öffentlichen Cloud Lizenzen wird basierend auf der Anzahl der in die private Cloud exportierten Thin Client Arbeitsplätze angepasst.

5 Kopieren Sie den generierten Lizenzschlüssel.

6 Melden Sie sich bei der privaten Cloud-Konsole der Wyse Management Suite an.

7 Gehen Sie zu **Portalverwaltung > Konten > Abonnement**.

8 Importieren Sie den exportierten Lizenzschlüssel in die private Cloud.

**ANMERKUNG:** Die Lizenz kann nicht importiert werden, wenn sie nicht über ausreichend Thin Client Arbeitsplätze verfügt, um die Anzahl von aktuell verwalteten Geräten in der privaten Cloud zu verwalten. In diesem Fall wiederholen Sie die Schritte 3-8 zur Zuweisung der Thin Client Arbeitsplätze.

## Lizenzbestellungen

In der Public 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 Public Cloud-Portal als Mandanten-Administrator anmelden.

## Verwalten des System-Setup

In diesem Abschnitt finden Sie Informationen zu den folgenden Themen:

- 1 Melden Sie sich am Wyse Management Suite-Portal an und klicken Sie auf die Registerkarte **Portaladministrator**.
- 2 Klicken Sie auf **Setup** unter **Systeme**.
- 3 Wählen Sie das Kontrollkästchen zur Durchführung der Validierung von Serverzertifikaten für jegliche Kommunikation zwischen Geräten und Servern.
- 4 Geben Sie die folgenden Details im Bereich **SMTP für E-Mail-Warnungen aktualisieren** ein:

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

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


**ANMERKUNG:** Zum Aktivieren der CA-Validierung für das Remote-Repository gehen Sie zu **Portalverwaltung > Dateirepository > Repository auswählen > Bearbeiten > CA-Validierung aktivieren > Einstellungen speichern**.

**ANMERKUNG:**

- 1 Wenn die CA-Validierung des Wyse Management Suite Servers aktiviert ist, sollte das Zertifikat im Client vorhanden sein. Alle Vorgänge, wie z. B., Apps und Daten, Bildabruf, sind erfolgreich. Wenn das Zertifikat nicht im Client vorhanden ist, bietet der Wyse Management Suite Server eine generische Audit-Ereignisbenachrichtigung **Validierung der Zertifizierungsstelle fehlgeschlagen** auf der Seite **Ereignisse**. Alle Vorgänge, wie z. B., Apps und Daten, Bildabruf, waren nicht erfolgreich.
- 2 Wenn die CA-Validierung von Wyse Management Suite Server nicht aktiviert ist, findet die Kommunikation zwischen Server und Client in einem sicheren Kanal ohne Validierung der Zertifikatssignatur statt.

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

- **Schlüssel/Zertifikat:** Dateipaar für HTTPS-Schlüssel/-Zertifikat hochladen (nur PEM-Format wird unterstützt).

- **PKCS-12:** HTTPS-PKCS-12 hochladen (.pfx, .p12). Ein Apache-Zwischenzertifikat ist für IIS pfx erforderlich.
- 6 Um die Details für externen MQTT zu aktualisieren, klicken Sie auf die Option **Externen MQTT ändern** und konfigurieren Sie die Informationen.
  - 7 Um die externe URL der Wyse Management Suite zu aktualisieren, klicken Sie auf die Option **Externe WMS-URL ändern** und konfigurieren Sie die Informationen.  
 **ANMERKUNG:** Um zu den vorherigen Konfigurationen zurückzukehren, klicken Sie auf die Option **Letzte URLs zurücksetzen und dann auf Speichern**.
  - 8 Klicken Sie auf **Speichern**.

# Konfigurieren von Wyse Easy Setup mithilfe der Wyse Management Suite

Sie können die Wyse Easy Setup Software mithilfe der Wyse Management Suite installieren und konfigurieren.

Themen:

- [Installieren von Wyse Easy Setup](#)
- [Implementieren einer Wyse Easy Setup-Konfiguration](#)

## Installieren von Wyse Easy Setup

### Vorbedingungen

- Mindestens 100 MB freier Speicherplatz
- RAM-Datenträgergröße von mindestens 100 MB
- Microsoft Visual C++ Redistributable 2012 32-Bit (x86) oder 64-Bit (x64)
- Microsoft .Net Framework 4.5 und aktueller
- Wyse Device Agent Version 14.0.0.237 und höher

### Schritte

- 1 Melden Sie sich bei der Wyse Management Suite-Konsole an.
- 2 Klicken Sie auf **Apps & Daten**.
- 3 Klicken Sie in den **App-Richtlinien** auf **Thin Client**.
- 4 Klicken Sie auf **Richtlinie hinzufügen**.  
Das Fenster **Standard-App-Richtlinie hinzufügen** wird angezeigt.
- 5 Geben Sie den Richtliniennamen ein.
- 6 Wählen Sie die Gruppe, eine Aufgabe, den Typ des Betriebssystems, eine Anwendung, den OS-Subtypfilter und den Plattformfilter aus der jeweiligen Dropdown-Liste aus.
- 7 Geben Sie /s in das Feld **Installationsparameter** ein.
- 8 Klicken Sie auf **Speichern**.
- 9 Gehen Sie zur Seite **Jobs** und legen Sie die Zeitplanung des Jobs für den Start der automatischen Installation von Wyse Easy Setup fest.

## Implementieren einer Wyse Easy Setup-Konfiguration

Stellen Sie vor der Bereitstellung einer Konfiguration sicher, dass der Thin Client bei [Wyse Management Suite](#) registriert ist.

- 1 Melden Sie sich bei der Wyse Management Suite-Konsole an.
- 2 Klicken Sie auf **Gruppen und Konfigurationen**.
- 3 Wählen Sie eine Gruppe aus und klicken Sie auf **Richtlinien bearbeiten**.
- 4 Klicken Sie auf **WES**.
- 5 Klicken Sie auf **Wyse Easy Setup**.
- 6 Klicken Sie nach der Konfiguration der Richtlinieneinstellungen auf **Speichern und veröffentlichen**.

**ANMERKUNG:**

- Wenn der Thin Client in der Wyse Management Suite registriert ist, werden alle lokalen Konfigurationen, die mithilfe der Wyse Easy Setup-Administrator-Shell konfiguriert wurden, verworfen. Die Remote-Konfigurationen, die mithilfe von Wyse Management Suite bereitgestellt wurden, werden angewendet.
- Wenn die Registrierung eines Thin Client in Wyse Management Suite aufgehoben wird, werden die Konfigurationen, die mithilfe von Wyse Management Suite bereitgestellt wurden, verworfen. Die lokalen Konfigurationen, die mithilfe der Wyse Easy Setup-Administrator-Shell bereitgestellt wurden, werden angewendet.

# Konfigurieren von Wyse Converter for PCs mithilfe der Wyse Management Suite

Sie können den Wyse Converter for PCs mithilfe der Wyse Management Suite installieren und konfigurieren.

Themen:

- Registrieren des Wyse Software Thin Clients bei der Wyse Management Suite
- Registrieren des Wyse Software Thin Client bei der Wyse Management Suite über den Wyse Geräte-Agenten
- Registrieren von Geräten durch die Verwendung von DHCP-Option-Tags bei der Wyse Management Suite
- Registrieren von Wyse Software Thin Clients mithilfe des DNS-SRV-Eintrags bei Wyse Management Suite
- Konfigurieren des Wyse Software Thin Clients mithilfe der Wyse Management Suite

## Registrieren des Wyse Software Thin Clients bei der Wyse Management Suite

Sie können den Wyse Software Thin Client mit einer der folgenden Methoden bei der Wyse Management Suite 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.

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

### Vorbedingungen

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


### Schritte

- 1 Öffnen Sie die Anwendung **Wyse Geräte-Agent**.  
Das Fenster **Wyse Geräte-Agent** wird angezeigt.
- 2 Geben Sie die Geräteregistrierungsinformationen ein.
- 3 Wählen Sie in der Dropdown-Liste **Verwaltungsserver** die Option **Wyse Management Suite** aus.
- 4 Geben Sie die Serveradresse und die Portnummer in die jeweiligen Felder ein.
- 5 Geben Sie das Gruppentoken ein. Für einen einzelnen Mandanten ist die Eingabe eines Gruppentokens ein optionaler Schritt.
- 6 Klicken Sie auf **Registrieren**.  
Nachdem die Registrierung abgeschlossen ist, wird die Meldung **An Wyse Management Suite registriert** angezeigt.

# Registrieren von Geräten durch die Verwendung von DHCP-Option-Tags bei der Wyse Management Suite

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

**Tabelle 294. Registrieren von Geräten mithilfe von DHCP-Options-Tags**

Options-Tag	Beschreibung
<p><b>Name</b> – WMS</p> <p><b>Datentyp</b> – Zeichenfolge</p> <p><b>Code</b> – 165</p> <p><b>Beschreibung</b> – WMS-Server-FQDN</p>	<p>Dieses Tag verweist auf die Wyse Management Suite-Server-URL. Beispiel: <b>wmsserver.acme.com:443</b>, wobei <b>wmsserver.acme.com</b> der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist.</p> <p> <b>ANMERKUNG: Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird.</b></p>
<p><b>Name</b> – MQTT</p> <p><b>Datentyp</b> – Zeichenfolge</p> <p><b>Code</b> – 166</p> <p><b>Beschreibung</b> – MQTT-Server</p>	<p>Dieses Tag leitet das Gerät zum Wyse Management Suite-Pushbenachrichtigungsserver (PNS) weiter. Bei einer Installation in einer privaten Cloud wird das Gerät an den MQTT-Dienst auf dem Wyse Management Suite-Server weitergeleitet. Beispiel: <b>wmsservername.domain.com:1883</b>.</p> <p>Zum Registrieren Ihrer Geräte in der öffentlichen Cloud der Wyse Management Suite sollte das Gerät auf die PNS-(MQTT-)Server in der öffentlichen Cloud verweisen. Beispiel:</p> <p>US1 –<a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>EU1 –<a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p>
<p><b>Name</b> – CA-Validation</p> <p><b>Datentyp</b> – Zeichenfolge</p> <p><b>Code</b> – 167</p> <p><b>Beschreibung</b> – Zertifizierungsstellenprüfung</p>	<p>Sie können die Option „CA-Validierung“ aktivieren oder deaktivieren, wenn Sie Ihre Geräte mit der Wyse Management Suite in der privaten Cloud registrieren. Standardmäßig ist die CA-Validierung in der öffentlichen Cloud aktiviert. Sie können die CA-Validierung auch in der öffentlichen Cloud deaktivieren.</p> <p>Geben Sie <b>Wahr</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server von einer bekannten Zertifizierungsstelle importiert haben.</p> <p>Geben Sie <b>Falsch</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server nicht von einer bekannten Zertifizierungsstelle importiert haben.</p>

Weitere Informationen zu den Sicherheitsumgebungen für Kunden finden Sie unter [Wyse-Geräte-Agent](#).

