



**HP ThinPro 6.1**

**Administratorhandbuch**

© Copyright 2016 HP Development Company, L.P.

Dokumentennummer: 903662-042

## Open-Source-Software

Citrix und XenDesktop sind Marken von Citrix Systems, Inc. und/oder einer der zugehörigen Tochtergesellschaften und sind beim United States Patent and Trademark Office sowie u. U. in anderen Ländern registriert. Linux® ist eine eingetragene Marke von Linus Torvalds in den USA und anderen Ländern. Microsoft, Windows, Windows Vista und Windows Server sind in den USA und/oder anderen Ländern Marken oder eingetragene Marken der Microsoft Corporation. UNIX ist eine eingetragene Marke von The Open Group. VMware und Horizon View sind in den USA und/oder anderen Ländern eingetragene Marken oder Marken von VMware, Inc.

Vertrauliche Computersoftware. Für den Besitz, die Verwendung oder das Kopieren dieser Computersoftware ist eine gültige Lizenz von HP erforderlich. Im Einklang mit FAR 12.211 und 12.212 werden der US-Regierung gewerbliche Computersoftware, Dokumentationen zur gewerblichen Computersoftware sowie technische Daten für „gewerbliche Einheiten“ (Commercial Items) gemäß der gewerblichen Standardlizenz des Anbieters zur Verfügung gestellt.

HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Ferner übernimmt sie keine Haftung für Schäden, die direkt oder indirekt auf die Bereitstellung, Leistung und Nutzung dieses Materials zurückzuführen sind. HP haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt.

Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Informationen in dieser Veröffentlichung werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt. Insbesondere enthalten diese Informationen keinerlei zugesicherte Eigenschaften. Alle sich aus der Verwendung dieser Informationen ergebenden Risiken trägt der Benutzer.

Die Garantien für HP Produkte und Services werden ausschließlich in der zum Produkt bzw. Service gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantieansprüche abzuleiten.

Zweite Ausgabe: Juli 2016

Erste Ausgabe: Juni 2016

Dieses Produkt enthält Software, die unter einer Open-Source-Software-Lizenz, wie der GNU General Public License und der GNU Lesser General Public License oder einer anderen Open-Source-Lizenz lizenziert ist. Soweit HP verpflichtet ist, oder nach eigenem Ermessen entscheidet, den Quellcode für solche Software unter der anwendbaren Open-Source-Software-Lizenz verfügbar zu machen, erhalten Sie den Quellcode für die Software unter ftp: <ftp://ftp.hp.com/pub/tcdebian/pool/thinpro60/source/>.

## Allgemeines

Die Befehlszeilensyntax in diesem Handbuch verwendet möglicherweise eines oder mehrere der in der folgenden Tabelle beschriebenen Elemente.



**HINWEIS:** Die Groß-/Kleinschreibung wird für die Befehlszeilensyntax *nicht* beachtet, sofern nicht anders angegeben.

Element	Beschreibung
<i>Kursiv</i>	<p>Kursivtext bezieht sich auf einen benutzerdefinierten Parameter wie nachfolgend angegeben:</p> <pre>location=<i>IpAddress</i>:<i>Port</i></pre> <p>Für den zuvor genannten Parameter wird etwa folgendes Beispiel eingegeben:</p> <pre>location=192.168.0.10:8080</pre>
[ ]	<p>Klammern kennzeichnen optionale Parameter wie unten angegeben:</p> <pre>location=<i>IpAddress</i>[ :<i>Port</i>]</pre> <p>Für den oben genannten Parameter würden Sie eines der beiden folgenden Beispiele eingeben:</p> <pre>location=192.168.0.10</pre> <pre>location=192.168.0.10:8080</pre>
 {   }	<p>Ein senkrechter Strich steht für den <code>or</code>-Operator und trennt Optionen für einen benutzerdefinierten Parameter, der einen begrenzten Satz an möglichen Werten aufweist. Eine Reihe von Optionen ist möglicherweise auch in geschweiften Klammern eingeschlossen, um sie von den anderen Teilen der Syntax zu unterscheiden, wie unten angezeigt:</p> <pre>speed={high   medium   low}</pre> <p>Für den oben genannten Parameter wird nur eine der folgenden Optionen eingegeben:</p> <pre>speed=high</pre> <pre>speed=medium</pre> <pre>speed=low</pre>
" " ' '	<p>Einige Parameter erfordern unter Umständen doppelte Anführungszeichen, einfache Anführungszeichen oder beide, wie unten angegeben:</p> <pre>location="<i>IpAddress</i> '<i>Port</i>' "</pre> <p>Für den zuvor genannten Parameter wird etwa folgendes Beispiel eingegeben:</p> <pre>location="'192.168.0.10' '8080'"</pre>
...	<p>Eine Ellipse bezieht sich auf einen sich wiederholenden Parameter. Die folgenden Beispiele demonstrieren verschiedene Möglichkeiten, mit denen ein sich wiederholender Parameter implementiert werden kann.</p> <p>Für den folgenden Parameter sind exakt zehn Gerätenamen erforderlich:</p> <pre>DeviceNames=<i>Device1</i> <i>Device2</i> ... <i>Device10</i></pre> <p>Für den folgenden Parameter ist mindestens ein Gerätenamen erforderlich und er kann insgesamt bis zu zehn Gerätenamen enthalten:</p> <pre>DeviceNames=<i>Device1</i> [<i>Device2</i> ... <i>Device10</i>]</pre> <p>Für den folgenden Parameter ist mindestens ein Gerätenamen erforderlich und er kann eine unbegrenzte Anzahl an zusätzlichen Gerätenamen enthalten:</p> <pre>DeviceNames=<i>Device1</i> [<i>Device2</i> ... ]</pre>



---

# Inhaltsverzeichnis

<b>1 Einführung</b>	<b>1</b>
So finden Sie weitere Informationsquellen	1
Auswählen einer Betriebssystemkonfiguration	2
Auswählen eines Remoteverwaltungsdiensts	3
Erstmaliges Starten des Thin Clients	3
Wechseln zwischen Administratormodus und Benutzermodus	4
<b>2 Übersicht über die Benutzeroberfläche</b>	<b>5</b>
Desktop	5
Taskleiste	6
Connection Manager (nur ThinPro)	7
<b>3 Verbindungskonfiguration</b>	<b>8</b>
Erweiterte Verbindungseinstellungen	8
Kioskmodus	9
<b>4 Verbindungstypen</b>	<b>10</b>
Citrix	10
Citrix – Allgemeine Einstellungen	10
Optionen	10
Local Resources (Lokale Ressourcen)	11
Window (Fenster)	11
Firewall	12
Keyboard Shortcuts (Tastenkombinationen)	12
Session (Sitzung)	13
Citrix-Einstellungen pro Verbindung	13
Connection (Verbindung)	13
Configuration (Konfiguration)	14
Advanced (Erweitert)	15
HP True Graphics	15
Serverseitige Anforderungen für HP True Graphics	15
XenApp/XenDesktop	15
HDX 3D Pro	15
Überprüfen der Serveroptionen für die Komprimierung	15
Clientseitige Konfiguration von HP True Graphics	16
Komprimierungseinstellungen	16

	Fenstereinstellungen .....	16
	Monitorlayout- und Hardwarebeschränkungen .....	16
RDP .....		17
	RDP – Allgemeine Einstellungen .....	17
	RDP-Einstellungen pro Verbindung .....	17
	Netzwerk .....	17
	Dienst .....	18
	Fenster .....	18
	Optionen .....	19
	Lokale Ressourcen .....	20
	Experience (Darstellung) .....	20
	Diagnostics (Diagnose) .....	21
	Erweitert .....	22
	RemoteFX .....	22
	RDP-Sitzungen mit mehreren Monitoren .....	22
	RDP-Multimedia-Umleitung .....	23
	RDP-Geräteumleitung .....	23
	RDP-USB-Umleitung .....	23
	RDP-Massenspeicherumleitung .....	24
	RDP-Druckerumleitung .....	24
	RDP-Audiumleitung .....	25
	RDP-Smart Card-Umleitung .....	26
VMware Horizon View .....		26
	VMware Horizon View-Einstellungen pro Verbindung .....	26
	Netzwerk .....	26
	Allgemein .....	26
	Security (Sicherheit) .....	27
	RDP-Optionen .....	27
	RDP Experience (RDP-Darstellung) .....	29
	Advanced (Erweitert) .....	30
	VMware Horizon View-Sitzungen mit mehreren Monitoren .....	30
	VMware Horizon View-Tastenkombinationen .....	31
	VMware Horizon View-Multimedia-Umleitung .....	31
	VMware Horizon View-Geräteumleitung .....	31
	VMware Horizon View-USB-Umleitung .....	31
	VMware Horizon View-Massenspeicherumleitung .....	31
	VMware Horizon View-Druckerumleitung .....	32
	VMware Horizon View-Audiumleitung .....	32
	VMware Horizon View-Smart Card-Umleitung .....	33
	VMware Horizon View-Webcam-Umleitung .....	33
	Ändern des VMware Horizon View-Protokolls .....	34

Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung .....	34
Web Browser .....	35
Web Browser – Allgemeine Einstellungen .....	35
Web Browser-Einstellungen pro Verbindung .....	36
Configuration (Konfiguration) .....	36
Advanced (Erweitert) .....	36
Zusätzliche Verbindungstypen (nur ThinPro) .....	36
TeemTalk .....	36
Configuration (Konfiguration) .....	36
TeemTalk Session Wizard (TeemTalk-Sitzungsassistent) .....	37
Advanced (Erweitert) .....	38
XDMCP .....	38
Configuration (Konfiguration) .....	38
Advanced (Erweitert) .....	38
SSH .....	39
Configuration (Konfiguration) .....	39
Advanced (Erweitert) .....	39
Telnet .....	39
Configuration (Konfiguration) .....	39
Advanced (Erweitert) .....	40
Custom .....	41
Configuration (Konfiguration) .....	41
Advanced (Erweitert) .....	41
<b>5 Systemsteuerung .....</b>	<b>42</b>
Peripheriegeräte .....	42
Clientaggregation .....	43
Konfigurieren der Clientaggregation .....	44
Konfigurieren der Aggregation-Clients .....	44
Konfigurieren des Aggregation-Servers .....	45
Anzeigeeinstellungen .....	45
Konfigurieren von Druckern .....	46
USB-Geräte umleiten .....	46
Setup .....	47
Netzwerkeinstellungen .....	47
Einstellungen für kabelgebundene Netzwerke .....	48
WLAN-E instellungen .....	49
DNS-Einstellungen .....	49
IPSec-Regeln .....	50
Konfigurieren von VPN-Einstellungen .....	50
Konfigurieren von HP Velocity .....	51

Anpassungszentrum .....	51
Verwaltung .....	52
Komponenten-Manager .....	53
Entfernen von Komponenten .....	53
Rückgängigmachen einer Änderung .....	53
Dauerhaftes Anwenden der Änderungen .....	53
HP ThinState .....	54
Verwalten von HP ThinPro-Images .....	54
Aufzeichnung von HP ThinPro-Images auf einem FTP-Server .....	54
Bereitstellung eines HP ThinPro-Images über FTP oder HTTP .....	54
Aufzeichnen eines HP ThinPro-Images auf einem USB-Flash-Laufwerk ....	55
Bereitstellung eines HP ThinPro-Images mit einem USB-Flash-	
Laufwerk .....	55
Verwalten eines Clientprofils .....	56
Speichern eines Clientprofils auf einem FTP-Server .....	56
Wiederherstellen eines Clientprofils über FTP oder HTTP .....	56
Speichern eines Clientprofils auf einem USB-Flash-Laufwerk .....	57
Wiederherstellen eines Clientprofils von einem USB-Flash-Laufwerk .....	57
VNC-Shadowing .....	57
Advanced (Erweitert) .....	58
Zertifikate .....	59
Zertifikat-Manager .....	59
SCEP Manager .....	59
DHCP-Optionen .....	59
<b>6 Systeminformationen .....</b>	<b>61</b>
<b>7 HP Smart Client Services .....</b>	<b>62</b>
Unterstützte Betriebssysteme .....	62
Voraussetzungen für HP Smart Client Services .....	62
Abrufen von HP Smart Client Services .....	63
Anzeigen der Automatic Update-Website .....	63
Erstellen eines Automatic Update-Profiles .....	63
Profile für bestimmte MAC-Adressen .....	63
Aktualisieren von Thin Clients .....	64
Verwenden der Methode zur Aktualisierung per Übertragung .....	64
Verwenden der Methode zur Aktualisierung per DHCP-Kennung .....	64
Beispiel für die Durchführung DHCP-Kennung .....	64
Verwenden der Methode zur Aktualisierung per DNS-Alias .....	65
Verwenden der Methode zur manuellen Aktualisierung .....	65
Durchführen einer manuellen Aktualisierung .....	66

<b>8 Profile Editor .....</b>	<b>67</b>
Öffnen von Profile Editor .....	67
Laden eines Clientprofils .....	67
Anpassung von Clientprofilen .....	67
Auswählen der Plattform für ein Clientprofil .....	67
Konfigurieren einer Standardverbindung für ein Clientprofil .....	68
Ändern von Registrierungseinstellungen eines Clientprofils .....	68
Hinzufügen von Dateien zu einem Clientprofil .....	68
Hinzufügen einer Konfigurationsdatei zu einem Clientprofil .....	69
Hinzufügen von Zertifikaten zu einem Clientprofil .....	69
Hinzufügen eines symbolischen Links zu einem Clientprofil .....	70
Speichern des Clientprofils .....	70
Konfiguration eines seriellen oder parallelen Druckers .....	70
Abrufen der Druckereinstellungen .....	70
Einrichten von Druckeranschlüssen .....	70
Installieren von Druckern auf dem Server .....	71
<b>9 Fehlerbeseitigung .....</b>	<b>73</b>
Fehlerbeseitigung bei der Netzwerkverbindung .....	73
Fehlerbeseitigung bei abgelaufenen Citrix-Kennwörtern .....	73
Verwenden der Systemdiagnose für die Fehlerbeseitigung .....	74
Speichern von Systemdiagnosedaten .....	74
Dekomprimieren der Systemdiagnosedateien .....	74
Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen .....	74
Dekomprimieren der Systemdiagnosedateien auf Linux- oder Unix-basierten Systemen .....	74
Anzeigen der Systemdiagnosedateien .....	74
Anzeigen von Dateien im Ordner Befehle .....	75
Anzeigen von Dateien im Ordner /var/log .....	75
Anzeigen von Dateien im Ordner /etc .....	75
<b>Anhang A USB-Updates .....</b>	<b>76</b>
HP ThinUpdate .....	76
<b>Anhang B BIOS-Tools .....</b>	<b>77</b>
BIOS-Tool für Einstellungen .....	77
BIOS Flashing-Tool .....	77
<b>Anhang C Ändern der Größe der Flash-Laufwerk-Partition .....</b>	<b>78</b>

<b>Anhang D Registrierungsschlüssel .....</b>	<b>79</b>
Audio .....	79
CertMgr .....	80
ConnectionManager .....	80
ConnectionType .....	80
custom .....	80
firefox .....	84
freerdp .....	89
ssh .....	100
teemtalk .....	105
telnet .....	108
view .....	112
xdmcp .....	121
xen .....	125
CpuMgr .....	139
DHCP .....	139
Dashboard .....	139
Display .....	140
Network .....	142
SCIM .....	148
ScepMgr .....	148
Search .....	149
Serial .....	150
SystemInfo .....	150
TaskMgr .....	151
USB .....	151
auto-update .....	152
background .....	154
config-wizard .....	155
desktop .....	155
entries .....	156
keyboard .....	156
logging .....	157
mouse .....	157
restore-points .....	158
screensaver .....	158
security .....	159
sshd .....	159
time .....	160
touchscreen .....	160
translation .....	162

usb-update .....	162
users .....	163
vncserver .....	165

<b>Index .....</b>	<b>168</b>
--------------------	------------



# 1 Einführung

Dieses Handbuch ist für Administratoren von HP Thin Clients vorgesehen, die auf dem HP ThinPro-Betriebssystem basieren. Es wird davon ausgegangen, dass Sie sich beim System als Administrator anmelden, wenn Sie anhand der Beschreibungen in diesem Handbuch Systemkonfigurationen ändern oder Verwaltungstools verwenden.

 **HINWEIS:** Für HP ThinPro sind zwei Betriebssystemkonfigurationen möglich: ThinPro und Smart Zero. HP ThinPro-basierte Thin Clients können mit einer der Betriebssystemkonfigurationen als Standard erworben werden. Sie können über die Systemsteuerung zwischen den Betriebssystemkonfigurationen wechseln.

Weitere Informationen über diese Betriebssystemkonfigurationen finden Sie unter [Auswählen einer Betriebssystemkonfiguration auf Seite 2](#). Weitere Informationen über das Wechseln zwischen Betriebssystemkonfigurationen finden Sie unter [Anpassungscenter auf Seite 51](#).

## So finden Sie weitere Informationsquellen

Ressource	Inhalt
HP Support-Website <a href="http://www.hp.com/support">http://www.hp.com/support</a>	Wiederherstellungs-Images, Verwaltungstools und weitere Software-Add-ons und -Updates  ▲ Suchen Sie nach dem Thin Client-Modell und dann sehen Sie den Abschnitt <b>Optionen herunterladen</b> der Supportseite für dieses Modell.  Handbücher für Administratoren, Hardware-Referenzhandbücher, White Papers und weitere Dokumentationen  ▲ Suchen Sie nach dem Thin Client-Modell und dann sehen Sie den Abschnitt <b>Handbücher</b> der Supportseite für dieses Modell.  <b>HINWEIS:</b> HP Device Manager und HP Remote Graphics Software verfügen jeweils über eine dedizierte Supportseite. Suchen Sie daher nach dem Namen der App und schauen Sie dann im Abschnitt <b>Handbücher</b> nach.  <b>HINWEIS:</b> Die Sprachunterstützung für Software und Dokumentation kann variieren. Einige Inhalte sind nur auf Englisch verfügbar.
Microsoft Support-Website <a href="http://support.microsoft.com">http://support.microsoft.com</a>	Dokumentation für Microsoft Software
Citrix Support-Website <a href="http://www.citrix.com/support">http://www.citrix.com/support</a>	Dokumentation für Citrix Software
VMware Support-Website <a href="http://www.vmware.com/support">http://www.vmware.com/support</a>	Dokumentation für VMware Software

# Auswählen einer Betriebssystemkonfiguration

HP ThinPro umfasst zwei Betriebssystemkonfigurationen, die jeweils auf ein anderes Thin Client-Bereitstellungsszenario zugeschnitten sind:

- Die **ThinPro**-Betriebssystemkonfiguration ist die vollständige Version des Betriebssystems und ist am besten für Umgebungen geeignet, die mehreren Zwecken dienen und in denen eine erweiterte Verwaltung oder Endbenutzeranpassung erforderlich ist. Folgende Funktionen gehören zu dieser Betriebssystemkonfiguration:
  - Anzeige des ThinPro-Desktops nach dem Systemstart
  - Mehr Verbindungstypen als Smart Zero
  - Gleichzeitige Konfiguration und Ausführung mehrerer Verbindungen (unterstützter Typen)
- Die **Smart Zero**-Betriebssystemkonfiguration ist eine einfachere, sicherere Version des Betriebssystems und ist am besten für Umgebungen geeignet, die wie Kioskcomputer einem Zweck dienen und in denen eine minimale Verwaltung und kaum oder sogar keine Endbenutzeranpassung erforderlich ist. Folgende Funktionen gehören zu dieser Betriebssystemkonfiguration:
  - Anzeige einer virtuellen Sitzung und Ausblenden des Desktops (wird auch als „Kioskmodus“ bezeichnet) nach dem Systemstart
  - Weniger Verbindungstypen als ThinPro
  - Konfiguration und Ausführung von nur einer Verbindung gleichzeitig



**HINWEIS:** Sie können über die Systemsteuerung zwischen Betriebssystemkonfigurationen wechseln (siehe [Anpassungszentrum auf Seite 51](#)).

Sie können auch einige der Standardeinstellungen der Betriebssystemkonfigurationen anpassen. Beispielsweise können Sie die verfügbaren Verbindungstypen ändern, den Kioskmodus für ThinPro aktivieren oder beim Systemstart für Smart Zero den Desktop anzeigen.

Weitere Informationen zum Kioskmodus finden Sie unter [Kioskmodus auf Seite 9](#).

In der folgenden Tabelle sind die standardmäßig verfügbaren Verbindungstypen für jede Betriebssystemkonfiguration aufgeführt.

Betriebssystemkonfiguration	Verfügbare Standard-Verbindungstypen
ThinPro	<ul style="list-style-type: none"><li>• Citrix®</li><li>• RDP</li><li>• VMware® Horizon® View™</li><li>• Web Browser (Firefox)</li><li>• TeamTalk</li><li>• XDMCP</li><li>• SSH</li><li>• Telnet</li><li>• Custom</li></ul>
Smart Zero	<ul style="list-style-type: none"><li>• Citrix</li><li>• RDP</li><li>• VMware Horizon View</li></ul>

Betriebssystemkonfiguration	Verfügbare Standard-Verbindungstypen
	<ul style="list-style-type: none"> <li>• Web Browser (Firefox)</li> </ul>

## Auswählen eines Remoteverwaltungsdiensts

Unabhängig von der Betriebssystemkonfiguration gibt es zwei verschiedene Remoteverwaltungsdienste, mit denen Sie HP ThinPro-basierte Thin Clients verwalten können:

- **HP Device Manager (HPDM)** ist ideal für große Umgebungen mit einer Vielzahl von Betriebssystemen, einschließlich einer Mischung von HP ThinPro- und Windows®-basierten Thin Clients. HPDM bietet eine größere Vielfalt bei den Verwaltungsoptionen als HP Smart Client Services. Weitere Informationen zu HPDM und eine Downloadoption finden Sie unter <http://www.hp.com/go/hpdm>.
- **HP Smart Client Services** können nur HP ThinPro-basierte Thin Clients verwalten und wurden für die Verwendung mit Smart Zero und ein Szenario ohne Verwaltung optimiert. Weitere Informationen finden Sie unter „[HP Smart Client Services](#)“ auf Seite 62. HP Smart Client Services können Sie von der HP Support-Website herunterladen (siehe [So finden Sie weitere Informationsquellen auf Seite 1](#)).

HP empfiehlt die Prüfung beider Dienste, um den für Ihre Bereitstellung am besten geeigneten Dienst auszuwählen.

## Erstmaliges Starten des Thin Clients

Wenn Sie einen neuen Thin Client mit HP ThinPro zum ersten Mal starten, wird ein Setup-Programm automatisch ausgeführt. Im folgenden Verfahren wird der Setup-Vorgang beschrieben:

1. Zuerst sucht das Setup-Programm nach einer Netzwerkverbindung. Wenn bestimmte Netzwerkeinstellungen erforderlich sind, wählen Sie die Schaltfläche **Netzwerkeinstellungen**, um Netzwerkmanager zu öffnen (weitere Informationen finden Sie unter [Netzwerkeinstellungen auf Seite 47](#)).
2. Dann bestimmt das Setup-Programm, ob der Thin Client von einem Remoteverwaltungsdienst (HPDM oder HP Smart Client Services) verwaltet wird.

Wenn der Thin Client von einem der Dienste remote verwaltet wird, wird das Setup-Programm beendet. Anschließend werden die über den Dienst vordefinierten Konfigurationen auf den Thin Client angewendet. Der Rest dieses Verfahrens gilt für Thin Clients mit Remoteverwaltung nicht.

Wird der Thin Client nicht von einem der Dienste remote verwaltet, fahren Sie mit diesem Verfahren fort.

3. Anschließend bestimmt das Setup-Programm, ob ein Image-Update von HP verfügbar ist. Falls ja, wählen Sie **IJetzt installieren** auf der Seite **Software-Update**, um das Image zu aktualisieren.
4. Wenn Sie ermitteln möchten, ob Service Packs oder Package-Updates verfügbar sind, wählen Sie **Easy Update**, um die HP Easy Tools zu starten. Im *Administratorhandbuch* für HP Easy Tools finden Sie weitere Informationen zur Verwendung von Easy Update. Fahren Sie dann mit diesem Verfahren fort.
5. Wenn Sie den HPDM Agent (die Clientkomponente von HPDM) oder die Automatic Update-Einstellungen für HP Smart Client Services manuell konfigurieren möchten, wählen Sie die Registerkarte **Geräteverwaltung** im Setup-Programm. Wählen Sie dann die entsprechende Option.

6. Wenn Sie bei jedem Start des Thin Clients nach Software-Updates suchen möchten, aktivieren Sie die Option **Bei jedem Start nach Software-Updates suchen**.