## Registrieren von Wyse Software Thin Clients mithilfe des DNS-SRV-Eintrags bei Wyse Management Suite

Der Wyse Geräte-Agent 13.0 und höhere Versionen unterstützen DNS-basierte Geräteregistrierung. Sie können Geräte mit dem Wyse Management Suite-Server registrieren, falls für die DNS-SRV-Eintragsfelder gültige Werte eingegeben wurden. Die folgende Tabelle listet die gültigen Werte für die DNS-SRV-Einträge auf:

Tabelle 295. Konfigurieren eines Geräts mithilfe eines DNS-SRV-Eintrags

URL/Tag	Beschreibung
<p><b>Eintragsname</b> – _WMS_MGMT</p> <p><b>Eintrags-FQDN</b> – _WMS_MGMT._tcp.&lt;Domänenname&gt;</p> <p><b>Eintragstyp</b> – SRV</p>	<p>Dieser Eintrag verweist auf die Wyse Management Suite Server-URL. Beispiel: <b>wmsserver.acme.com:443</b>, wobei <b>wmsserver.acme.com</b> der vollqualifizierte Domänenname des Servers ist, auf dem die Wyse Management Suite installiert ist.</p> <p><b>ANMERKUNG:</b> Verwenden Sie in der Server-URL nicht „https://“, da der Thin Client sonst nicht bei der Wyse Management Suite registriert wird.</p>
<p><b>Eintragsname</b> – _WMS_MQTT</p> <p><b>Eintrags-FQDN</b> – _WMS_MQTT._tcp.&lt;Domänenname&gt;</p> <p><b>Eintragstyp</b> – SRV</p>	<p>Dieser Eintrag leitet das Gerät zum Wyse Management Suite-Pushbenachrichtigungsserver (PNS) weiter. Bei einer Installation in einer privaten Cloud wird das Gerät an den MQTT-Dienst auf dem Wyse Management Suite-Server weitergeleitet. Beispiel: <b>wmsservername.domain.com:1883</b>.</p> <p><b>ANMERKUNG:</b> MQTT ist bei der neuesten Version der Wyse Management Suite optional.</p> <p>Zum Registrieren Ihrer Geräte in der öffentlichen Cloud der Wyse Management Suite sollte das Gerät auf die PNS-(MQTT-)Server in der öffentlichen Cloud verweisen. Beispiel:</p> <p>US1 –<a href="https://us1-pns.wysemanagementsuite.com">us1-pns.wysemanagementsuite.com</a></p> <p>EU1 –<a href="https://eu1-pns.wysemanagementsuite.com">eu1-pns.wysemanagementsuite.com</a></p>
<p><b>Eintragsname</b> – _WMS_CAVALIDATION</p> <p><b>Eintrags-FQDN</b> – _WMS_CAVALIDATION._tcp.&lt;Domänenname&gt;</p> <p><b>Eintragstyp</b> – TEXT</p>	<p>Sie können die Option „CA-Validierung“ aktivieren oder deaktivieren, wenn Sie Ihre Geräte mit der Wyse Management Suite in der privaten Cloud registrieren. Standardmäßig ist die CA-Validierung in der öffentlichen Cloud aktiviert. Sie können die CA-Validierung auch in der öffentlichen Cloud deaktivieren.</p> <p>Geben Sie <b>Wahr</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server von einer bekannten Zertifizierungsstelle importiert haben.</p> <p>Geben Sie <b>Falsch</b> ein, wenn Sie die SSL-Zertifikate für die https-Kommunikation zwischen dem Client und dem Wyse Management Suite-Server nicht von einer bekannten Zertifizierungsstelle importiert haben.</p> <p><b>ANMERKUNG:</b> CA Validation ist bei der neuesten Version der Wyse Management Suite optional.</p>

Weitere Informationen zu den Sicherheitsumgebungen für Kunden finden Sie unter [Wyse-Geräte-Agent](#).

## Konfigurieren des Wyse Software Thin Clients mithilfe der Wyse Management Suite

Sie können Ihren Wyse Software Thin Client mithilfe der Wyse Management Suite 1.1 oder einer höheren Version konfigurieren, wenn das Gerät mithilfe von Wyse Converter for PCs zu einem Thin Client konvertiert wird. Bevor Sie den Wyse Software Thin Client konfigurieren müssen Sie ihn bei der Wyse Management Suite registrieren.

- 1 Melden Sie sich bei der Wyse Management Suite-Konsole an.
- 2 Klicken Sie im Dashboard auf **Gruppen und Konfigurationen**.
- 3 Wählen Sie eine Gruppe aus und klicken Sie auf **Richtlinien bearbeiten**.
- 4 Klicken Sie auf **Wyse Software Thin Client**.

Die Seite **Wyse Software Thin Client** wird angezeigt.

- 5 Klicken Sie nach der Konfiguration der Optionen auf **Speichern und veröffentlichen**.

# Teradici-Geräteverwaltung

Der Abschnitt zur Teradici-Geräteverwaltung enthält Informationen zur Verwaltung und zur Ermittlung von Teradici-Geräten. Die Teradici-Verwaltungskonsole verwendet SDKs zur Unterstützung der Verwaltung und Konfiguration von Tera-Geräten. Dies gilt nur für die private Cloud der Wyse Management Suite mit einer Pro-Lizenz. Weitere Informationen zu den Konfigurationsrichtlinien von Teradici finden Sie unter [Bearbeiten von Teradici-Richtlinieneinstellungen](#).

Themen:

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

## Ermittlung von Teradici-Geräten

Vorbedingungen

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

## Sicherheitsstufe

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

Endgeräte, die für mittlere oder hohe Sicherheit konfiguriert sind, müssen ein 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 296. Zertifikatsanforderungen für Endpunkte**

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

## Manuelle Ermittlung über den Client

- 1 Gehen Sie zu **https://<clientIP>**.
- 2 Bestätigen Sie die Zertifikat-Warnmeldung.
- 3 Geben Sie das Administratorkennwort ein (Standardkennwort lautet „Administrator“) und melden Sie sich an.
- 4 Gehen Sie zu **Hochladen > Zertifikat**. Wählen Sie die Datei `cert.pem` aus dem Standardpfad aus und klicken Sie auf **Hochladen**.
- 5 Gehen Sie zu **Konfiguration > Verwaltung**. Klicken Sie auf die Schaltfläche **Verwaltungsstatus löschen**, um das Gerät beim neuen Verwaltungsserver zu registrieren.
- 6 Stellen Sie den **Manager-Erkennungsmodus** auf manuell ein.
- 7 Geben Sie die **Endpoint Bootstrap Manager-URL** in folgendem Format ein: **wss://<IP-Adresse des WMS-Servers>**

**ANMERKUNG:** Wenn EMSDK mit einem benutzerdefinierten Port installiert ist, geben Sie die Endpoint Bootstrap Manager-URL in folgendem Format ein: **wss://<IP-Adresse:benutzerdefinierter Port>**.

- 8 Klicken Sie auf **Anwenden** und dann auf **Weiter**.
- 9 Für den **Verwaltungsstatus** wird „Verbunden mit dem Endpunktserver“ angezeigt.

## Hinzufügen der PCoIP-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.
- 3 Klicken Sie mit der rechten Maustaste auf die Option **IPv4** und wählen Sie dann **Anbieter-Klassen definieren**.
- 4 Klicken Sie auf **Hinzufügen**, um eine neue DHCP-Anbieterklasse hinzuzufügen.
- 5 Geben Sie den **PCoIP-Endpunkt** in das Feld **Anzeigename** ein.
- 6 Geben Sie als Hersteller-ID den **PCoIP-Endpunkt** in der Spalte **ASCII** ein.
- 7 Klicken Sie auf **OK**, um die Einstellungen zu speichern.

# Konfigurieren von DHCP-Optionen

- 1 Klicken Sie mit der rechten Maustaste auf die Option **IPv4** und wählen Sie dann **Vordefinierte Optionen festlegen** aus.
- 2 Wählen Sie den **PCoIP-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.
- 8 Aktivieren Sie das Kontrollkästchen **010 EBM URI** und geben Sie dann eine gültige Verwaltungskonsolen-URI im Feld **Zeichenkette** ein. Klicken Sie auf **Anwenden**. Diese URI erfordert ein gesichertes WebSocket-Präfix, z. B., **wss://<MC IP address>:[port number]. „5172“** ist der Überwachungsport des MC. Die Eingabe dieser Portnummer ist ein optionaler Schritt.
- 9 Klicken Sie auf **OK**, um die Einstellungen zu speichern.
- 10 Wählen Sie **PCoIP-Endpunkt** als Klasse **Option** aus und klicken Sie auf **Hinzufügen**.
- 11 Geben Sie im Dialogfeld **Optionstyp** den Namen als **Fingerabdruck EBM X.509 SHA-256**, den Datentyp **Zeichenkette**, den Code **11** und die Beschreibung **Fingerabdruck EBM X.509 SHA-256** ein und klicken Sie dann auf **OK**.
- 12 Erweitern Sie den DHCP-Bereich, auf den Sie die Optionen anwenden möchten.
- 13 Klicken Sie mit der rechten Maustaste auf **Bereichsoptionen** und wählen Sie anschließend **Optionen konfigurieren** aus.
- 14 Klicken Sie auf die Registerkarte **Erweitert** und wählen Sie anschließend die Herstellerklasse **PCoIP-Endpunkt** aus.
- 15 Aktivieren Sie das Kontrollkästchen **Fingerabdruck 011 EBM X.509 SHA-256** und fügen Sie den SHA-256-Fingerabdruck ein.
- 16 Klicken Sie auf **OK**, um die Einstellungen zu speichern.
- 17 Gehen Sie zum Webbrowser des Clients.
- 18 Gehen Sie zu **Konfiguration > Verwaltung** und legen Sie den **Manager-Erkennungsmodus** auf **Automatisch** fest.
- 19 Der Client ist mit dem Server verbunden, der auf dem DHCP-Server angegeben ist.

# Erstellen des DNS-SRV-Eintrags

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

 **ANMERKUNG:** Die FQDN des MC muss eingegeben werden, da die DNS-Spezifikation keine IP-Adressen in den SRV-Einträgen zulässt.

- 6 Klicken Sie auf **OK**.

## Hinzufügen eines DNS-TXT-Eintrags

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

## Erstellen eines SHA-256-Fingerabdrucks

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

## CIFS-Anwendungsszenarien

Die folgenden Anwendungsfälle werden in der Wyse Management Suite unterstützt:

- Wenn Sie **Wyse Management Suite** als **Setup-Typ** während der Installation der privaten Cloud der Wyse Management Suite auswählen.
  - Die Seite „CIFS-Konfiguration“ wird angezeigt. Diese Seite ist erforderlich zum Konfigurieren des freigegebenen Ordners.  
**ANMERKUNG:** Die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** ist standardmäßig deaktiviert.
- Wenn Sie **Teradici EMSDK** als **Setup-Typ** während der Installation der privaten Cloud der Wyse Management Suite auswählen.
  - Als CIFS-Anmeldeinformationen können Sie ein vorhandenes Konto verwenden oder ein neues erstellen.
- Wenn Sie **Wyse Management Suite** und **Teradici EMSDK** als **Setup-Typ** während der Installation der privaten Cloud der Wyse Management Suite auswählen.
  - Die Seite „CIFS-Konfiguration“ wird angezeigt. Diese Seite ist erforderlich zum Konfigurieren des freigegebenen Ordners.  
**ANMERKUNG:** Die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** ist standardmäßig deaktiviert.
  - Als CIFS-Anmeldeinformationen können Sie ein vorhandenes Konto verwenden oder ein neues erstellen.
- Wenn Sie nur EMSDK auf einem System installieren, auf dem bereits der EMSDK-Dienst installiert ist.
  - Wenn Teradici EMSDK ausgewählt ist, wird eine Warnmeldung angezeigt, wenn Sie auf **Weiter** auf der Seite **Setup-Typ** klicken. Die Meldung lautet: **Das Installationsprogramm hat erkannt, dass Teradici EMSDK bereits installiert ist. EMSDK wird bei Bedarf aktualisiert.** Es ist keine Portnummer erforderlich.
    - Wenn die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** ausgewählt ist (standardmäßig)
      - a Halten Sie den Dienst an.
      - b Aktualisieren Sie den EMSDK-Dienst.
      - c Starten Sie den Dienst neu. Er wird unter demselben vorkonfigurierten Benutzer ausgeführt.

- Wenn die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** mit der Option **Verwenden eines vorhandenen Benutzers** ausgewählt ist.
  - a Halten Sie den Dienst an.
  - b Aktualisieren Sie den EMSDK-Dienst.
  - c Aktualisieren Sie den Benutzer für die Anmeldung beim Dienst auf den ausgewählten Benutzer.
  - d Starten Sie den Dienst neu. Er wird unter demselben vorkonfigurierten Benutzer ausgeführt.
- Wenn die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** mit der Option **Einen neuen Benutzer erstellen** ausgewählt ist.
  - a Halten Sie den Dienst an.
  - b Aktualisieren Sie den EMSDK-Dienst.
  - c Aktualisieren Sie den Benutzer für die Anmeldung beim Dienst auf den neu erstellten Benutzer.
  - d Starten Sie den Dienst neu. Er wird unter demselben vorkonfigurierten Benutzer ausgeführt.
- Wenn Sie **Wyse Management Suite** und **Teradici EMSDK** auf einem System installieren, auf dem bereits der EMSDK-Dienst installiert ist.
  - Die Vorgehensweise entspricht **Wenn Sie nur EMSDK auf einem System installieren, auf dem bereits der EMSDK-Dienst installiert ist.** mit Ausnahme dessen, dass die Option **CIFS-Benutzeranmeldeinformationen konfigurieren** standardmäßig ausgewählt und ausgegraut ist. Sie müssen CIFS-Anmeldeinformationen eingeben.

## Wyse-Geräte-Agent

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

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

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

Der Ordner **Agent Configuration** ist an folgendem Speicherort verfügbar:

- Windows Embedded Standard-Geräte: `%SYSTEMDRIVE%\Wyse\WCM\ConfigMgmt\Certificates`
- ThinLinux-Geräte: `/etc/addons.d/WDA/certs`
- ThinOS-Geräte: `wnos/cacerts/`



**ANMERKUNG:** Sie müssen das Zertifikat über ein USB-Laufwerk oder FTP-Pfade auf einen Thin Client mit ThinOS-Betriebssystem importieren.


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

# Beheben von Fehlern in der Wyse Management Suite

Tabelle 297. Troubleshooting

Problem	Problemlösung
E-Mail-Benachrichtigungen funktionieren nicht.	Konfigurieren Sie den SMTP-Server vom Wyse Management Suite Server-Portal-Admin.
Wake-On-LAN funktioniert nicht.	Aktivieren Sie das lokale oder Remote-Datei-Repository.
Eine Warnmeldung über einen unbekanntes Dateityp wird angezeigt, wenn Sie auf das Startsymbol der Wyse Management Suite doppelklicken.	Überprüfen Sie die Sicherheitseinstellungen oder UAC des Servers. Stellen Sie sicher, dass Windows mit allen Patches aktualisiert wird.
Thin Client-Protokolldatei kann nicht abgerufen werden, wenn das ThinLinux Gerät nicht mit NTP-Server synchronisiert ist.	Konfigurieren Sie das Gerät mit einem angemessenen NTP-Server.
Warnmeldung <b>Fehler bei der Synchronisierung der TC Dateien</b> wird angezeigt, wenn Sie versuchen, das Datei-Repository zu synchronisieren.	Stellen Sie sicher, dass jeder die volle Berechtigung für das lokale Repository hat und keine Benutzerzugriff-Meldung angezeigt wird, wenn Sie das Image oder Anwendungen auf das lokale Repository kopieren.
Datei-Download wie Wallpaper, Zertifikate schlagen fehl für ThinOS, wenn der Server nicht mehr synchron ist.	Konfigurieren Sie das Gerät mit dem richtigen NTP-Server.
ThinOS DHCP-Erkennung schlägt fehl, wenn DNS-SRV-Tags mit leeren Werten verfügbar sind.	Entfernen Sie die leeren DNS-Tags.
<b>Auf neue Geräte anwenden</b> funktioniert nicht für ThinOS App-Richtlinien während der Registrierung.	Erstellen Sie einen Job, um die App Richtlinie zu übermitteln.
Nach der Änderung des Hostnamens des Repository-Servers wird die Repository-Benutzeroberfläche nicht über die Verknüpfung auf dem Desktop geöffnet. Nach der Änderung des Hostnamens des Repository-Servers ändert sich das Zertifikat und Sie erhalten eine Zertifikatsfehlermeldung beim Öffnen der Repository-Benutzeroberfläche und ein selbstsigniertes Zertifikat für die CA Validierung schlägt auch fehl.	Sie müssen den aktualisierten Hostnamen in der URL angeben.
Wenn auf Windows Embedded Standard Geräten die benutzerdefinierten Werte nicht eingerichtet sind, werden Gruppen nicht erstellt, wenn Sie benutzerdefinierte Werte als Gruppentyp auswählen. In der Gruppenstruktur wird eine Ebene ausgelassen.	Benutzerdefinierte Felder müssen Werte enthalten, bevor Gruppen für Windows Embedded Standard Geräte erstellt werden.
Synchronisierungszeitpunkt-Befehl schlägt auf Windows Embedded Standard Geräten fehl.	Keine Problemlösung verfügbar.

Problem	Problemlösung
Im Rahmen der RSP-Übermittlung, CU - Confirm User-Befehl wird immer der Fehler <b>Kein Benutzer</b> angemeldet angezeigt, selbst wenn ein gültiger Benutzer beim Thin Client angemeldet ist.	Keine Problemlösung verfügbar.
Die 404-Fehler wird angezeigt, wenn der Server 2 Tage lang inaktiv gelassen wird.	Der Server wird aufgrund von Windows neu gestartet. Starten Sie alle zu Wyse Management Suite gehörigen Dienste.
Der Wyse Management Suite Server reagiert nicht, wenn das Speicherplatz weniger als 300 MB beträgt.	Erhöhen Sie den Speicherplatz und starten Sie die zu Wyse Management Suite gehörigen Dienste neu.
Wenn der Agent sich mit http anmeldet, sendet Wyse Management Suite die https-URL und alle neuen Agenten wechseln zu https.	12.x Agenten weisen dieses Verhalten nicht auf, da der Agent die Wechsel-Anmeldung nicht versteht.
Fehler <b>Keine unterstützten Subautorisierungstypen</b> wird angezeigt, wenn Sie versuchen, die-VNC-Sitzung nach dem Deaktivieren der Option <b>Erforderliches Kennwort für VNC-Benutzer</b> vom Wyse Management Suite Server zu starten.	Starten Sie das VNC mit der Option <b>Erforderliches Kennwort für VNC-Benutzer</b> Option.
Die Schaltflächen Richtlinie hinzufügen und Erweiterte Richtlinie hinzufügen sind nach dem Entfernen der Anwendungsordner funktionslos.	Löschen Sie den Repository-Ordner nicht.
Durch das manuelle Löschen von Bestandsdateien manuell vom physischen Pfad (c: \Repository\Data) wird die Datei nicht von der Wyse Management Suite Benutzeroberfläche gelöscht – der Fehler <b>Datei existiert nicht</b> wird angezeigt.	Löschen Sie die Datei nicht manuell aus dem Repository-Ordner.
ThinOS Anwendungen werden zweimal installiert, wenn die Anwendungen mit Firmware übermittelt werden.	Die root-Diskette wird formatiert, wenn Sie <b>Base.pkg</b> hoch- oder herunterstufen.
Mit dem Import-Tool können Sie RSP-Pakete importieren, auch wenn Sie eine Datei (part1Image.img, vmlinuz, MBR usw.) aus dem RSP-Paket im WDM-Repository löschen.	Gültige RDP Pakete müssen in Wyse Device Manager vorhanden sein.
Wyse Management Suite zeigt einen 404-Fehler an.	Überprüfen Sie, ob ein Java-Code durch das Antivirusprogramm gelöscht wird.
Windows Embedded Standard App-Download schlägt fehl.	App-Download-Authentifizierung ist erforderlich für Window Embedded Standard Agent.  Wenn der Anwendungs-Download mit <b>https</b> fehlschlägt, versuchen Sie es mit <b>http</b> . Stellen Sie sicher, dass die Firewall-Einstellungen <b>http</b> -Ports zulassen. Der vorgegebene Port ist „8080“.
Wenn das Gerät bei der Deregistrierung oder beim Entfernen der Richtlinie zur Domäne hinzugefügt wird, kehrt das Gerät zur Arbeitsgruppe von der Domäne zurück.	Legen Sie die Standardrichtlinie für Domäneneinstellungen fest und übermitteln Sie die Richtlinie.
RemoteFX USB-Umleitungsrichtlinie wird für USB-Massenspeichergeräte nicht angewendet.	Fügen Sie die folgenden Registrierungseinträge zum Gerät hinzu:  1 Melden Sie sich als Administrator beim Gerät an und deaktivieren Sie den Schreibfilter. 2 Gehen Sie zu Befehl ausführen und geben Sie Regedit ein. 3 Gehen Sie zu <b>HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces</b> 4 Fügen Sie den Registrierungsschlüssel als 100 hinzu und legen Sie den Wert für Massenspeichergerät wie folgt fest: <b>{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}</b> für CD-ROM : <b>{53F56308-B6BF-11D0-94F2-00A0C91EFB8B}</b>