Wenn Sie beim Upgrade der Image-Version alle lokalen Einstellungen beibehalten möchten, aktivieren Sie die Option **Thin Client-Konfiguration beibehalten**.

7. Wenn Sie das Setup-Programm schließen, ohne dass Verbindungen konfiguriert sind, wird ein Assistent geöffnet, der Ihnen beim Konfigurieren einer Verbindung hilft.

---

 **TIPP:** Wenn Sie die Konfiguration eines Thin Clients ändern und dann die Konfiguration kopieren und auf anderen Thin Clients bereitstellen möchten, ändern Sie zuerst mit der Systemsteuerung die Konfiguration (weitere Informationen finden Sie unter [„Übersicht über die Benutzeroberfläche“ auf Seite 5](#) und [„Systemsteuerung“ auf Seite 42](#)). Stellen Sie dann die Konfiguration mit HPDM oder HP ThinState bereit (siehe [HP ThinState auf Seite 54](#)).

---

## Wechseln zwischen Administratormodus und Benutzermodus

- ▲ Klicken Sie mit der rechten Maustaste auf den Desktop und wählen Sie dann im Menü **Wechseln zwischen Administrator-/Benutzermodus**.

Weitere Informationen zum Desktop finden Sie unter [Desktop auf Seite 5](#).

– oder –

Wählen Sie in der Systemsteuerung **Wechseln zwischen Administrator-/Benutzermodus**.

Weitere Informationen zur Systemsteuerung finden Sie unter [Taskleiste auf Seite 6](#) und [„Systemsteuerung“ auf Seite 42](#).

---

 **HINWEIS:** Wenn Sie zum ersten Mal in den Administratormodus wechseln, werden Sie aufgefordert, ein Administratorkennwort einzurichten. Das Administratorkennwort muss dann jedes Mal eingegeben werden, wenn Sie wieder in den Administratormodus wechseln.

Wenn Sie sich im Administratormodus befinden, ist der Bildschirm rot umrandet.

---

## 2 Übersicht über die Benutzeroberfläche

### Desktop

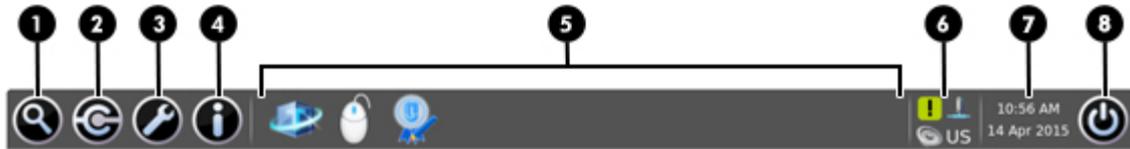
 **HINWEIS:** In der folgenden Abbildung wird der Desktop für ThinPro mit einem US-Gebietsschema veranschaulicht. Bei Smart Zero ist die Taskleiste standardmäßig senkrecht und rechtsbündig. Das Desktopdesign hängt vom Verbindungstyp ab. Das Anzeigeformat einiger Informationen der Taskleiste unterscheidet sich je nach Gebietsschema.



Symbol	Beschreibung
(1)	Desktop In ThinPro können Sie Verbindungsverknüpfungen im Desktopbereich anordnen und das Hintergrunddesign anpassen. In Smart Zero wird der Desktop durch einen anpassbaren Anmeldebildschirm ersetzt. Das Design hängt dabei vom ausgewählten Verbindungstyp ab.
(2)	Verbindungsverknüpfungen Doppelklicken Sie auf eine Verbindungsverknüpfung, um eine Verbindung zu starten.
(3)	Taskleiste Ermöglicht schnellen Zugriff auf Programme und Systemfunktionen (weitere Informationen finden Sie unter <a href="#">Taskleiste auf Seite 6</a> ).

# Taskleiste

**HINWEIS:** In der folgenden Abbildung wird die Taskleiste für ThinPro mit einem US-Gebietsschema veranschaulicht. Bei Smart Zero ist die Taskleiste standardmäßig senkrecht und rechtsbündig. Das Anzeigeformat einiger Informationen der Taskleiste unterscheidet sich je nach Gebietsschema.



Symbol	Beschreibung
(1)	Suchen Zum Suchen und Ausführen von konfigurierten Verbindungen, Verbindungs-Managern, Elementen der Systemsteuerung und Energiesparfunktionen.
(2)	Connection Manager In ThinPro wird mit dieser Schaltfläche Connection Manager in einem neuen Fenster geöffnet. Weitere Informationen finden Sie unter <a href="#">Connection Manager (nur ThinPro) auf Seite 7</a> .  In Smart Zero wird mit dieser Schaltfläche ein Menü angezeigt, über das Sie eine Verbindung hinzufügen oder bearbeiten können.
(3)	Systemsteuerung Zum Konfigurieren des Thin Clients, Wechseln zwischen Administratormodus und Benutzermodus und Suchen nach Software-Updates. Weitere Informationen finden Sie unter „ <a href="#">Systemsteuerung</a> “ auf Seite 42.
(4)	Systeminformationen Zum Anzeigen von System-, Netzwerk- und Softwareinformationen zum Thin Client. Weitere Informationen finden Sie unter „ <a href="#">Systeminformationen</a> “ auf Seite 61.
(5)	Anwendungsbereich Zeigt die Symbole für die derzeit geöffneten Anwendungen.  <b>TIPP:</b> Um eine Anwendung auszuwählen und in den Vordergrund zu holen, können Sie <b>Strg+Alt</b> gedrückt halten und dann wiederholt auf die <a href="#">Tabulatortaste</a> drücken.
(6)	Systeminfo Bietet schnellen Zugriff auf Informationen bzw. Informationen zu bestimmten Funktionen und Diensten. Elemente in der Systeminfo können unter anderem folgende sein; einige Elemente werden jedoch möglicherweise abhängig von der Systemkonfiguration nicht angezeigt: <ul style="list-style-type: none"> <li>• Audiomixer</li> <li>• Virtuelle Tastatur</li> <li>• Netzwerkstatus</li> <li>• Automatischer Update-Status – ein grünes Symbol mit einem Häkchen zeigt an, dass die automatische Aktualisierung erfolgreich abgeschlossen. Ein gelbes Symbol mit einem Ausrufezeichen weist darauf hin, dass das automatische Update-Server nicht gefunden wurde oder dass einige Probleme mit den serverseitigen Einstellungen bestehen. Ein rotes Symbol mit einem X weist darauf hin, dass der automatische Update (Automatic Update) fehlgeschlagen ist, wie beispielsweise bei einem ungültigem Paket oder Profil. Ein blaues Symbol mit einem rotierenden Pfeil zeigt an, dass Automatic Update derzeit nach Updates sucht.</li> <li>• Zum Einstellen der Smart Common Input Method (SCIM)</li> <li>• Citrix-Anwendungen</li> </ul>
(7)	Datum und Uhrzeit Zeigt aktuelle Datums- und Uhrzeitangaben an und öffnet Datums- und Uhrzeiteinstellungen.
(8)	Ein/Aus-Taste Zum Abmelden, Neustarten oder Herunterfahren des Thin Clients.

# Connection Manager (nur ThinPro)

 **HINWEIS:** In der folgenden Abbildung wird Connection Manager mit einem US-Gebietsschema veranschaulicht.



Symbol		Beschreibung
(1)	Verbindungsliste	Listet die konfigurierten Verbindungen auf und gibt an, ob eine Verbindung aktiv oder inaktiv ist.
(2)	Start	Startet die ausgewählte Verbindung.
(3)	Stopp	Beendet die ausgewählte Verbindung.
(4)	Bearbeiten	Zum Bearbeiten der ausgewählten Verbindung.
(5)	Löschen	Löscht die ausgewählte Verbindung.
(6)	Hinzufügen	Zum Hinzufügen einer neuen Verbindung. <b>HINWEIS:</b> Siehe <a href="#">Auswählen einer Betriebssystemkonfiguration auf Seite 2</a> für eine Liste der verfügbaren Verbindungstypen.
(7)	Einstellungen	Zum Bearbeiten der allgemeinen Einstellungen für Citrix-, RDP- oder Web Browser-Verbindungen. Diese Einstellungen sind für alle Verbindungen dieses Typs wirksam.

Weitere Informationen über das Konfigurieren von Verbindungen finden Sie unter den folgenden Themen:

- [„Verbindungskonfiguration“ auf Seite 8](#)
- [„Verbindungstypen“ auf Seite 10](#)

# 3 Verbindungskonfiguration

## Erweiterte Verbindungseinstellungen

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer Verbindung mit einem beliebigen Verbindungstyp in der erweiterten Kategorie verfügbar sind.



**HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

Option	Beschreibung
Alternative Verbindung	<p>Spezifiziert die Ausweichverbindung. Wenn die Verbindung nicht gestartet werden kann, wird versucht stattdessen die Ausweichverbindung zu starten.</p> <p><b>HINWEIS:</b> Diese Option ist nicht verfügbar für den Verbindungstyp VMware Horizon View.</p>
Autostart Priorität	<p>Bestimmt die Reihenfolge, in der die Verbindungen automatisch gestartet werden. <b>0</b> bedeutet, dass die Autostartfunktion deaktiviert ist. Die anderen Werte bestimmen die Startreihenfolge, wobei <b>1</b> die höchste Priorität hat.</p>
Anmeldeinformationen mit Bildschirmschoner teilen	<p>Ermöglicht den Benutzern den lokalen Bildschirmschoner zu entsperren, indem sie ihre Anmeldeinformationen für diese Verbindung eingeben.</p> <p><b>HINWEIS:</b> Diese Option ist nur für die Verbindungstypen Citrix, RDP und VMware Horizon View verfügbar.</p>
Automatische Verbindungswiederherstellung	<p>Wenn aktiviert, wird diese Verbindung automatisch versuchen, die Verbindung wiederherzustellen, wenn sie unterbrochen wurde.</p> <p><b>HINWEIS:</b> Das Beenden einer Verbindung über Connection Manager verhindert eine automatische Neuverbindung.</p>
Vor der Anmeldung auf Netzwerkverbindung warten	<p>Deaktivieren Sie diese Option, wenn Ihre Verbindung das Netzwerk zum Starten nicht benötigt, oder wenn Sie nicht auf das Netzwerk zum Starten der Verbindung warten möchten.</p>
Symbol auf Desktop anzeigen	<p>Wenn aktiviert, wird für diese Verbindung ein Desktopsymbol erstellt.</p>
Benutzer gestatten, diese Verbindung zu starten	<p>Wenn aktiviert, kann diese Verbindung von einem Endbenutzer gestartet werden.</p>
Benutzer gestatten, diese Verbindung zu bearbeiten	<p>Wenn aktiviert, kann diese Verbindung von einem Endbenutzer geändert werden.</p>
Anmeldedialogoptionen	<p>Aktivieren Sie oder deaktivieren Sie diese Optionen im Anmeldedialog, um die Verbindung zu konfigurieren.</p> <p><b>HINWEIS:</b> Diese Option ist nur für die Verbindungstypen Citrix, RDP und VMware Horizon View verfügbar.</p> <p>Die folgenden Optionen sind verfügbar:</p> <ul style="list-style-type: none"><li>• <b>Feld „Benutzername“ anzeigen</b></li><li>• <b>Feld „Kennwort“ anzeigen</b></li><li>• <b>Feld „Domäne“ anzeigen</b></li><li>• <b>Kontrollkästchen „SmartCard“ anzeigen</b></li><li>• <b>Kontrollkästchen „Merken“ anzeigen</b></li></ul>

Option	Beschreibung
	<p><b>HINWEIS:</b> Diese Option speichert den Benutzernamen und die Domäne, das Kennwort muss jedoch jedes Mal erneut eingegeben werden.</p> <ul style="list-style-type: none"> <li>• <b>Schaltfläche „Kennwort einblenden“ anzeigen</b></li> </ul>

## Kioskmodus

Wenn ein Thin Client für den Kioskmodus konfiguriert ist, führt er beim Start eine automatische Anmeldung für die Standardverbindung durch, wobei er die vordefinierten Benutzer-Anmeldeinformationen verwendet. Wenn die Verbindung aufgrund einer Abmeldung, Trennung oder eines Netzwerkfehlers abbricht, wird sie automatisch wieder aufgebaut, sobald sie wiederhergestellt werden kann.

 **TIPP:** Der Remote-Host kann so konfiguriert werden, dass er die Ressourcen automatisch bei der Anmeldung startet, sodass der Kioskmodus praktisch nahtlos arbeitet.