Problem	Probleumlösung
	 <b>ANMERKUNG: Geschweifte Klammern sind obligatorisch.</b>
Die USB-Sperrungskonfiguration wird nicht angewandt, wenn Sie auf die Schaltfläche „Aktualisieren“ klicken.	Dieses Problem tritt nur bei Wyse Software Thin Clients auf. Melden Sie sich erneut an, um die Richtlinie anzuwenden.
Wenn Sie SD-Befehl im Rahmen von RSP übermitteln, wird der Windows Embedded Standard Client neu gestartet statt heruntergefahren.	In Wyse Device Manager sendet das Gerät eine V02-Meldung und wechselt in den abgemeldeten Zustand. Dieser Vorgang wird nicht unterstützt für Wyse Management Suite.
Die Anwendungsinstallation schlägt fehl, wenn eine Richtlinie von zwei verschiedenen Repository-Servern erstellt wird.	<p>Stellen Sie sicher, dass vom Gerät auf alle Repositories zugegriffen werden kann.</p> <p>Wyse Geräte-Agent versucht immer den Test-Download mit der vom ersten Repository-Server erstellten Anwendung. Wenn der Test-Download fehlschlägt, kann der Agent nicht fortzufahren und ein Fehlerbericht wird an den Server gesendet.</p>
Sie können keine RAW-Images mit RSP über Wyse Management Suite erstellen.	<p>Zur Durchführung einer ThinLinux RAW Image-Erstellung über Wyse Management Suite gehen Sie wie folgt vor:</p> <ol style="list-style-type: none"> <li>1 Erstellen Sie einen FTP-Speicherort.</li> <li>2 Kopieren Sie das RAW-Image an den FTP-Speicherort.</li> <li>3 Kopieren Sie die RAW-Image-Datei erneut vom Wyse Management Suite Repository.</li> <li>4 Erstellen Sie eine Standard-App-Richtlinie mit RAW Image durch die Angabe von FTP-Speicherort, Benutzername und Kennwort als Installationsparameter.</li> <li>5 Planen Sie einen Richtlinien-Job.</li> </ol>
Der Wyse Management Suite Server funktioniert nicht, nachdem Sie ihn mit der Remote-Datenbank-Option auf demselben Server, auf dem MongoDB installiert ist, installiert haben.	Löschen Sie den Stratus-Datenbankeintrag, falls vorhanden.
Die Wyse Management Suite Server-Benutzeroberfläche wird nach der Installation des Servers nicht geladen und es erfolgt keine Anmeldung beim Server.	Der Hostname des Servers enthält möglicherweise Unterstriche (_). Ändern Sie den Hostnamen, sodass er keine Unterstriche enthält.
Die Registrierung des Wyse Geräte-Agenten schlägt nach der Installation der Servers mit benutzerdefinierten Anschlüssen fehl.	Geben Sie das Präfix http/https im Serverfeld vom Agenten an.
Die statische IP wird auf dem Thin Client nach einer Image-Übermittlung (Sysprep) nicht beibehalten.	Weisen Sie dem Thin Client eine statische IP zu und starten Sie das Gerät neu.
Auf der Wyse Geräte-Agent Benutzeroberfläche wird <b>Dienst wird nicht ausgeführt</b> oder ein leerer Bildschirm angezeigt, wenn ein up- oder Downgrade für den ThinLinux Wyse Geräte-Agenten durchgeführt wird.	Warten Sie einige Sekunden, bis alle Dienste ausgeführt werden.
Importieren von Benutzern mit LDAPS-Konfiguration nicht möglich.	<p>Gehen Sie bezüglich Wyse Management Suite wie folgt vor:</p> <ol style="list-style-type: none"> <li>1 Importieren Sie das AD-Domänenserver-Stammzertifikat durch Ausführen des folgenden Befehls manuell in den Java-Schlüsselspeicher: <code>&lt;C:\ProgramFiles\DELL\WMS\jdk1.8.0_152\jre\bin&gt;keytool.exe -importcert -alias "WIN-O358EA52H8H" -keystore "&lt;C:\ProgramFiles\DELL\WMS\jdk1.8.0_152\jre\lib\security\cacerts&gt;" -storepass changeit -file "Root Certificate Path"</code></li> <li>2 Starten Sie den Tomcat-Dienst neu.</li> </ol>

Problem	Problemlösung
	<p>Im Wyse Management Suite-Repository führen Sie Folgendes aus:</p> <ol style="list-style-type: none"> <li>1 Verwenden Sie die Option auf der Benutzeroberfläche zum Importieren des Zertifikats in den Java-Schlüsselspeicher.</li> <li>2 Starten Sie den Tomcat-Dienst neu.</li> </ol>
Die Option für mehrere Monitore ist für den Wyse Software Thin Client nicht vorhanden.	Die Funktion für mehrere Monitore wird auf Wyse Converter für PCs nicht unterstützt.
Wyse Management Suite Upgrade von 1.0 auf 1.1 funktioniert nicht mit externer Mongo- und integrierter Maria-Datenbank.	Führen Sie direkt ein Upgrade auf Wyse Management Suite 1.2 durch.
Image-Erstellung über HTTP funktioniert nicht.	<p>Stellen Sie sicher, dass HTTP manuell aktiviert wird. Ab Wyse Management Suite Version 1.2 aufwärts ist HTTP standardmäßig deaktiviert und der Administrator muss es über Tomcat manuell aktivieren.</p> <p><b>ANMERKUNG:</b>  Wenn der Anwendungs-Download mit <b>https</b> fehlschlägt, versuchen Sie es mit <b>http</b>. Stellen Sie sicher, dass die Firewall-Einstellungen <b>http</b>-Ports zulassen. Der vorgegebene Port ist „8080“.</p>
Mongo-, Maria- und Tomcat-Dienste werden nach dem Neustart des Wyse Management Suite Servers angehalten.	Der Windows Defender Dienst löscht die zu Wyse Management Suite gehörigen Dateien. Überprüfen Sie die Protokolle des Defender Dienstes auf gelöschte Dateien. Rufen Sie die gelöschte Dateien ab.
Die Installation des VC++ Pakets dauert ca. 20 Minuten.	<p>Stellen Sie sicher, dass der Windows Server mit den neuesten Service Packs und Updates aktualisiert ist.</p> <p>Stellen Sie sicher, dass das Windows Update nicht während der Installation von Wyse Management Suite ausgeführt wird.</p>
ThinLinux Agent-Aktualisierung von 0.2.24 auf 2.2.11 funktioniert nicht.	ThinLinux Geräte mit Agent-Version 0.2.24 müssen vor einem Upgrade auf 2.2.11 auf 1.2.23 aktualisiert werden, da der 0.2.24 Agent die <b>.tar</b> -Dateien nicht installiert.
Agent-Aktualisierung von 3.0.7 auf 2.3.13 schlägt mit Thinlinux Gerät auf dem 3040 Wyse Thin-Client fehl.	Aktualisieren Sie den Agenten auf Version 0.3.10 mit Paket <b>wda3040_3.0.10-01_amd64.deb</b> . Dieses Paket ist im Wyse Management Suite 1.2 Installationsprogramm enthalten. Führen Sie anschließend ein Upgrade auf den neueste WDA 2.3.13 durch.
Die Threadx-6.x-Teradici-Geräte können nach dem Zurücksetzen auf die Werkseinstellungen nicht in EMSDK registriert werden.	Verbinden Sie den Zero-Client mit dem NTP-Server vor dem Anschluss an das Endgerät, ähnlich wie bei Verwendung der DHCP-Option. Sie können auch ein Zertifikat mit einem gültigen Startdatum installieren. Das Datum muss vor dem Firmware-Datum liegen.
Wenn die Wyse Management Suite-UI mit eingebettetem Maria und Remote-Mongo installiert ist und der Datenbankserver als Localhost in Remote-Mongo bereitgestellt ist, dann wird der Fehler <b>HTTP 404 Not Found</b> angezeigt.	Verwenden Sie die lokale IP 127.0.0.1 oder die Server-IP.
Das Abbild, das vom USB-Tool abgerufen wird, ist nicht auf dem Wyse Management Suite-Server registriert.	Ändern Sie die Abbildversion zu einer <b>.rsp</b> -Datei und nehmen Sie die Registrierung in der Wyse Management Suite vor.

Problem	Probleumlösung
Der Teradici-Server wird nicht synchronisiert, wenn die IP-Adresse des Wyse Management Suite-Servers geändert wird (EMSDK auf demselben Server), auch nach dem Neustart des Servers.	Aktualisieren Sie die Teradici-Server-IP über <b>Portal &gt; Verwaltung &gt; Teradici &gt; Server bearbeiten</b> .
Beim Importieren der Gruppen und Geräte mithilfe von WDM-Standardgruppentypen aus dem Import-Tool wird der Betriebssystemtyp zweimal angezeigt.	Starten Sie den Importvorgang neu.
Wenn Sie die Einrichtungssseite nach dem Ändern der Wyse Management Suite-Server-IP-Adresse auswählen, wird die Meldung <b>Error:Error</b> angezeigt.	Starten Sie die Wyse Management Suite-Dienste nach dem Ändern der IP-Adresse.
Nach der Installation der Wyse Management Suite mit benutzerdefiniertem Port (bekannte Ports), kann die Weboberfläche nicht gestartet werden.	Dell empfiehlt die Verwendung von Port 1024 oder höher.
Bei der ThinLinux Version 2.0 wird der Fehler <b>Medienvvalidierung fehlgeschlagen</b> angezeigt, wenn versucht wird, ein Downgrade von der Testversion 2.0.25 auf die Versionen 2.0.22/2.0.14(5070/3040) vorzunehmen.	Installieren Sie die neueste Version von Merlin (höher als 3.7.7).
Nach dem Merlin-Upgrade werden keine Startdateien in den Ordner <b>/boot</b> kopiert	Deinstallieren und installieren Sie die neueste Version von Merlin.
Fehler beim Einloggen auf dem Wyse Management Suite-Server, wenn alle Konten gesperrt sind und die 2FA-Option aktiviert ist.	Legen Sie den Wert für „TwoStepVerificationEnabled“ auf „Falsch“ (0) über die Tabelle „stratus.tenant“ in der MariaDB fest.
Warnmeldung <b>SHA-256 nicht gefunden</b> wird auf Thin Clients mit dem Betriebssystem Windows Embedded Standard 7 angezeigt, wenn das Upgrade der Wyse Device Agent App-Richtlinien fehlschlägt.	Sie müssen KB3033929 installieren.
Nach dem Upgrade von ThinLinux 1.x auf ThinLinux 2.1 erscheint auf dem Thin Client eine Warnmeldung, wenn Sie auf die Schaltfläche <b>Einstellungen</b> klicken.	Schließen Sie das Fenster <b>Einstellungen</b> , bevor Sie den Pull-Vorgang für das Abbild durchführen. Sie können auch auf <b>Profil entsperren und neu starten</b> klicken, um die Schaltfläche <b>Einstellungen</b> wiederherzustellen.

# Installieren oder Aktualisieren von Wyse Geräte-Agent

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

- **Windows Embedded Standard-Geräte** – Der Wyse Geräte-Agent Version 14 kann von [Dell Support](#) heruntergeladen und auf Windows Embedded Standard-Geräten unter Verwendung einer der folgenden Methoden installiert oder aktualisiert werden:
  - [Aktualisieren von Wyse Geräte-Agent mit einer Wyse Management Suite-Anwendungsrichtlinie.](#)
  - [Manuelles Installieren von Wyse Geräte-Agent.](#)

**ANMERKUNG:** Der Wyse Geräte-Agent kann nur auf dem Betriebssystem Windows Embedded Standard 7 installiert werden, wenn KB3033929 verfügbar ist.

- **Linux- und ThinLinux-Geräte** – Der Wyse Gerät-Agent kann auf Linux- und ThinLinux-Geräten mithilfe der Wyse Management Suite installiert oder aktualisiert werden. Weitere Informationen finden Sie unter [Installieren oder Aktualisieren von Wyse Geräte-Agenten auf ThinLinux- und Linux-Clients.](#)

Themen:

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

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

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

- 1 Nachdem die Datei **WDA.exe** in das Repository kopiert wurde, gehen Sie in den Abschnitt **Anwendungen und Daten** und erstellen Sie eine normale Anwendungsrichtlinie mit diesem Paket.

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

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

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

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

# Manuelles Installieren von Wyse Geräte-Agent

So installieren Sie den Wyse Geräte-Agent manuell:

- 1 Kopieren Sie die Datei **WDA.exe** in den Thin Client.
- 2 Doppelklicken Sie auf die Datei **WDA.exe**.

**ANMERKUNG:**

- Verschiedene Wyse Geräte-Agent-Pakete sind für jede Variante von Windows Embedded Standard verfügbar.
- Es wird eine Warnmeldung angezeigt, wenn eine ältere Version von Wyse Geräte-Agent oder HAgent auf dem Gerät installiert ist.

- 3 Klicken Sie auf **Ja**.
- 4 Geben Sie in das Feld **Gruppentoken** ein Gruppentoken ein. Dieses Feld ist optional. Wenn Sie diesen Schritt überspringen, klicken Sie auf **Weiter**. Sie können die Einzelheiten des Gruppentokens im weiteren Verlauf über die Wyse Geräte-Agent-Benutzeroberfläche eingeben.
- 5 Wählen Sie aus der Dropdownliste **Region** die Region des öffentlichen Cloud-Servers der Wyse Management Suite.  
Nach der erfolgreichen Installation der Wyse Management Suite registriert der öffentliche Cloud-Server automatisch das Gerät in der Wyse Management Suite-Konsole.

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

So führen Sie ein Upgrade des Wyse Geräte-Agents und der Plattform-Dienstprogramm Pakete auf Linux und ThinLinux Clients über den Wyse Management Suite-Server aus:

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

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

- 1 Wenn Sie mit einer öffentlichen Cloud oder einem Remote-Repository in einer privaten Cloud arbeiten, kopieren Sie die RPM-Datei in den Ordner **thinClientApps** im Repository. Standardmäßig sind die aktuellsten Wyse Geräte-Agents und die Plattform-Dienstprogramm-RPMs für Linux und ThinLinux Clients im lokalen Repository verfügbar.
- 2 Gehen Sie auf die Seite **Jobs** und planen Sie einen Job für das Upgrade des Plattform-Dienstprogramm-Add-Ons. Sie müssen warten, bis das Plattform-Dienstprogramm-Add-On erfolgreich auf dem Thin Client installiert wurde.

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

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

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

# Wyse Management Suite-Funktionsmatrix

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

**Tabelle 298. Funktionen im Überblick für jeden Abonnementtyp**

Funktionen	Wyse Management Suite Standard	Wyse Management Suite Pro – private Cloud	Wyse Management Suite Pro – Cloud Edition
Hochgradig skalierbare Lösung zur Verwaltung von Thin Clients	Bis zu 10.000 Geräte freimachen	50.000 Geräte und mehr	1 Million Geräte und mehr
Lizenzschlüssel	Nicht erforderlich	Erforderlich	Erforderlich
Gruppenbasierte Verwaltung	Unterstützt	Unterstützt	Unterstützt
Gruppen mit mehreren Ebenen und Vererbung	Unterstützt	Unterstützt	Unterstützt
Konfigurationsrichtlinienverwaltung	Unterstützt	Unterstützt	Unterstützt
Betriebssystempatch und Abbildverwaltung	Unterstützt	Unterstützt	Unterstützt
Effektive Konfiguration auf Geräteebene nach Vererbung anzeigen	Unterstützt	Unterstützt	Unterstützt
Anwendungsrichtlinienverwaltung	Unterstützt	Unterstützt	Unterstützt
Anlagen-, Bestands- und Systemverwaltung	Unterstützt	Unterstützt	Unterstützt
Automatische Geräteermittlung	Unterstützt	Unterstützt	Unterstützt
Echtzeit-Befehle	Unterstützt	Unterstützt	Unterstützt
Smart planen	Unterstützt	Unterstützt	Unterstützt
Warnungs-, Ereignis- und Überwachungsprotokolle	Unterstützt	Unterstützt	Unterstützt
Sichere Kommunikation (HTTPS)	Unterstützt	Unterstützt	Unterstützt
Verwalten von Geräten hinter einer Firewall	Eingeschränkt*	Eingeschränkt*	Unterstützt
Mobile Anwendung	Nicht unterstützt	Unterstützt	Unterstützt
Warnungen unter Verwendung von E-Mail und mobilen Anwendungen	Nicht unterstützt	Unterstützt	Unterstützt
Scripting-Support für benutzerspezifische Anwendungsinstallation	Nicht unterstützt	Unterstützt	Unterstützt

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

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

# Unterstützte Thin Clients auf der Wyse Management Suite

Tabelle 299. Unterstützte Thin Clients

Thin Clients	Gerätetyp	Build-Nummer und Wyse Geräte-Agent-Versionen
Linux	Wyse 5010 Thin Client Wyse 7010 Thin Client  Wyse 5020 Thin Client Wyse 7020 Thin Client	11.3.106  Wyse Geräte-Agent-Version 2.0.13-00.1  Plattform Utility 1.0.4-01
ThinLinux 1.0	Wyse 5020 Thin Client Wyse 5060 Thin Client Wyse 7020 Thin Client Wyse 3030 LT	1.0.7  Wyse Geräte-Agent-Version 2.4.3-00.01
	Wyse 3040 Thin Client	1.0.71  Wyse Geräte-Agent-Version 2.4.3-00.01
ThinLinux 2.0	Wyse 3040 Thin Client Wyse 5070 Thin Client Wyse 5070 Extended Thin Client	2.2.0.00  Wyse Geräte-Agent 3.4.6-05
ThinLinux 2.2.1	Wyse 5470 Thin Client	2.2.1.00  Wyse Geräte-Agent 3.4.6-06
Windows Embedded Standard 7 (WES7)	Wyse 5010 Thin Client Wyse 7010 Thin Client  Wyse 5020 Thin Client Wyse 7020 Thin Client	7064  Wyse Device Agent 14.4.0.135
	Wyse 3030 Thin Client	7077  Wyse Device Agent 14.4.0.135
	Wyse 7010 Extended Thin Client	7064  Wyse Device Agent 14.4.0.135
Windows Embedded Standard 7P (WES7P)	Wyse 5010 Thin Client Wyse 7010 Thin Client	896  Wyse Device Agent 14.4.0.135

<b>Thin Clients</b>	<b>Gerätetyp</b>	<b>Build-Nummer und Wyse Geräte-Agent-Versionen</b>
	Wyse 5020 Thin Client Wyse 7020 Thin Client	7091 Wyse Device Agent 14.4.0.135
	Wyse 7010 Extended Thin Client	896 Wyse Device Agent 14.4.0.135
	Wyse 7040 Thin Client	7091 Wyse Device Agent 14.4.0.135
	Latitude 3460 mobiler Thin Client Latitude E7270 Mobile Thin Client	7065 Wyse Device Agent 14.4.0.135
	Wyse 5060 Thin Client	7091 Wyse Device Agent 14.4.0.135
Windows 10 IoT Enterprise	Wyse 5020 Thin Client Wyse 7020 Thin Client Wyse 7040 Thin Client	0A79 Wyse Device Agent 14.4.0.135
	Wyse 5070 Thin Client Wyse 5070 Extended Thin Client	10.03.06.10.18.00 Wyse Device Agent 14.4.0.135
	Wyse 5060 Thin Client	0A71 Wyse Device Agent 14.4.0.135
	Latitude 5280 mobiler Thin Client	0A73 Wyse Device Agent 14.4.0.135
	Latitude 3480 mobiler Thin Client	0A72 Wyse Device Agent 14.4.0.135
	Wyse 5470 Thin Client	10.03.08.06.19.00 Wyse Device Agent 14.4.1.5
	Wyse 5470 All-in-One Thin Client	10.03.07.06.19.00 Wyse Device Agent 14.3.0.66
Windows Embedded Standard 8	Wyse 5010 Thin Client Wyse 7010 Thin Client Wyse 5020 Thin Client Wyse 7020 Thin Client	930 Wyse Device Agent 14.4.0.135
	Wyse 5040 AIO Wyse 3010 Thin Client Wyse 3020 Thin Client Wyse 5010 Thin Client (ThinOS, PCOIP)	Firmware 8.5

Thin Clients	Gerätetyp	Build-Nummer und Wyse Geräte-Agent-Versionen
	Wyse 7010 Thin Client Wyse 3030 LT Thin Client Wyse 5060 Thin Client Wyse 3040 Thin Client	
	Wyse 5070 Thin Client Wyse 5070 Extended Thin Client Wyse 5470 Thin Client Wyse 5470 All-in-One Thin Client	Firmware 8.6_185
Teradici	Wyse 5030 Thin Client, Wyse 7030 Thin Client Wyse 5050 Thin Client	Firmware 5.x (5.5.1, 5.4, 5.3) 6.x (6.0, 6.1.1)

# Funknetzwerkprofil-Kennworteditor

Dieser Funknetzwerkprofil-Kennworteditor kann zum Erfassen der Funknetzwerkprofile und zum Bearbeiten von Kennwörtern verwendet werden. Die Profile werden in einer XML-Datei gespeichert. Die gleiche XML-Datei kann zur Konfiguration der Wyse Management Suite über den Cloud Client Manager verwendet werden.