Der einfachste Weg, einen Thin Client für den Kioskmodus zu konfigurieren, ist, ihn auf Smart Zero umzuschalten (siehe [Anpassungszentrum auf Seite 51](#)) und eine Verbindung zu konfigurieren. Wenn dies erfolgt ist, werden die folgenden Einstellungen automatisch festgelegt:

- Die Taskleiste wird automatisch ausgeblendet.
- Die Verbindung wird automatisch gestartet.
- Die Verbindung wird automatisch wiederhergestellt.
- Die Verbindung gibt die Benutzeranmeldeinformationen für lokalen Bildschirmschoner frei.
- Das Desktop-Motiv wird auf das Standard-Motiv für diesen Verbindungstyp eingestellt.
- Das USB-Umleitungsprotokoll im USB-Manager wird auf das Protokoll dieses Verbindungstyps festgelegt.

Wenn Sie einen Thin Client in ThinPro für den Kioskmodus konfigurieren möchten (wenn Sie z. B. einen Verbindungstyp verwenden möchten, der nur mit ThinPro verfügbar ist), konfigurieren Sie die folgenden Einstellungen für die gewünschte Verbindung manuell:

- Legen Sie im Anpassungszentrum die Taskleiste auf **Auto hide** (Automatisch ausblenden) fest.
- Führen Sie in den Verbindungseinstellungen folgende Schritte aus:
  - Legen Sie die **Autostart Priorität** auf **1** fest.
  - Aktivieren Sie **Automatische Verbindungswiederherstellung**.
  - Falls verfügbar, aktivieren Sie **Anmeldeinformationen mit Bildschirmschoner teilen**.
  - Wenn Sie nur eine Web Browser-Verbindung herstellen möchten, wählen Sie **Kiosk-Modus aktivieren**.
- Legen Sie bei Bedarf im USB-Manager das richtige USB-Umleitungsprotokoll fest.

 **TIPP:** Um im Kioskmodus die Verbindung zu minimieren und auf den lokalen Desktop zurückzukehren, drücken Sie **Strg+Alt+Ende**.

# 4 Verbindungstypen

## Citrix

In der folgenden Tabelle werden die unterstützten Citrix XenApp-Back-Ends beschrieben.

Zugriffstyp	XenApp-Version
Direct (Vorgängerversion)	4,5/5/6/6.4
PNAgent (Vorgängerversion)	4.5 / 5 / 6 / 6.5 / 7.X
Web Browser	4.5 / 5 / 6 / 6.5 / 7.X
StoreFront	4.5 / 5 / 6 / 6.5 / 7.X

In der folgenden Tabelle werden die unterstützten Citrix XenDesktop®-Back-Ends beschrieben.

Zugriffstyp	XenApp-Version
PNAgent (Vorgängerversion)	4.5 / 5.5 / 5.6.5 / 7.X
Web Browser	4.5 / 5.5 / 5.6.5 / 7.X
StoreFront	4.5 / 5.5 / 5.6.5 / 7.X

In der folgenden Tabelle werden die unterstützten Citrix VDI-in-a-Box-Back-Ends beschrieben.

Zugriffstyp	XenApp-Version
PNAgent (Vorgängerversion)	5.x
Web Browser	5.x
StoreFront	5.x

## Citrix – Allgemeine Einstellungen



**HINWEIS:** Diese Einstellungen haben Auswirkungen auf alle Citrix-Verbindungen.

### Optionen

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten der allgemeinen Citrix-Einstellungen in der Kategorie „Optionen“ (Optionen) verfügbar sind.

Option	Beschreibung
HDX MediaStream aktivieren	Aktiviert HDX MediaStream.
Automatische Neuverbindung aktivieren	Ermöglicht eine automatische Verbindungswiederholung für Verbindungen, die getrennt wurden.

Option	Beschreibung
Sitzungszuverlässigkeit aktivieren	Aktiviert die Funktion für die Citrix-Sitzungszuverlässigkeit. Weitere Informationen finden Sie in der Citrix-Dokumentation.
Zwischenablageumleitung aktivieren	Ermöglicht die Zwischenablageumleitung.
Datenkomprimierung verwenden	Aktiviert die Datenkomprimierung für diese Verbindung.
H264-Komprimierung aktivieren	Aktiviert die H.264-Komprimierung. Schauen Sie in der Citrix-Dokumentation nach, um festzustellen, ob diese Methode der Datenkomprimierung am besten für Ihren Anwendungsfall geeignet ist.
Einfügen mit mittlerer Taste aktivieren	Aktiviert die Einfügefunktion der mittleren Maustaste.
Benutzer-Agent-Zeichenfolge	Geben Sie eine Benutzer-Agent-Zeichenfolge ein, die für das Senden von Anforderungen an den Citrix-Server verwendet wird. Diese Option ist für NetScaler-Konfigurationen nützlich.
HDX Flash-Umleitung	Aktiviert die HDX Flash-Umleitung, um Flash-Inhalte lokal abzuspielen.
Serverseitiges Abrufen der HDX Flash-Inhalte	Ermöglicht dem Server, die Flash-Inhalte zur Umleitung einzuholen.
Audio	Legt die Audioqualität fest oder deaktiviert den Sound vollständig.
Verschlüsselungsebene	Gibt die Verschlüsselungsstufe einer ICA-Sitzung an.

## Local Resources (Lokale Ressourcen)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten der allgemeinen Citrix-Einstellungen in der Kategorie „Local Resources“ (Lokale Ressourcen) verfügbar sind.

Option	Beschreibung
Drucker	Steuert, wie die lokale Druckerumleitung behandelt wird.
Webcam/Audio-Input (Webcam/Audio-Eingang)	Steuert, wie die Umleitung der lokalen Webcam und des Audioeingangs behandelt wird.
USB-Umleitung	Ermöglicht die USB-Umleitung.
Dynamische Laufwerkszuordnung	Aktiviert die dynamische Laufwerkszuordnung.
Statische Laufwerkszuordnung (Vorgängerversion)	Aktiviert die statische Laufwerkszuordnung, sodass Sie Laufwerkszuordnungen zu lokalen Pfaden angeben können.

## Window (Fenster)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten der allgemeinen Citrix-Einstellungen in der Kategorie „Window“ (Fenster) verfügbar sind.

Option	Beschreibung
TWI-Modus	Ermöglicht die Anzeige eines einzigen nahtlosen Fensters auf dem lokalen ThinPro-Desktop, als ob es eine systemeigene Anwendung wäre.
Standard-fenstergröße	Wenn <b>TWI Mode</b> (TWI-Modus) auf <b>Force Seamless Off</b> (Nahtlos erzwingen - Aus) eingestellt ist, wird damit die Standard-Fenstergröße gesteuert.
Standard-Fensterfarben	Legt die Standard-Farbtiefe fest.

Option	Beschreibung
Virtuellen Desktop auf allen Monitoren anzeigen	Wenn die Option aktiviert ist, wird der virtuelle Desktop auf allen Monitoren angezeigt.
Linker Monitor	Wenn <b>Show the Virtual Desktop on all monitors</b> (Virtuellen Desktop auf allen Monitoren anzeigen) deaktiviert ist, können Sie mit diesen Feldern angeben, wie der virtuelle Desktop auf bestimmten Monitoren angezeigt wird.
Rechter Monitor	
Oberer Monitor	
Unterer Monitor	

## Firewall

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten der allgemeinen Citrix-Einstellungen in der Kategorie „Firewall“ verfügbar sind.

Option	Beschreibung
Proxy-Typ	Gibt den Proxy-Typ an.
Proxy-Adresse	Die IP-Adresse des Proxy-Servers.
Proxy-Port	Der Port für die Verbindung zum Proxy-Server.
Benutzername	Der Benutzername für die Verbindung zum Proxy-Server.
Kennwort	Das Kennwort für die Verbindung zum Proxy-Server.
Alternative Adresse für Firewall-Verbindung verwenden	Der Citrix ICA-Client fordert eine alternative, für den Server definierte Adresse an, wenn Verbindungen zu Servern innerhalb der Firewall hergestellt werden. Für jeden Server in einer Serverfarm muss eine alternative Adresse angegeben werden.

## Keyboard Shortcuts (Tastenkombinationen)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten der allgemeinen Citrix-Einstellungen in der Kategorie „Keyboard Shortcuts“ (Tastenkombinationen) verfügbar sind.

Option	Beschreibung
UseLocalIM aktivieren	Verwendet die lokale Eingabemethode, um die Tastatureingabe zu interpretieren. Dies wird nur für europäische Sprachen unterstützt.
EUKS-Nummer verwenden	Regelt die Verwendung von Extended Unicode Keyboard Support (EUKS, Erweiterte Unicode-Tastaturunterstützung) auf Windows Servern. Gültige Optionen werden nachfolgend beschrieben: <ul style="list-style-type: none"> <li>• 0 – EUKS wird nicht verwendet.</li> <li>• 1 – EUKS wird als Ausweichoption verwendet.</li> <li>• 2 – EUKS wird möglichst immer verwendet.</li> </ul>
Verwendung von Tastaturkurzbefehlen	Gibt an, wie Tastenkombinationen verarbeitet werden sollen. Die folgenden Einstellungen sind verfügbar: <ul style="list-style-type: none"> <li>• <b>Translated (Übersetzt)</b> – Tastenkombinationen gelten für den lokalen Desktop (Client)</li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>• <b>Direct in full screen desktops only (Direkt nur bei Vollbild-Desktops)</b> – Tastenkombinationen gelten für den Remotedesktop (Server), aber nur für eine nicht nahtlose ICA-Sitzung im Vollbildmodus</li> <li>• <b>Direct (Direkt)</b> – Tastenkombinationen gelten für den Remotedesktop (Server) für nahtlose und nicht nahtlose ICA-Sitzungen, wenn ihre Fenster den Tastaturfokus haben.</li> </ul>
Verwendung von Direktaufruftasten stoppen	Gibt die Tastenkombination an, die die direkte Verarbeitung der Tastenkombinationen deaktiviert.
Alt + F1 ... Alt + F12	Zum Hinzufügen von zu verarbeitenden Tastenkombinationen.

## Session (Sitzung)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten der allgemeinen Citrix-Einstellungen in der Kategorie „Session“ (Sitzung) verfügbar sind.

Option	Beschreibung
Automatische Abmeldungsverzögerung vor Anwendungsstart	Wenn Sie einen Citrix-Server mit mehreren veröffentlichten Ressourcen verwenden, wird mit dieser Option die Anzahl der Sekunden festgelegt, die einem Benutzer zur Verfügung stehen, um eine Anwendung nach der Anmeldung zu starten, bevor das System automatisch eine Abmeldung durchführt und zum Anmeldebildschirm zurückkehrt.
Automatische Abmeldungsverzögerung nach Schließen einer Anwendung	Wenn Sie einen Citrix-Server mit mehreren veröffentlichten Ressourcen verwenden, wird mit dieser Option die Anzahl der Sekunden festgelegt, die zur Verfügung stehen zwischen dem Schließen der letzten von Xen veröffentlichten Ressource und dem automatischen Abmelden des Benutzers und Zurückkehren zum Anmeldebildschirm.
Server-Test-Timeout	Zur Durchführung einer grundlegenden Konnektivitätsprüfung am ausgewählten Server und Port, legen Sie diese Option auf einen Wert fest, der nicht dem Standardwert <b>-1</b> entspricht.

**TIPP:** Durch Einstellen eines dieser Werte auf weniger als 0 wird die automatische Abmeldung deaktiviert.

**HINWEIS:** Verzögerungen bei Citrix-Verarbeitungsprozessen können die Zeit bis zur automatischen Abmeldung verlängern.

## Citrix-Einstellungen pro Verbindung



**HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

## Connection (Verbindung)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer Citrix-Verbindung in der Kategorie „Connection“ (Verbindung) verfügbar sind.

Option	Beschreibung
Name	Der Verbindungsname.
Verbindungsmodus	Legt den Verbindungsmodus auf eine der folgenden Optionen fest: <ul style="list-style-type: none"> <li>• <b>PNAgent</b></li> <li>• <b>StoreFront</b></li> </ul>

Option	Beschreibung
	<ul style="list-style-type: none"> <li>• <b>Direct</b></li> </ul> <p><b>HINWEIS:</b> Authentifizierungsoptionen werden nach dieser Option angezeigt und hängen vom ausgewählten Verbindungsmodus ab. Weitere Informationen finden Sie in der Citrix-Dokumentation.</p> <p><b>HINWEIS:</b> Sie können die Verbindungseinstellungen testen, indem Sie die Schaltfläche <b>Verbindung testen</b> auswählen.</p>
URL	<p>Der Citrix Server-Hostname oder die IP-Adresse. Wenn Sie eine Verbindung zu einem Server auf einer HTTPS-Website konfigurieren, geben Sie den FQDN des Standorts und das lokale Stammzertifikat im Citrix-Zertifikatsspeicher ein.</p> <p>Ist das Kontrollkästchen neben dieser Option aktiviert, wird eine HTTPS-Verbindung erzwungen.</p>

## Configuration (Konfiguration)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer Citrix-Verbindung in der Kategorie „Configuration“ (Konfiguration) verfügbar sind.