## ANMERKUNG:

.NET Framework 4.5 muss installiert sein, um dieses Tool auf einem Windows-Betriebssystem oder Windows Embedded Betriebssystem auszuführen.

Themen:

- Konfigurieren des Windows Wireless-Profiles
- Konfigurieren des Funknetzwerkprofil-Kennworteditors
- Einschränkungen des Funknetzwerkprofil-Kennworteditors

## Konfigurieren des Windows Wireless-Profiles

So konfigurieren Sie das Windows Wireless-Profil

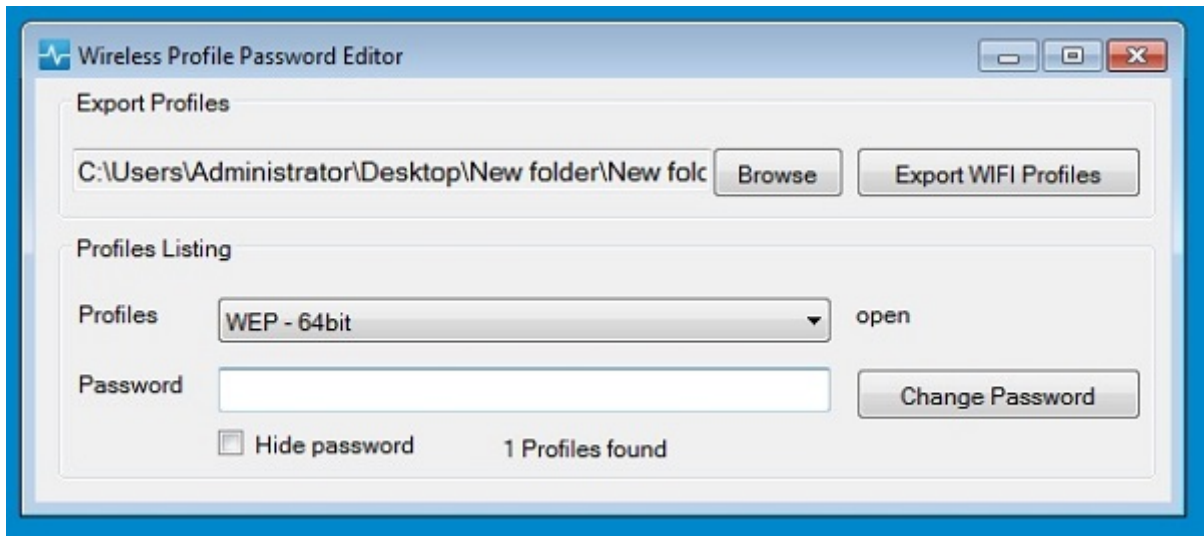
- 1 Gehen Sie zu `C:\Program files\Wyse\WDA\bin\<DWirelessProfileEditor.exe>`.
- 2 Klicken Sie mit der rechten Maustaste auf die EXE-Datei und wählen Sie die Option **Als Administrator ausführen** aus. Das Fenster **Funknetzwerkprofil-Kennworteditor** wird angezeigt.
- 3 Klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort für das neue XML-Profil.
- 4 Klicken Sie auf **Speichern**.
- 5 Wählen Sie aus der Dropdownliste **Profile** das gewünschte Funknetzwerk aus. Klicken Sie auf **Kennwort ändern** zum Ändern des Kennworts, falls erforderlich.
- 6 Klicken Sie auf **Funknetzwerkprofile exportieren**, um das Profil zu speichern.

**ANMERKUNG:** Die exportierte Datei kann von der Seite „Bestand“ in „Apps & Daten“ der Wyse Management Suite importiert werden, um sie auf den Geräten bereitzustellen.

## Konfigurieren des Funknetzwerkprofil-Kennworteditors

So konfigurieren Sie den Funknetzwerkprofil-Kennworteditor:

- 1 Gehen Sie zu `C:\Program files\Wyse\WDA\bin\<DWirelessProfileEditor.exe>`.
- 2 Klicken Sie mit der rechten Maustaste auf die EXE-Datei und wählen Sie die Option **Als Administrator ausführen** aus. Das Fenster **Funknetzwerkprofil-Kennworteditor** wird angezeigt.



**Abbildung 15. Funknetzwerkprofil-Kennworteditor**

- 3 Klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort für das neue XML-Profil.
- 4 Klicken Sie auf die Option **Funknetzwerkprofile exportieren**.  
Das aktuelle Funknetzwerkprofil wird auf die Registerkarte **Profile** exportiert. Das aktuelle Kennwort für die Funkverbindung wird auf der Registerkarte **Kennwort** eingetragen.
- 5 Bearbeiten Sie das Kennwort und klicken Sie auf die Option **Kennwort ändern**.  
Das geänderte Kennwort wird verschlüsselt und im XML-Profil gespeichert.
- 6 Klicken Sie auf der Server-Seite der Wyse Management Suite-Konsole auf die Registerkarte **App & Daten**. Weitere Informationen finden Sie unter [Verwalten des Datei-Repository](#).

## Einschränkungen des Funknetzwerkprofil-Kennworteditors

Im Folgenden werden die Einschränkungen des Funknetzwerkprofil-Kennworteditors beschrieben:

- Kennwörter sind nur für die folgenden Authentifizierungsmethoden gültig:
  - WPAPSK
  - WPA2PSK
- Es sind keine Kennwörter für die folgenden Enterprise-Authentifizierungstypen vorhanden:
  - WPA
  - WPA2

# Erstellen und Konfigurieren von DHCP-Options-Tags

① **ANMERKUNG:** Weitere Informationen zur Sicherheitsumgebung für Kunden finden Sie unter [Wyse-Geräte-Agent](#).

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

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

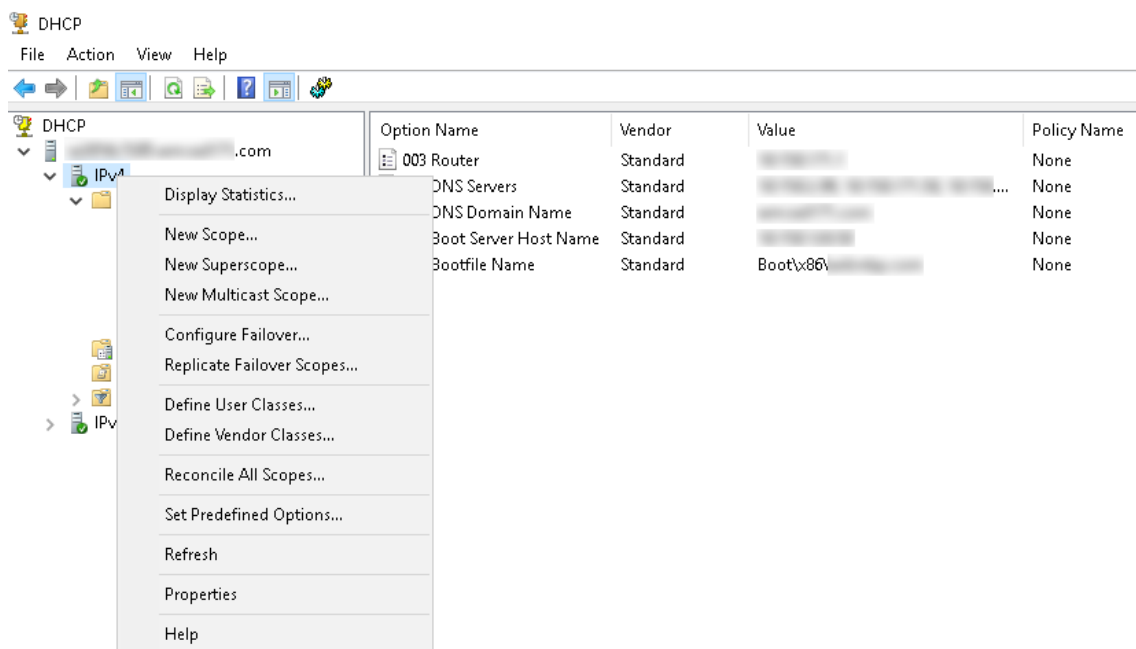


Abbildung 16. DHCP

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

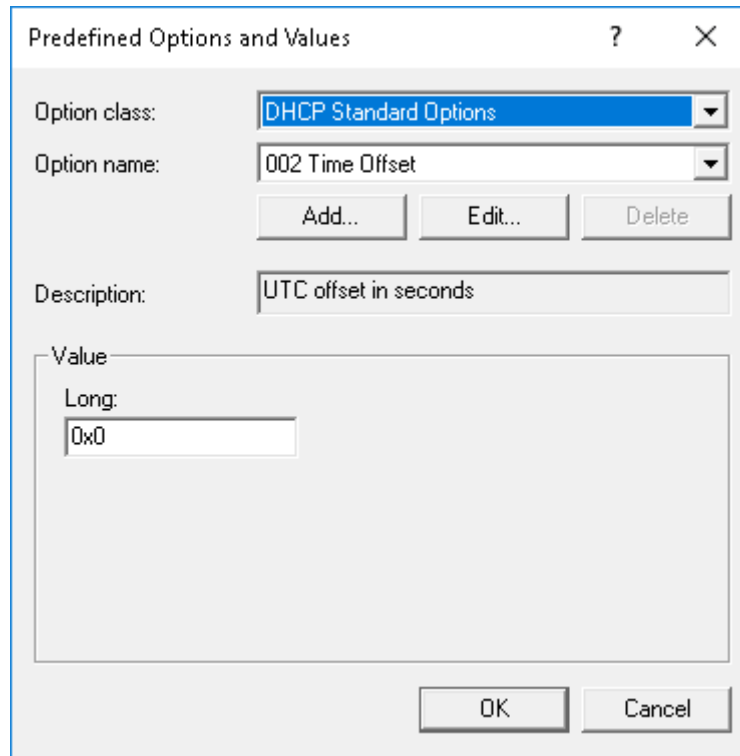


Abbildung 17. Vordefinierte Optionen und Werte

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

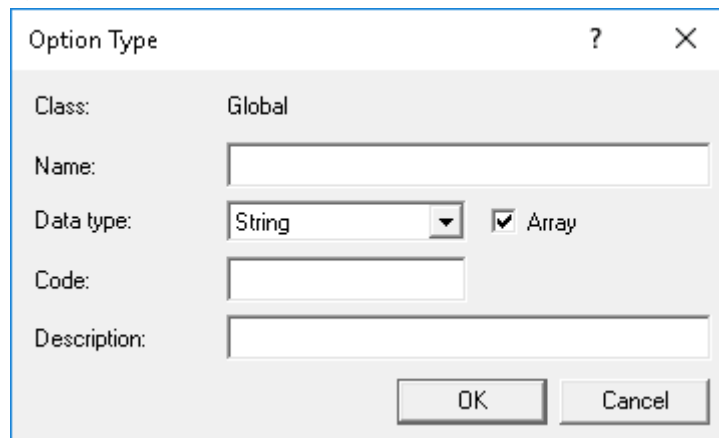


Abbildung 18. Optionstyp

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

### Konfigurieren der DHCP-Option-Tags

- Zum Erstellen des Option-Tags 165 Wyse Management Suite Server-URL gehen Sie wie folgt vor:
  - 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

The image shows a dialog box titled "Predefined Options and Values". It has a standard Windows-style title bar with a question mark and a close button. The dialog contains several input fields and buttons. At the top, there are two dropdown menus: "Option class:" set to "DHCP Standard Options" and "Option name:" set to "165 WMS". Below these are three buttons: "Add...", "Edit...", and "Delete". A text field labeled "Description:" contains the text "WMS\_Server". Below the description field is a section titled "Value" which contains a sub-section "String:" with a text input field containing the text "WMSServerName.YourDomain.Com:443". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

**Abbildung 19. Option-Tag 165 Wyse Management Suite Server-URL**

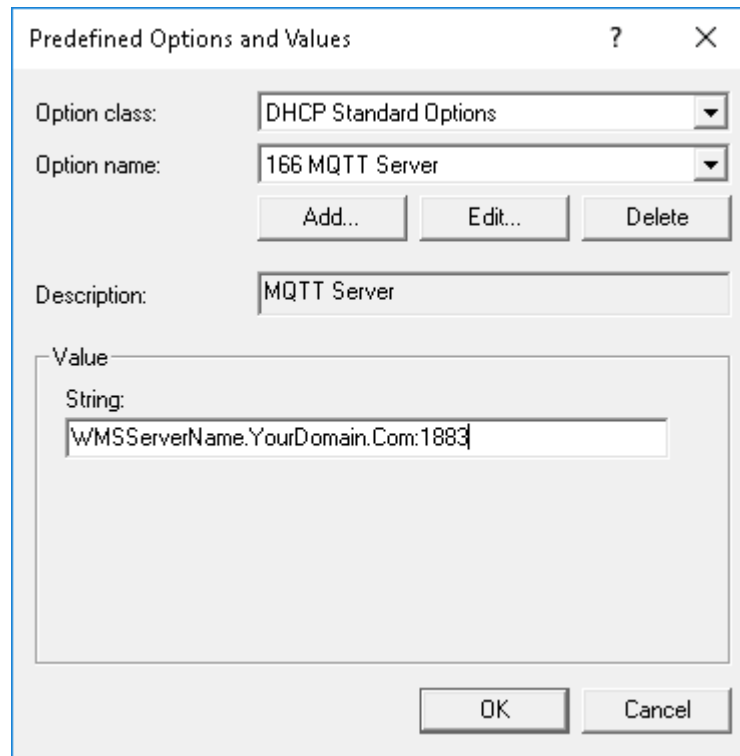
• Zum Erstellen des Option-Tags 166 MQTT-Server-URL gehen Sie wie folgt vor:

- 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**.

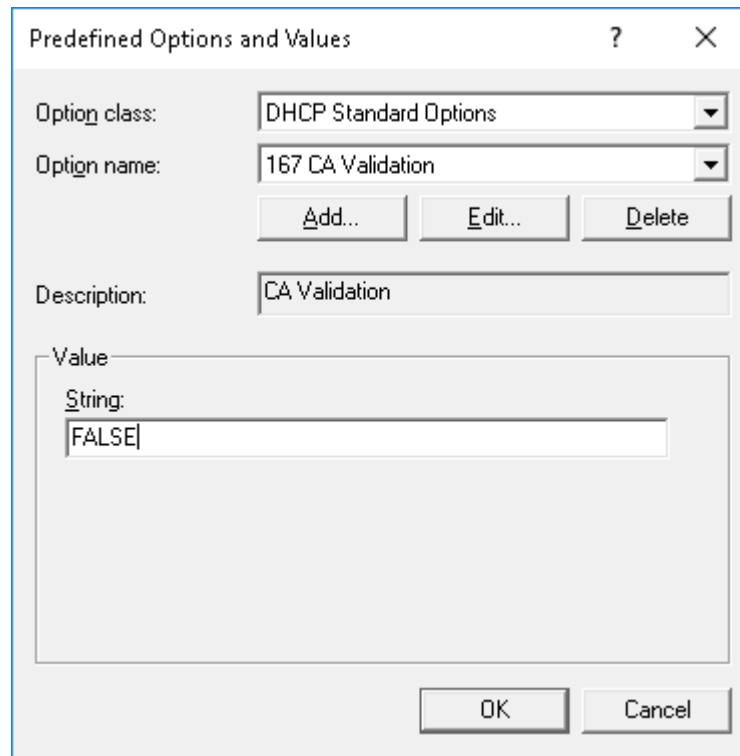
Zeichenfolge –MQTT FQDN

Zum Beispiel WMSServerName.YourDomain.Com:1883



**Abbildung 20. Option-Tag 166 Wyse Management Suite Server-URL**

- Zum Erstellen des Option-Tags 167 Wyse Management Suite CA-Validation-Server-URL gehen Sie wie folgt vor:
  - a Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
    - Name – CA-Validation
    - Datentyp – Zeichenfolge
    - Code – 167
    - Name – CA-Validation
  - b Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.  
Zeichenfolge –WAHR/FALSCH



**Abbildung 21. Option-Tag 167 Wyse Management Suite Server-URL**

- Zum Erstellen des Option-Tags 199 Wyse Management Suite Gruppentoken-Server-URL gehen Sie wie folgt vor:
  - a Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
    - Name – Gruppentoken
    - Datentyp – Zeichenfolge
    - Code – 199
    - Beschreibung – Gruppentoken
  - b Geben Sie die folgenden Werte ein und klicken Sie auf **OK**.
    - Zeichenfolge – defa-Quarantäne

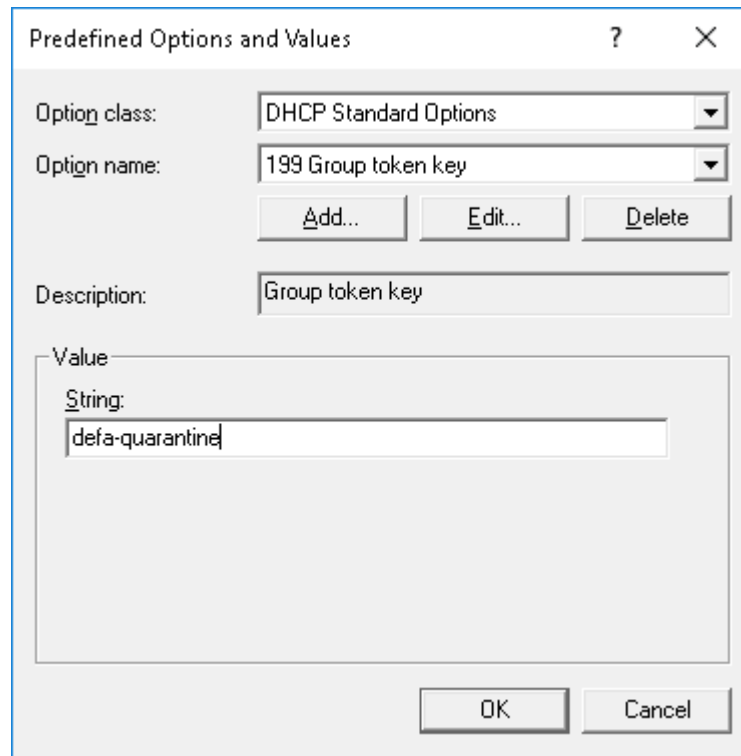


Abbildung 22. Option-Tag 199 Wyse Management Suite Server-URL

# Erstellen und Konfigurieren von DNS-SRV-Einträgen

① **ANMERKUNG:** Weitere Informationen zur Sicherheitsumgebung für Kunden finden Sie unter [Wyse-Geräte-Agent](#).