Option	Beschreibung
Anwendungen bei Anmeldung automatisch erneut verbinden	<p>Wenn diese Option ausgewählt ist, werden Ressourcen, die geöffnet waren, als sich der Benutzer zuletzt abgemeldet hat, wieder geöffnet, wenn er sich erneut anmeldet.</p> <p><b>TIPP:</b> Wenn Sie die Citrix SmoothRoaming-Funktion nicht verwenden, deaktivieren Sie diese Option, um Ihre Verbindungsgeschwindigkeit zu erhöhen.</p>
Modus für automatisches Starten	<p>Zum Festlegen einer bestimmten Anwendung oder eines Desktops, die bzw. der mit Beginn der Citrix-Verbindung automatisch gestartet wird. Wenn die Option auf <b>Eine Ressource automatisch starten</b> festgelegt ist und nur eine veröffentlichte Ressource vorhanden ist, wird diese Ressource automatisch gestartet.</p> <p><b>HINWEIS:</b> Diese Option hat keine Auswirkungen, wenn <b>Anwendungen bei Anmeldung automatisch erneut verbinden</b> ausgewählt ist und entsprechende Anwendungen vorhanden sind.</p> <p>Wenn Sie das automatische Starten einer Anwendung oder eines Desktops ausgewählt haben, wählen Sie die Schaltfläche <b>Enumeration</b>, um eine Liste der Ressourcen (Anwendungen oder Desktops) abzurufen und in Citrix Connection Manager anzuzeigen. So können Sie die Ressourcen auswählen, die beim Herstellen einer Verbindung automatisch gestartet werden.</p> <p>Wenn Sie das automatische Starten einer Ressource ausgewählt haben, wählen Sie die Schaltfläche <b>Enumeration</b>, um die Anzahl der Ressourcen abzurufen. Wenn nur eine Ressource vorhanden ist, wird sie beim Herstellen der Verbindung automatisch gestartet.</p>
Ressourcen auf Desktop anzeigen	<p>Wenn diese Option ausgewählt ist, werden Remoteressourcen der Verbindung auf dem lokalen ThinPro-Desktop angezeigt.</p>
Ressourcen auf der Taskleiste anzeigen	<p>Wenn diese Option ausgewählt ist, werden Remoteressourcen der Verbindung auf der lokalen ThinPro-Taskleiste angezeigt.</p>
Nur abonnierte Ressourcen anzeigen	<p>Wenn diese Option ausgewählt ist, werden während einer Citrix-Verbindung nur abonnierte Ressourcen angezeigt.</p>

## Advanced (Erweitert)



**HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

## HP True Graphics

Mit HP True Graphics werden umfangreiche Multimedia-Inhalte an die GPU ausgelagert, um Bilder mit hoher Frequenz darzustellen und die Effizienz zu steigern.

HP True Graphics erfordert eine der folgenden Citrix-Umgebungen:

- Citrix XenApp/XenDesktop 7 oder neuer
- Citrix HDX 3D Pro (nicht im Modus **Always Lossless** (Immer verlustfrei))

## Serverseitige Anforderungen für HP True Graphics

### XenApp/XenDesktop

Der Citrix-Server muss das Senden von Sitzungsdaten im Format H.264 unterstützen. H.264 ist standardmäßig aktiviert und wird mit dem DeepCompressionV2-Encoder verarbeitet, einem CPU-basierten Komprimierungsalgorithmus.

Nur vollständige Desktops oder nicht nahtlos arbeitende Anwendungen werden derzeit beschleunigt, wenn HP True Graphics verwendet wird. Remoteanwendungen, die in einem nahtlosen Fenster ausgeführt werden, profitieren von HP True Graphics nicht. Informationen, wie Sie erzwingen, dass Anwendungen nicht nahtlos ausgeführt werden, indem Sie die Einstellung **TWI-Modus** auf dem Thin Client konfigurieren, finden Sie unter [Clientseitige Konfiguration von HP True Graphics auf Seite 16](#).

### HDX 3D Pro

HDX 3D Pro-Desktop-PCs können das Format H.264 verwenden und von der Verwendung von HP True Graphics profitieren, selbst wenn sie ältere Versionen von XenDesktop ausführen. Sie könnten HDX 3D Pro verwenden, um die serverseitige H.264-Codierung über den DeepCompression-Encoder in die GPU auszulagern. Weitere Informationen finden Sie in der Citrix-Dokumentation.



**HINWEIS:** HP True Graphics bietet keine Leistungsverbesserungen, wenn HDX 3D Pro verwendet wird und die visuelle Qualität auf **Immer verlustfrei** festgelegt ist, da dann die grafischen Informationen nicht im Format H.264 an den Thin Client gesendet werden.

## Überprüfen der Serveroptionen für die Komprimierung

Verwenden Sie nach dem Herstellen einer Verbindung mit einem Citrix-Desktop den Citrix HDX Monitor, um zu bestimmen, welcher Encoder für die Sitzung verwendet wird, indem Sie die Informationen unter **Grafik > Thinwire erweitert > Komponentenencoder** prüfen. Wenn der Wert **DeepCompressionV2Encoder** oder **DeepCompressionEncoder** lautet, sendet der Server ordnungsgemäß die Daten in einem Format, das von HP True Graphics beschleunigt wird.



**HINWEIS:** Wenn betriebssystemunabhängige Grafiken über eine Serverrichtlinie wie CompatibilityEncoder oder LegacyEncoder erzwungen werden, komprimiert der Server Grafiken mit einer Methode, die mit älteren Versionen von Citrix-Clients kompatibel ist, und Sie werden keine Leistungsverbesserungen durch HP True Graphics feststellen.

## Clientseitige Konfiguration von HP True Graphics

### Komprimierungseinstellungen

H.264-Komprimierung muss auf dem Thin Client aktiviert sein, damit HP True Graphics Vorteile bietet. Um die H.264-Komprimierung auf dem Thin Client zu aktivieren, aktivieren Sie das Kontrollkästchen **H264-Komprimierung aktivieren** in Xen Connection General Settings Manager.

Einige Bildschirmdaten wie Text werden möglicherweise mit anderen Methoden als H.264 gesendet. Im Allgemeinen sollte diese Funktion aktiviert bleiben, aber für die Fehlerbeseitigung oder für bestimmte Anwendungsfälle können die folgenden Registrierungsschlüssel auf **0** eingestellt werden, um diese Funktion zu deaktivieren:

- `root/ConnectionType/xen/general/enableTextTracking`
- `root/ConnectionType/xen/general/enableSmallFrames`

### Fenstereinstellungen

Für Remoteanwendungen im nahtlosen Modus bietet HP True Graphics keine Vorteile. Um für Remoteanwendungen den Fenstermodus zu erzwingen, legen Sie in Xen Connection General Settings Manager die Option **TWI-Mode** auf **Seamless erzwingen Aus** fest.

### Monitorlayout- und Hardwarebeschränkungen

Beachten Sie die folgenden Beschränkungen für das Monitorlayout:

- Die meisten Konfigurationen mit maximal zwei Monitoren mit einer Auflösung von jeweils 1920 × 1200 werden unterstützt.
- HP t420 Thin Client: Durch die Standard-BIOS-Konfiguration verwendet dieses Produkt HP True Graphics standardmäßig nur für einen Monitor. Weitere Informationen finden Sie unter [Aktivieren von HP True Graphics für mehrere Monitore auf dem HP t420 auf Seite 16](#).
- HP t730 Thin Client: Dieses Modell unterstützt maximal drei Monitore mit einer Auflösung von 1920 × 1200.
- Gedrehte Monitore werden möglicherweise nicht korrekt angezeigt.

### Aktivieren von HP True Graphics für mehrere Monitore auf dem HP t420

So aktivieren Sie HP True Graphics für mehrere Monitore auf dem HP t420:

1. Starten Sie den Thin Client neu und drücken Sie **F10**, um auf das BIOS zuzugreifen.
2. Navigieren Sie zu **Advanced > Integrated Graphics** (Erweitert > Integrierte Grafik).
3. Legen Sie **Integrated Graphics** (Integrierte Grafik) auf **Force** (Erzwingen) fest.
4. Legen Sie **UMA Frame Buffer Size** (Größe des UMA-Frame-Puffers) auf **512M** fest.

Nachdem Sie diese Schritte durchgeführt haben, wird die für Grafiken verfügbare Größe des Arbeitsspeichers erweitert und HP True Graphics kann für zwei Monitore verwendet werden.

---

 **TIPP:** Diese Einstellungen können auch über HPDM oder über die BIOS-Tools konfiguriert werden, die in HP ThinPro enthalten sind (weitere Informationen finden Sie unter [BIOS-Tool für Einstellungen auf Seite 77](#)).

---

# RDP

Der RDP-Client basiert auf FreeRDP 1.1 und erfüllt die folgenden Anforderungen für RDP:

- Hardware-beschleunigtes RemoteFX
- MMR wird beim Herstellen einer Verbindung mit Windows Hosts unterstützt, wenn die Funktion für die Desktopdarstellung aktiviert ist
- USBR wird beim Herstellen einer Verbindung mit RDP-Servern unterstützt, die dies aktivieren

## RDP – Allgemeine Einstellungen

In der folgenden Tabelle werden die allgemeinen RDP-Einstellungen beschrieben.



**HINWEIS:** Diese Einstellungen haben Auswirkungen auf alle RDP-Verbindungen.

Option	Beschreibung
Hostname senden als	Gibt an, ob der Hostname oder die MAC-Adresse des Thin Client als der angegebene Hostname an das Remotesystem gesendet werden soll.
Multimedia-Umleitung aktivieren	Aktiviert die Multimedia-Umleitung.

## RDP-Einstellungen pro Verbindung



**HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

## Netzwerk

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer RDP-Verbindung in der Kategorie „Netzwerk“ verfügbar sind.

Option	Beschreibung
Name	Ein benutzerdefinierter Name für diese Verbindung.
Adresse	Die IP-Adresse oder der Servername für diese Verbindung oder die URL des RD Web Access-Feeds. Falls erforderlich, kann der Port nach einem Doppelpunkt an den Server angehängt werden (standardmäßig ist der Port für eine direkte RDP-Verbindung 3389). <b>HINWEIS:</b> Die URL des RD Web Access-Feeds muss mit <code>https://</code> beginnen. Standardmäßig wird dies automatisch hinzugefügt, gemäß den Angaben im Registrierungsschlüssel <code>rdWebFeedUrlPattern</code> , der das Muster der URL definiert.
Benutzername	Der Benutzername für diese Verbindung.
Kennwort	Das Kennwort für diese Verbindung.
Domäne	Der Domänenname für diese Verbindung (optional).
Smart Card-Anmeldung zulassen	Ermöglicht die Smart Card-Authentifizierung.
RD-Gateway aktivieren	Ermöglicht zusätzliche RD-Gateway-Optionen, wie Gateway-Adresse, -Port und -Anmeldeinformationen).
Servertest	Startet den Servertest, der verwendet werden kann, um festzustellen, welche RDP-Funktionen von Ihrem RDP-Server unterstützt werden.

## Dienst

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer RDP-Verbindung in der Kategorie „Dienst“ verfügbar sind.

Option	Beschreibung
Dienst	<p>Legt den RDP-Dienst auf eine der folgenden Optionen fest:</p> <ul style="list-style-type: none"><li>• <b>Remotecomputer</b> – Wenn dieser Dienst verwendet wird, wird eine direkte RDP-Verbindung mit einem Remotecomputer erstellt. Eine Remoteanwendung oder eine andere Shell kann optional beim Herstellen einer Verbindung gestartet werden. Die folgenden zusätzlichen Optionen stehen für einen Remotecomputerdienst zur Verfügung:<ul style="list-style-type: none"><li>– Wenn <b>Modus auf Remoteanwendung</b> festgelegt ist, ist im Feld <b>Anwendung</b> der Pfad der auszuführenden Anwendung angegeben.<p><b>TIPP:</b> Wenn Sie den Modus „RDP Seamless Windows“ (RDP Nahtlose Fenster) verwenden, geben Sie den Pfad der <code>seamlessrdpshell.exe</code> auf Ihrem Server ein, gefolgt von einem Leerzeichen und anschließend den Pfad, auf dem die Anwendung ausgeführt wird. Siehe folgendes Beispiel:</p><pre>c:\seamless\seamlessrdpshell.exe c:\Program Files \Microsoft\Word.exe</pre></li><li>– Wenn <b>Modus auf Andere Shell</b> festgelegt ist, ist im Feld <b>Befehl</b> der Befehl angegeben, der die Anwendung ausführt, die in der anderen Shell ausgeführt werden soll. Um Microsoft® Word auszuführen, geben Sie z. B. <code>Word.exe</code> ein.<p>Wenn <b>Modus auf Andere Shell</b> festgelegt ist, gibt das Feld <b>Verzeichnis</b> den Pfad des Arbeitsverzeichnisses des Servers für Programmdateien der Anwendung an. Beispiel: Das Arbeitsverzeichnis für Microsoft Word ist <code>C:\Program Files\Microsoft.</code></p></li></ul></li><li>• <b>RD Web Access</b> – Wenn dieser Dienst verwendet wird, wird eine Liste von RemoteApp-Ressourcen vom Server abgerufen und für den Benutzer angezeigt. Die eigentliche RDP-Verbindung wird gestartet, wenn eine Ressource ausgewählt wurde. Die folgenden zusätzlichen Optionen sind für RD Web Access verfügbar:<ul style="list-style-type: none"><li>– <b>Fenster für die Ressourcenauswahl nicht schließen</b> – Wenn diese Option ausgewählt ist, können Benutzer mehrere Ressourcen gleichzeitig im Ressourcenauswahlfenster öffnen.</li><li>– <b>Eine Ressource automatisch starten</b> – Wenn diese Option ausgewählt ist und nur eine veröffentlichte Ressource vorhanden ist, startet diese Ressource beim Herstellen einer Verbindung automatisch.</li><li>– <b>Ressourcenfilter und Browser für Web-Feeds</b> – Diese Optionen können verwendet werden, um die Remoteressourcen zu beschränken, die dem Benutzer im Ressourcenauswahlfenster zur Verfügung gestellt werden.<p><b>HINWEIS:</b> Ein Vorteil der Verwendung von RD Web Access ist, dass damit die Details der vermittelten Verbindungen und die Lastenausgleichs-URL automatisch verarbeitet werden.</p></li></ul></li></ul> <p>Weitere Informationen finden Sie im HP ThinPro-Whitepaper <i>RD Web Access Deployment Example</i> (nur auf Englisch verfügbar).</p>

## Fenster

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer RDP-Verbindung in der Kategorie „Window“ (Fenster) verfügbar sind.

Option	Beschreibung
Fensterdekoration ausblenden	Mit dieser Einstellung wird sichergestellt, dass Bildelemente, wie z. B. die Menüleiste, die Minimierungs- und Schließ-Optionen sowie die Ränder von Fensterbereichen nicht angezeigt werden.
Fenstergröße	Legt die Fenstergröße auf <b>full</b> (voll), <b>fixed</b> (fest) oder <b>percent</b> (prozentual) fest.
Größe (Prozent)	Wenn <b>Window Size</b> (Fenstergröße) auf <b>percent</b> (prozentual) eingestellt ist, legt diese Option den Prozentsatz fest, den ein Desktopfenster auf dem Bildschirm einnimmt. <b>HINWEIS:</b> Die daraus resultierenden Größen können gerundet werden. <b>HINWEIS:</b> RemoteFX unterstützt nur eine feste Liste von Auflösungen.
Feste Größe	Wenn <b>Window Size</b> (Fenstergröße) auf <b>fixed</b> (fest) eingestellt ist, legt diese Option die Breite und Höhe, die das Desktopfenster einnimmt, in Pixeln fest.

## Optionen

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer RDP-Verbindung in der Kategorie „Optionen“ verfügbar sind.

Option	Beschreibung
Bewegungsereignisse aktivieren	Wenn aktiviert, werden die Mausbewegungen beständig an den RDP-Server übermittelt.
Datenkomprimierung aktivieren	Ermöglicht die Massenkompromierung von Daten zwischen dem RDP-Server und dem RDP-Client.
Veraltete RDP-Verschlüsselung aktivieren	Aktiviert die RDP-Verschlüsselung der letzten Generation, wenn NLA nicht verfügbar ist.
Nicht sichtbaren Cache aktivieren	Wenn aktiviert, wird der Offscreen-Speicher verwendet, um Bitmaps zu cachen.
An Administratorkonsole anheften	Fügt die Verbindung zum Administrator-Konsolenanschluss hinzu.
Sitzungsübergreifendes Kopieren/Einfügen	Wenn aktiviert, ist das Kopieren und Einfügen zwischen verschiedenen RDP-Sitzungen möglich.
Pufferung von RDP6-Grundtypen aktivieren	Wenn diese Option aktiviert ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
Progressive RemoteFX Codec aktivieren	Aktiviert den progressiven RemoteFX-Codec, mit dem der Desktop in einer Reihe immer schärferer Bilder übertragen wird. <b>HINWEIS:</b> Dieser Codec kann auf Desktops mit sehr dynamischem Inhalt zu visuellen Artefakten führen. Er kann also bei Bedarf deaktiviert werden.
Richtlinie zur Zertifikatsüberprüfung	Führen Sie eine der folgenden Aktionen aus: <ul style="list-style-type: none"> <li>• <b>Akzeptieren Sie alle RDP-Server-Zertifikate</b></li> <li>• <b>Verwenden beibehaltener Hosts; Bei unbekanntem oder ungültigen Zertifikaten warnen</b></li> <li>• <b>Überspringen beibehaltener Hosts; Bei unbekanntem oder ungültigen Zertifikaten warnen</b></li> <li>• <b>Nur mit vorab genehmigten RDP-Servern verbinden</b></li> </ul>
TLS-Version	Legt die Transport Layer Security-Version fest, die in den Anfangsphasen der Aushandlung mit dem RDP-Server verwendet wird. Legen Sie diese Option auf die TLS-Version Ihres RDP-Servers fest oder verwenden Sie <b>auto</b> .

Option	Beschreibung
	<b>HINWEIS:</b> Durch einige Serverfehler auf einigen ungepatchten RDP-Servern kann die automatische Einstellung zu einem Fehler führen, deshalb ist es nicht die Standardeinstellung.
Zu sendender Hostname	Normalerweise wird der Thin Client-Hostname für Client-Zugriffslizenzen verwendet. Dieses Feld erlaubt das Senden eines anderen Werts.  <b>TIPP:</b> Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.
Lastenausgleichsinfo	Verwenden Sie diese Option mit einer vermittelten RDP-Verbindung.  <b>TIPP:</b> Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.

 **HINWEIS:** Weitere Informationen zu den Optionen **Veraltete RDP-Verschlüsselung aktivieren** und **TLS-Version** finden Sie im HP ThinPro-Whitepaper *Security Layers for RDP Connections* (nur auf Englisch verfügbar).

## Lokale Ressourcen

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer RDP-Verbindung in der Kategorie Lokale Ressourcen verfügbar sind.

 **HINWEIS:** HP empfiehlt für lokale Geräte eine High-Level-Geräteumleitung, wenn es keinen Grund gibt, stattdessen die USB-Umleitung (USBR) zu verwenden. Weitere Informationen finden Sie im HP ThinPro-Whitepaper *USB Manager* (nur auf Englisch verfügbar).

Option	Beschreibung
Audiogeräte	Gibt an, ob die Audiogeräte über High-Level RDP-Audiumleitung oder Low-Level USB-Umleitung umgeleitet werden oder für diese Verbindung deaktiviert sind.
Drucker	Gibt an, ob die Drucker über eine High-Level Druckerumleitung (für die eine Einrichtung über das Drucker-Tool in der Systemsteuerung erforderlich ist) oder über eine Low-Level-USB-Umleitung umgeleitet werden oder für diese Verbindung deaktiviert sind.
Serielle/parallele Ports	Gibt an, ob die seriellen und parallelen Ports umgeleitet werden oder für diese Verbindung deaktiviert sind.
USB-Speicher	Gibt an, ob USB-Speichergeräte, wie z. B. Flash-Laufwerke und optische Laufwerke, von High-Level Storage-Umleitung oder Low-Level USB-Umleitung umgeleitet werden oder für diese Verbindung deaktiviert sind.
Lokale Partitionen	Gibt an, ob lokale Partitionen des Thin Client Flash-Laufwerks umgeleitet werden oder für diese Verbindung deaktiviert sind.
Andere USB-Geräte	Gibt an, ob andere Klassen von USB-Geräten (wie z. B. Webcams und Tablets) über eine Low-Level USB-Umleitung umgeleitet werden oder für diese Verbindung deaktiviert sind.

## Experience (Darstellung)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer RDP-Verbindung in der Kategorie „Experience“ (Darstellung) verfügbar sind.

Option	Beschreibung
Auswahl der Verbindungsgeschwindigkeit zur Optimierung der Leistung	<p>Das Auswählen einer Verbindungsgeschwindigkeit (<b>LAN, Broadband</b> (Breitband) oder <b>Modem</b>) wird die folgenden Optionen aktivieren oder deaktivieren, um die Leistung zu optimieren:</p> <ul style="list-style-type: none"> <li>• <b>Desktop background</b> (Desktop-Hintergrund)</li> <li>• <b>Font smoothing</b> (Schriftglättung)</li> <li>• <b>Desktop composition</b> (Desktopgestaltung)</li> <li>• <b>Show contents of window while dragging</b> (Inhalte des Fensters beim Verschieben anzeigen)</li> <li>• <b>Menu and window animation</b> (Menü- und Fensteranimation)</li> <li>• <b>Themes</b> (Designs)</li> </ul> <p>Die Auswahl von <b>Client Preferred Settings</b> (Vom Client bevorzugte Einstellungen) ermöglicht dem RDP-Client die Auswahl der Optionen, die zur besten RDP-Erfahrung führen.</p> <p>Sie können auch Ihre eigene benutzerdefinierte Kombination von Optionen auswählen.</p>
Ende-zu-Ende Verbindungs-Health-Überwachung	<p>Dient zum Aktivieren der Timeout-Optionen.</p> <p><b>HINWEIS:</b> Weitere Informationen finden Sie im HP ThinPro-Whitepaper <i>RDP Connection Drop Detection</i> (nur auf Englisch verfügbar).</p>
Zeitlimit bei Warnung	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, bevor der Benutzer eine Warnung zur abgebrochenen Verbindung erhält. Diese Funktion kann deaktiviert werden, indem Sie die Option löschen oder die Zeit auf Null setzen.</p> <p>Wenn die Option <b>Show Warning Dialog</b> (Dialogfeld mit Warnung anzeigen) ausgewählt ist, wird ein Warnungsdialogfeld angezeigt, wenn dieses Zeitlimit erreicht ist. Andernfalls wird die Warnung nur in das Verbindungsprotokoll geschrieben.</p> <p><b>TIPP:</b> HP empfiehlt, den Wert des Zeitlimits für Netzwerke, die regelmäßig hoch belastet oder zeitweise überlastet sind bzw. ausfallen, zu erhöhen.</p>
Zeitlimit bei Wiederherstellung	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client auf die Wiederherstellung der Verbindung wartet, bevor eine bestimmte Maßnahme eingeleitet wird. Am Ende dieser Frist versucht der RDP-Client kurz, erneut eine Verbindung mit der Sitzung aufzubauen.</p>
Zeitlimit bei Fehler	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client wartet, bevor er aufhört zu versuchen, die Verbindung mit diesem Server wiederherzustellen.</p> <p><b>TIPP:</b> Wählen Sie das Symbol ? neben diesem Feld, um weitere Informationen zu erhalten.</p>

## Diagnostics (Diagnose)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer RDP-Verbindung in der Kategorie „Diagnostics“ (Diagnose) verfügbar sind.