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

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

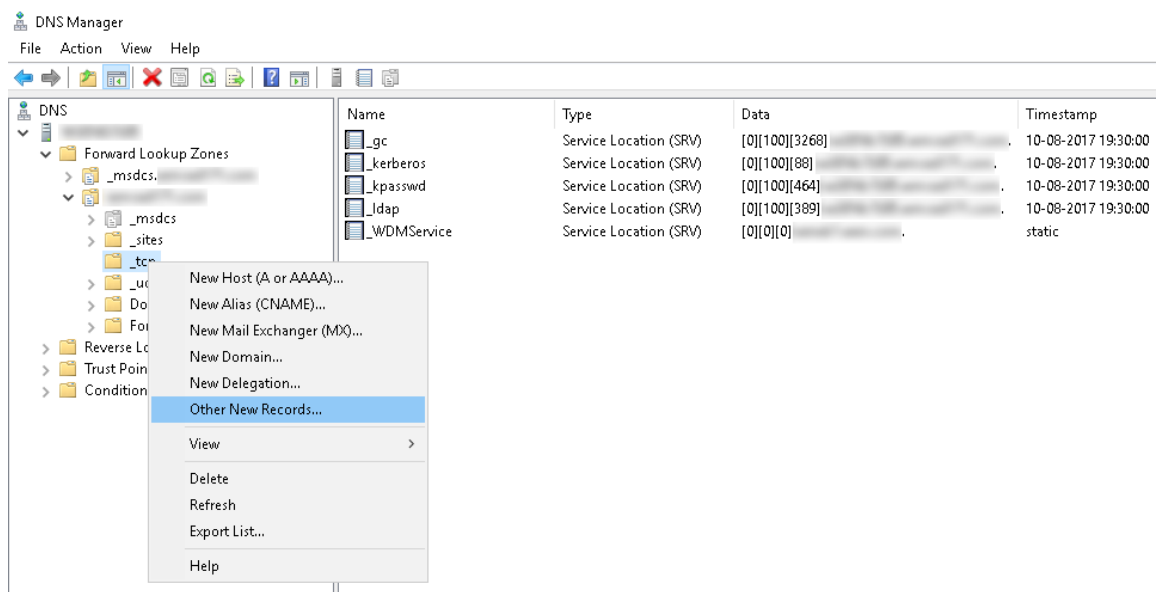


Abbildung 23. DNS-Manager

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

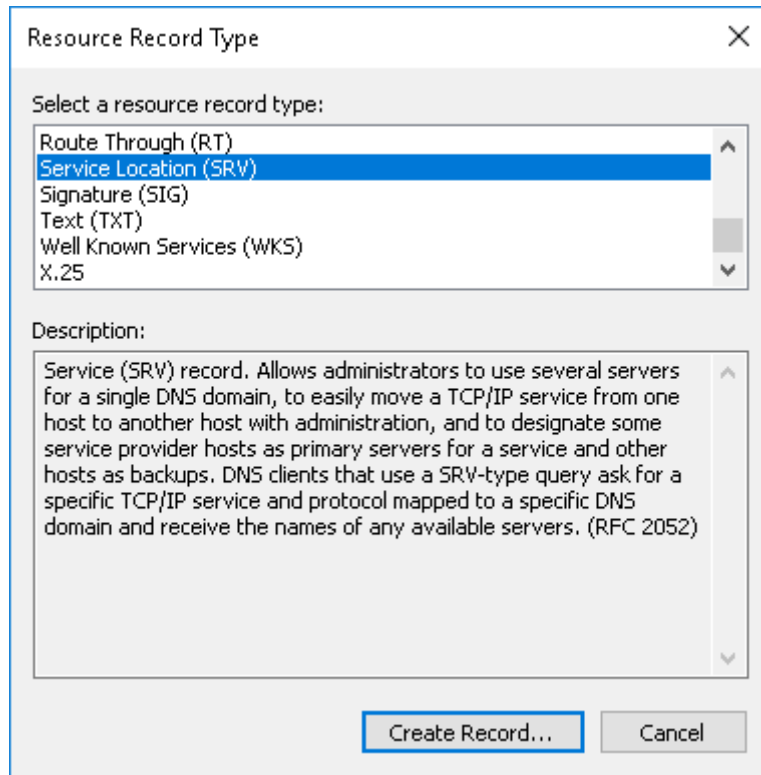


Abbildung 24. Ressourcendatensatztyp

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

New Resource Record

Service Location (SRV)

Domain: [ ]

Service: [\_WMS\_MGMT]

Protocol: [\_tcp]

Priority: [0]

Weight: [0]

Port number: [443]

Host offering this service:  
FQDN of WMS server

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

OK Cancel Help

**Abbildung 25. \_WMS\_MGMT Service**

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

New Resource Record

Service Location (SRV)

Domain: [ ]

Service: \_WMS\_MQTT

Protocol: \_tcp

Priority: 0

Weight: 0

Port number: 1883

Host offering this service:  
FQDN of MQTT server

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

OK Cancel Help

Abbildung 26. \_WMS\_MQTT Service

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

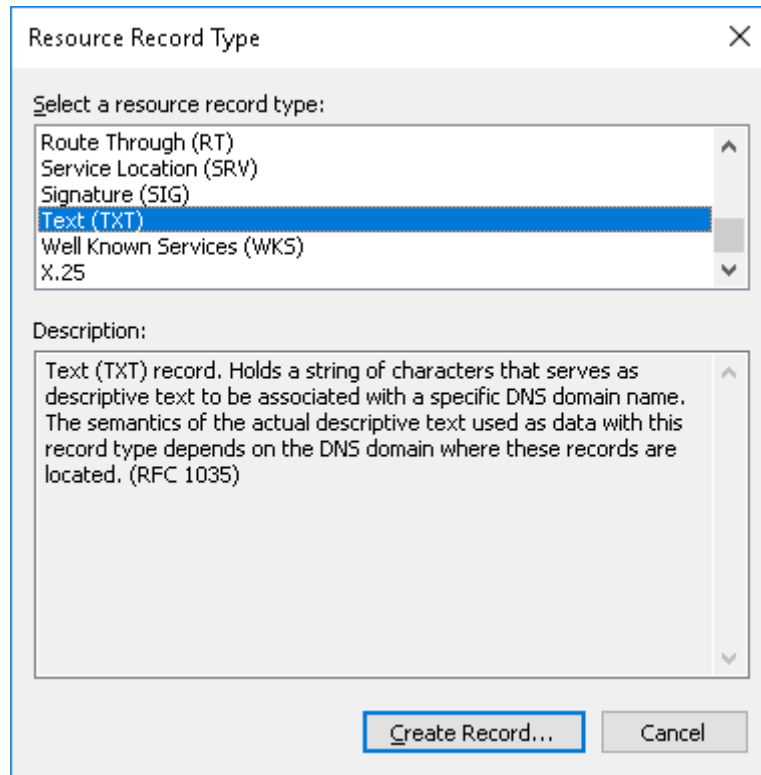
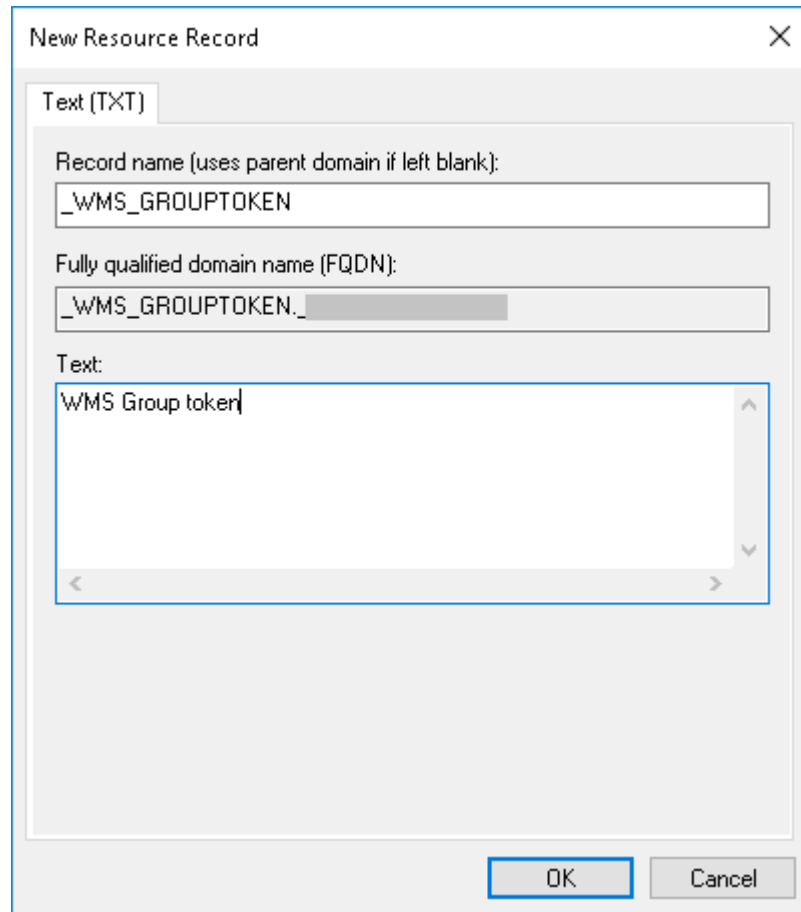


Abbildung 27. Ressourcendatensatztyp

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



**Abbildung 28. \_WMS\_GROUPTOKEN Datensatzname**

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

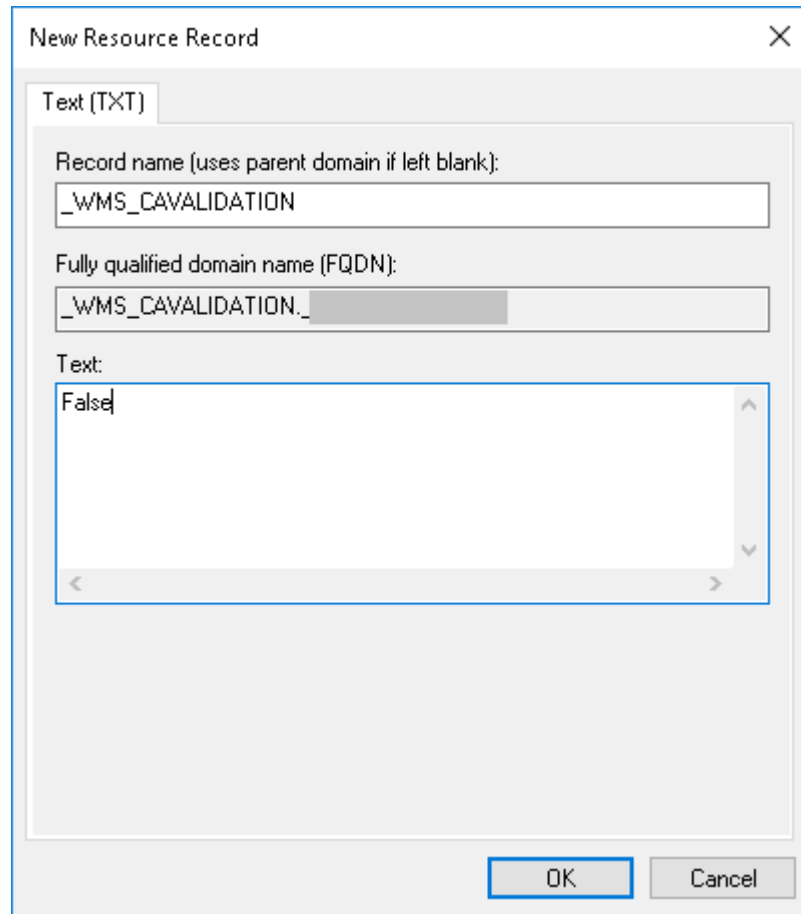


Abbildung 29. \_WMS\_CAVALIDATION Datensatzname

# Schritte zum Ändern des Hostnamens zur IP-Adresse

Schritte zum Ändern des Hostnamens zur IP-Adresse beim Fehlschlagen von Hostnamenlösungen:

- 1 Öffnen Sie die DOS-Eingabeaufforderung im erhöhten Administratormodus
- 2 Ändern Sie das Verzeichnis zu `C:\Program Files\DELL\WMS\MongoDB\bin`.
- 3 Geben Sie den folgenden Befehl ein: `mongo localhost -username stratus -p --authenticationDatabase admin`  
Ausgabe: MongoDB Shell Version v3.4.10
- 4 Geben Sie das Kennwort ein.  
Ausgabe:
  - connecting to: mongod://127.0.0.1:27017/localhost
  - MongoDB-Serverversion: 3.4.10
- 5 Geben Sie Folgendes ein: `use stratus`  
Ausgabe: switched to db stratus
- 6 Geben Sie den folgenden Befehl ein: `> db.bootstrapProperties.updateOne( {'name': 'stratusapp.server.url'}, {$set : {'value' : "https://IP:443/ccm-web"}} )`  
Ausgabe: `{ "acknowledged" : true, "matchedCount" : 1, "modifiedCount" : 1 }`
- 7 Geben Sie den folgenden Befehl ein: `> db.getCollection('bootstrapProperties').find({'name': 'stratusapp.server.url'})`  
Ausgabe: `{ "_id" : ObjectId("5b97905e48b7b7e99ad22aa6"), "name" : "stratusapp.server.url", "value" : "https://IP:443/ccm-web", "isActive" : true, "committed" : true }`