Option	Beschreibung
RDP-Dashboard anzeigen	<p>Wenn diese Option aktiviert ist, wird das RDP-Dashboard während der Verbindung angezeigt.</p> <p><b>TIPP:</b> Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.</p>
Diagramm zum Verbindungszustand anzeigen	<p>Wenn diese Option aktiviert ist, wird ein zweidimensionales Diagramm der Antwortzeit vom RDP-Server angezeigt, wenn die Verbindung gestartet wird.</p>

Option	Beschreibung
	<b>TIPP:</b> Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.
Analyse der USB-Umleitungen	Diese Funktion bestimmt und zeigt die aktuelle Umleitungsmethode für jedes umgeleitete USB-Gerät.  <b>TIPP:</b> Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.
Synchrones X11	Erzwingt das häufige Übertragen von X11-Puffern zulasten der Leistung.
Protokollierung	Aktiviert die X11-Protokolldatei. Wählen Sie die Option <b>Automatische Leerung</b> , um die Häufigkeit von Protokollausgaben zulasten der Leistung zu erhöhen.
Aufzeichnen	Ermöglicht die Aufzeichnung und Wiedergabe von X11-Ausgaben einer Sitzung.

## Erweitert



**HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

## RemoteFX

RemoteFX ist ein erweitertes Grafikanzeigeprotokoll, das dafür vorgesehen ist, die Grafikkomponente herkömmlicher RDP-Protokolle zu ersetzen. Es verwendet die Funktionen zur Hardwarebeschleunigung der Server-GPU, um Bildschirminhalte über den RemoteFX-Codec zu codieren und Bildschirmaktualisierungen an den RDP-Client zu senden. RemoteFX verwendet erweiterte Pipelining-Technologien und adaptive Grafiken, um sicherzustellen, dass basierend auf dem Inhaltstyp, der CPU, der Verfügbarkeit der Netzwerkbandbreite und der Darstellungsgeschwindigkeit die bestmögliche Erfahrung ermöglicht wird.

RemoteFX ist standardmäßig aktiviert. Der Administrator oder Benutzer muss keine Änderungen an den Einstellungen vornehmen, um es zu aktivieren. Der RDP-Client verhandelt mit jedem RDP-Server, den er kontaktiert, und wenn RemoteFX verfügbar ist, wird es verwendet.

Um RemoteFX zu deaktivieren, setzen Sie den folgenden Registrierungsschlüsselwert auf 0:

```
root/ConnectionType/freerdp/connections/<UUID>/remoteFx
```



**TIPP:** Für eine vereinfachte Verwaltung empfiehlt HP, dass Sie RemoteFX auf dem Remote-Host aktivieren oder deaktivieren.



**HINWEIS:** Weitere Informationen finden Sie im HP ThinPro-Whitepaper *Enabling RemoteFX for RDP* (nur auf Englisch verfügbar).

## RDP-Sitzungen mit mehreren Monitoren

Eine True-Multi-Monitor-Unterstützung benötigt keine spezielle Konfiguration. Der RDP-Client identifiziert automatisch, welcher Monitor als primärer Monitor in den lokalen Einstellungen angegeben ist, und platziert die Taskleiste und die Desktop-Symbole auf diesem Monitor. Wenn ein Fenster innerhalb der Remote-Sitzung maximiert wird, wird das Fenster nur den Monitor abdecken, auf dem es maximiert wurde.

Die Bildschirmeinstellungen und Monitorauflösungen können angezeigt, aber nicht innerhalb der Remote-Sitzung geändert werden. Um die Sitzungsauflösung zu ändern, melden Sie sich von der Sitzung ab und ändern Sie die Auflösung auf dem lokalen Thin Client.

Standardmäßig sind alle RDP-Sitzungen Vollbildsitzungen und decken alle Monitore ab, um die Virtualisierungserfahrung zu verbessern. Zusätzliche Fensteroptionen stehen in RDP Connection Manager zur Verfügung.

---

 **HINWEIS:** Remote Desktop Virtualization Host (RDVH)-Sitzungen mit Grafikkarten-Unterstützung unterstützen möglicherweise nur bestimmte Auflösungen und eine bestimmte Anzahl an Monitoren. Die Grenzwerte werden angegeben, wenn das RemoteFX virtuelle Grafikerät für die RDVH virtuelle Maschine konfiguriert wird.

 **HINWEIS:** Weitere Informationen zu RDP-Sitzungen mit mehreren Monitoren finden Sie im HP ThinPro-Whitepaper *True Multi-Monitor Mode for RDP* (nur auf Englisch verfügbar).

---

## RDP-Multimedia-Umleitung

Die Multimedia-Umleitung (MMR, Multimedia Redirection) ist eine Technologie, die mit dem Windows Media Player auf dem Remote-Host integriert ist und die die codierten Medien zum RDP-Client streamt, anstatt sie auf dem Remote-Host abzuspielen und über RDP neu zu codieren. Diese Technologie reduziert die Serverlast und den Netzwerk-Datenverkehr und verbessert die Multimedia-Erfahrung erheblich, da sie eine 24 fps-Wiedergabe von 1080p-Videos mit automatischer Audio-Synchronisierung unterstützt. MMR ist standardmäßig aktiviert. Der RDP-Client verhandelt mit jedem RDP-Server, den er kontaktiert, und wenn MMR verfügbar ist, wird es verwendet.

MMR verwendet außerdem ein erweitertes Codec-Erkennungsschema, das ermittelt, ob der Thin Client den vom Remote-Host angeforderten Codec unterstützt, bevor versucht wird, ihn umzuleiten. Das Ergebnis ist, dass nur unterstützte Codecs umgeleitet werden und für alle nicht unterstützten Codecs eine serverseitige Darstellung genutzt wird.

Um MMR auf dem Thin Client für alle RDP-Verbindungen zu deaktivieren, setzen Sie den folgenden Registrierungsschlüsselwert auf 0:

```
root/ConnectionType/freerdp/general/enableMMR
```

Da RemoteFX bereits akzeptable Multimedia-Leistung bietet, können Sie MMR mit RemoteFX deaktivieren, indem Sie den folgenden Registrierungsschlüsselwert auf 1 setzen:

```
root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX
```

---

 **TIPP:** Für eine vereinfachte Verwaltung empfiehlt HP, MMR auf dem Remote-Host zu aktivieren oder zu deaktivieren.

---

## RDP-Geräteumleitung

Die Geräteumleitung stellt sicher, dass ein Gerät automatisch erkannt wird und in der Remotesitzung verfügbar ist, wenn ein Benutzer ein Gerät mit dem Thin Client verbindet. RDP unterstützt die Umleitung von vielen verschiedenen Arten von Geräten.

## RDP-USB-Umleitung

Die USB-Umleitung funktioniert durch die Übermittlung von USB-Protokollaufrufen auf niedriger Stufe über das Netzwerk an den Remote-Host. Ein am lokalen Host angeschlossenes USB-Gerät wird auf dem Remote-Host als systemeigenes USB-Gerät dargestellt, als wäre es lokal angeschlossen. Windows Standardtreiber unterstützen das Gerät in der Remotesitzung und alle Gerätetypen werden unterstützt, ohne dass zusätzliche Treiber auf dem Thin Client erforderlich sind.

Nicht alle Geräte sind standardmäßig auf USB-Umleitung eingestellt. Beispielsweise sind USB-Tastaturen, -Mäuse und andere Eingabegeräte in der Regel nicht so eingestellt, dass sie umgeleitet werden, da die Remotesitzung erwartet, dass die Eingabe vom Thin Client kommt. Einige Geräte wie z. B. Massenspeicher, Drucker und Audiogeräte verwenden möglicherweise zusätzliche Optionen für die Umleitung.

Beachten Sie die folgenden zusätzlichen Informationen über die USB-Umleitung mit RDP:

- Der Server muss die USB-Umleitung unterstützen, um für den Thin Client verfügbar zu sein. Die USB-Umleitung für allgemeine Zwecke wird bei RDVH-Servern mit RemoteFX, Windows 8 und Windows Server 2012 unterstützt.
- Das Protokoll im USB-Manager in der Systemsteuerung muss auf RDP festgelegt werden.
- Für RDP-Verbindungen bestimmen die Steuerelemente im USB-Manager, ob ein USB-Gerät umgeleitet wird. Die Einstellungen für die einzelnen Verbindung bestimmen, wie ein USB-Gerät umgeleitet wird.

## RDP-Massenspeicherumleitung

Standardmäßig leitet die RDP-Sitzung alle Massenspeichergeräte über eine High-Level-Laufwerksumleitung an den Remote-Host um. Wenn ein Gerät wie ein USB-Flash-Laufwerk, ein USB-DVD-ROM-Laufwerk oder ein externes USB-Festplattenlaufwerk an den Thin Client angeschlossen ist, erkennt der Thin Client dies und stellt es im lokalen Dateisystem bereit. RDP erkennt dann ein bereitgestelltes Laufwerk und leitet es zum Remote-Host um. Auf dem Remote-Host erscheint es als neue Festplatte in Windows Explorer, mit dem Namen `<device label> on <client hostname>`; **Beispiel:** `Bill_USB on HP04ab598100ff`.

Es gibt drei Einschränkungen für diese Art von Umleitung.

- Das Gerät wird nicht in der Taskleiste auf dem Remote-Host mit einem Symbol zum Auswerfen angezeigt. Aus diesem Grund müssen Sie dem Gerät nach einer Kopie genügend Zeit zur Datensynchronisation geben, bevor Sie das Gerät entfernen, um sicherzustellen, dass das Gerät nicht beschädigt wird. In der Regel dauert dies weniger als eine Sekunde nachdem der Dialog Datei kopieren beendet ist, aber es können bis zu 10 Sekunden erforderlich sein, je nach der Schreibgeschwindigkeit des Geräts und der Netzwerklatenz.
- Nur vom Thin Client unterstützte Dateisysteme werden bereitgestellt. Die unterstützten Dateisysteme sind FAT32, NTFS, ISO9660 (CD-ROMs), UDF (DVD-ROMs) und ext3.
- Das Gerät wird als Verzeichnis behandelt. Häufige Laufwerksaufgaben wie die Formatierung und die Änderung der Festplattenbezeichnung stehen nicht zur Verfügung.

Die USB-Umleitung von Speichergeräten kann in den Einstellungen der einzelnen Verbindungen deaktiviert werden. Wenn gewünscht, können Sie auch die gesamte Massenspeicher-Umleitung deaktivieren. Um dies zu tun, schalten Sie USB-Umleitung aus und ändern Sie den Registrierungsschlüssel, wie in der folgenden Tabelle beschrieben.

Registrierungseintrag	Einzurichtender Wert	Beschreibung
<code>root/USB/root/holdProtocolStatic</code>	1	Stellen Sie sicher, dass der USBR-Typ nicht automatisch geändert wird, wenn eine Verbindung festgelegt oder deren Festlegung aufgehoben wird.
<code>root/USB/root/protocol</code>	lokal	Stellen Sie sicher, dass die RDP-Verbindung nicht versucht, irgendwelche Geräte zur Remotesitzung umzuleiten.

Um die lokale Bereitstellung von USB-Massenspeichergeräten vollständig zu deaktivieren oder um die Umleitung von USB-Massenspeichergeräten zu deaktivieren, jedoch anderen Geräten die Umleitung weiterhin zu ermöglichen, löschen Sie im Thin Client-Dateisystem die udev-Regel `/etc/udev/rules.d/010_usbdrive.rules`.

## RDP-Druckerumleitung

Standardmäßig hat RDP zwei Methoden der Druckerumleitung aktiviert:

- **USB-Umleitung** – Alle am Gerät angeschlossenen USB-Drucker werden in der Remote-Sitzung als lokale Drucker angezeigt. Der Standardvorgang für die Druckerinstallation muss in der Remote-Sitzung durchgeführt werden, falls der Drucker noch nicht am Remote-Host installiert ist. Es müssen lokal keine Einstellungen vorgenommen werden.
- **High-Level-Umleitung** – Wenn die USB-Umleitung auf dem Remote-Host nicht verfügbar ist oder wenn der Drucker ein paralleler oder serieller Drucker ist, verwenden Sie die High-Level-Umleitung. Konfigurieren Sie den Drucker für die Verwendung eines lokalen Druckerspoolers und der RDP-Client richtet automatisch einen Remotedrucker ein, der Befehle für Druckspoolvorgänge über einen virtuellen Kanal vom Remote-Host an den Thin Client sendet.

Diese Methode erfordert, dass der Drucker auf dem Thin Client konfiguriert ist und ein Windows-Treiber auf dem Thin Client angegeben wurde, da der RDP-Client für den Remote-Host angeben muss, welcher Treiber für den Remotedrucker verwendet werden soll. Dieser Windows-Treiber muss mit dem Treiber übereinstimmen, den der Drucker verwenden würde, wenn er an ein Windows-Betriebssystem lokal angeschlossen wäre. Diese Informationen finden Sie normalerweise unter **Modell** in den Druckereigenschaften.



**HINWEIS:** Weitere Informationen finden Sie unter [Konfiguration eines seriellen oder parallelen Druckers auf Seite 70](#).

## RDP-Audiumleitung

Standardmäßig leitet eine High-Level-Audiumleitung Audioinhalte vom Remote-Host an den Thin Client um. Möglicherweise muss eine grundlegende Sprachsteuerung eingerichtet werden. Zudem enthält RDP 7.1 eine Reihe von erweiterten Audiumleitungsfunktionen, die eine zusätzliche Konfiguration erfordern könnten.

Siehe die folgenden Hinweise zur Verwendung der Audio-Umleitung mit RDP:

- RDP liefert die höchste Audioqualität, die die Netzwerkbandbreite zulässt. RDP reduziert die Audioqualität für die Wiedergabe bei Verbindungen mit geringer Bandbreite.
- Bei Standard-RDP stehen keine nativen Audio- oder Videosynchronisationsmechanismen zur Verfügung. Längere Videos können möglicherweise nicht mit Audio synchronisiert werden. MMR oder RemoteFX können dieses Problem beheben.
- HP empfiehlt eine High-Level Audio-Umleitung; eine USB-Umleitung der Audiogeräte ist jedoch nur möglich, wenn zusätzliche Funktionen, wie z. B. eine digitale Lautstärkeregelung, vorhanden sind. Für analoge Geräte ist nur eine High-Level-Umleitung verfügbar.
- Die Mikrofon-Umleitung ist standardmäßig aktiviert. Die Standard-Mikrofonlautstärke muss möglicherweise auf dem Thin Client angepasst werden. Die Einstellungen älterer Windows RDP-Server müssen geändert werden, um einen Audioeingang zu aktivieren.
- Sowohl die lokalen wie die Remote-Lautstärkeinstellungen haben Auswirkungen auf die endgültige Lautstärke. HP empfiehlt, die lokale Lautstärke auf das Maximum einzustellen und die Lautstärke innerhalb des Remote-Host anzupassen.

## RDP-Smart Card-Umleitung

Standardmäßig werden Smart Cards mit High-Level-Umleitung umgeleitet. Dadurch können sie zur Anmeldung bei der Sitzung und anderen Remote-Anwendungen verwendet werden.

So aktivieren Sie die Smart Card-Anmeldung für eine RDP-Verbindung:

- ▲ Wählen Sie in RDP Connection Manager **Smart Card-Anmeldung erlauben**.

Dies ermöglicht dem Benutzer eine Verbindung, ohne zuerst die Anmeldedaten angeben zu müssen. Der RDP-Client startet die RDP-Sitzung und der Benutzer wird aufgefordert, sich über die Smart Card zu authentifizieren.

Diese Technologie erfordert, dass Treiber für den Treiber des Smart Card-Lesegeräts auf dem Thin Client installiert werden. Standardmäßig werden die CCID- und Gemalto-Treiber installiert, die Unterstützung für die meisten der verfügbaren Smart Card-Lesegeräte bieten. Zusätzliche Treiber können installiert werden, indem Sie sie `/usr/lib/pkcs11/` hinzufügen.



**HINWEIS:** Wenn die Smart Card-Anmeldung aktiviert ist, wird auf Netzwerkebene die Authentifizierung nicht unterstützt und ist automatisch deaktiviert.

## VMware Horizon View

### VMware Horizon View-Einstellungen pro Verbindung



**HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

#### Netzwerk

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer VMware Horizon View-Verbindung in der Kategorie „Netzwerk“ verfügbar sind.

Option	Beschreibung
Name	Eingabe des Namens für diese Verbindung.
Server	Den Hostnamen oder die IP-Adresse des VMware Horizon View-Servers eingeben.
Benutzername	Den für die Verbindung zu verwendenden Benutzernamen eingeben.
Kennwort	Das für die Verbindung zu verwendende Kennwort eingeben.
Domäne	Die für die Verbindung zu verwendende Domäne eingeben.
Desktop	Zur Angabe des optionalen Desktop-Pools, mit dem automatisch eine Verbindung hergestellt werden soll.

#### Allgemein

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer VMware Horizon View-Verbindung in der Kategorie „Allgemein“ verfügbar sind.

Option	Beschreibung
Automatische Anmeldung	Wenn aktiviert, wird der Benutzer automatisch angemeldet, wenn die Verbindung hergestellt ist.

**HINWEIS:** HP empfiehlt das Aktivieren dieser Option.

Option	Beschreibung
Smart Card Anmeldung zulassen	Aktiviert die Smart Card-Anmeldung.  <b>HINWEIS:</b> Weitere Informationen zu Smart Cards finden Sie unter <a href="#">VMware Horizon View-Smart Card-Umleitung auf Seite 33</a> .
Anwendung nicht maximiert starten	Wenn aktiviert, starten Anwendungen nicht maximiert in Windows.
Bevorzugtes Protokoll	Ermöglicht die Auswahl von PCoIP, RDP oder BLAST als bevorzugtes Protokoll. Sie können das Protokoll aber auch später auswählen.
Anwendungsgröße	Legt die Fenstergröße der Anwendung fest. Sie können <b>All Monitors</b> (Alle Monitore), <b>Full Screen</b> (Vollbild), <b>Large Window</b> (Großes Fenster) oder <b>Small Window</b> (Kleines Fenster) auswählen.
Desktopgröße	Legt die Fenstergröße des Desktops fest. Sie können <b>All Monitors</b> (Alle Monitore), <b>Full Screen</b> (Vollbild), <b>Large Window</b> (Großes Fenster) oder <b>Small Window</b> (Klines Fenster) auswählen.

## Security (Sicherheit)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer VMware Horizon View-Verbindung in der Kategorie „Security“ (Sicherheit) verfügbar sind.

Option	Beschreibung
Nach der Trennung schließen	Sorgt dafür, dass sich der VMware Horizon View-Client automatisch schließt, nachdem sich Benutzer an ihren Desktops abgemeldet haben oder die Sitzung aufgrund eines Fehlers beendet wurde.  Diese Option ist eine Sicherheitsfunktion und so konzipiert, dass ein Benutzer keinen weiteren Schritt durchführen muss, um sich vollständig abzumelden nachdem er mit seiner Desktop-Sitzung fertig ist.  Diese Option ist standardmäßig aus Sicherheitsgründen aktiviert, kann aber deaktiviert werden, wenn Benutzer nach dem Abmelden von einer Sitzung häufig zu einem neuen Desktop-Pool wechseln und sich nicht wieder komplett neu anmelden möchten.
Obere Menüleiste ausblenden	Macht die obere Menüleiste für Benutzer unsichtbar.  Diese Option ist standardmäßig aktiviert. Deaktivieren Sie diese Option, wenn der Benutzer während einer VMware Horizon View-Sitzung Zugriff auf Optionen für die Fenstergröße oder Desktop-Pool-Auswahl haben möchte.
Benutzern das Ändern der Server-Adresse nicht erlauben	Wenn aktiviert, können Endbenutzer die Serveradresse nicht ändern.
Sicherheitsstufe der Verbindung	Verwenden Sie die <b>Sicherheitsstufe der Verbindung</b> zum Einstellen der Sicherheitsstufe, die der VMware Horizon View-Client bei der Verbindung zum Server verwendet.  <b>HINWEIS:</b> Nähere Informationen über das Verhalten von Verbindungs-Sicherheitsstufen finden Sie unter <a href="#">Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung auf Seite 34</a> .

## RDP-Optionen

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer VMware Horizon View-Verbindung in der Kategorie „RDP-Optionen“ verfügbar sind.

Option	Beschreibung
Bewegungseignisse aktivieren	Aktiviert das Senden von Bewegungen für diese Verbindung.
Datenkomprimierung aktivieren	Aktiviert die Datenkomprimierung für diese Verbindung.
Veraltete RPD-Verschlüsselung aktivieren	Aktiviert die Verschlüsselung für diese Verbindung.
Offscreen-Cache aktivieren	Wenn aktiviert, wird der Offscreen-Speicher verwendet, um Bitmaps zu cachen.
An Administratorkonsole anheften	Fügt die Verbindung zum Administrator-Konsolenanschluss hinzu.
Sitzungsübergreifendes Kopieren/Einfügen	Wenn aktiviert, ist das Kopieren und Einfügen zwischen verschiedenen RDP-Sitzungen möglich.
Pufferung von RDP6-Grundtypen aktivieren	Wenn diese Option aktiviert ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
Progressive RemoteFX Codec aktivieren	Aktiviert den progressiven RemoteFX-Codec, mit dem der Desktop in einer Reihe immer schärferer Bilder übertragen wird.
Richtlinie zur Zertifikatsüberprüfung	Führen Sie eine der folgenden Aktionen aus: <ul style="list-style-type: none"> <li>• <b>Alle RDP-Server-Zertifikate akzeptieren</b></li> <li>• <b>Beibehaltene Hosts verwenden; Bei unbekanntem oder ungültigen Zertifikaten warnen</b></li> <li>• <b>Beibehaltene Hosts überspringen; Bei unbekanntem oder ungültigen Zertifikaten warnen</b></li> <li>• <b>Nur mit vorab genehmigten RDP-Servern verbinden</b></li> </ul>
TLS-Version	Legt die Transport Layer Security-Version fest, die in den Anfangsphasen der Aushandlung mit dem RDP-Server verwendet wird. Legen Sie diese Option auf die TLS-Version Ihres RDP-Servers fest oder verwenden Sie <b>auto</b> .  <b>HINWEIS:</b> Durch einige Serverfehler auf einigen ungepatchten RDP-Servern kann die automatische Einstellung zu einem Fehler führen, deshalb ist es nicht die Standardeinstellung.
Zu sendender Hostname	Normalerweise wird der Thin Client-Hostname für Client-Zugriffslizenzen verwendet. Dieses Feld erlaubt das Senden eines anderen Werts.  <b>TIPP:</b> Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.
Lastenausgleichsinfo	Verwenden Sie diese Option mit einer vermittelten RDP-Verbindung.  <b>TIPP:</b> Wählen Sie das Symbol ? neben dieser Option, um weitere Informationen zu erhalten.
Sounds auf dem Remotecomputer	Gibt an, wo der Remotecomputer-Sound wiedergegeben werden sollte (remote oder lokal), oder ob er überhaupt nicht wiedergegeben werden sollte.
Portzuweisung aktivieren	Ordnet die seriellen und parallelen Anschlüsse des Thin Client der Remotesitzung zu.
Druckerzuweisung aktivieren	Ordnet die lokale Druckwarteschlange der Remotesitzung zu. Verwenden Sie diese Option, wenn die USB-Umleitung auf dem Remote-Host nicht verfügbar ist oder wenn der Drucker ein paralleler oder serieller Drucker ist. Konfigurieren Sie den Drucker für die Verwendung eines lokalen Druckerspoolers und der VMware Horizon View-Client richtet automatisch einen Remotedrucker ein, der Befehle für Druckpoolvorgänge über einen virtuellen Kanal vom Remote-Host an den Thin Client sendet.  Diese Methode erfordert, dass der Drucker auf dem Thin Client konfiguriert ist und ein Windows Treiber auf dem Thin Client angegeben wurde, da der VMware Horizon View-Client für den Remote-Host angeben muss, welcher Treiber für den Remotedrucker verwendet werden soll. Dieser Windows Treiber muss mit dem Treiber übereinstimmen, den der Drucker verwenden würde, wenn er an ein Windows Betriebssystem lokal

Option	Beschreibung
	angeschlossen wäre. Diese Informationen finden Sie normalerweise unter <b>Modell</b> in den Druckereigenschaften.
Freigegebene Ordner	<b>Add</b> (Hinzufügen), <b>Remove</b> (Entfernen) oder <b>Edit</b> (Bearbeiten) freigegebener Ordner.

## RDP Experience (RDP-Darstellung)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer VMware Horizon View-Verbindung in der Kategorie „RDP Experience“ (RDP-Darstellung) verfügbar sind.

Option	Beschreibung
MMR aktivieren	Aktiviert die Multimedia-Umleitung.
Auswahl der Verbindungsgeschwindigkeit zur Optimierung der Leistung	<p>Das Auswählen einer Verbindungsgeschwindigkeit (<b>LAN</b>, <b>Broadband</b> (Breitband) oder <b>Modem</b>) wird die folgenden Optionen aktivieren oder deaktivieren, um die Leistung zu optimieren:</p> <ul style="list-style-type: none"> <li>• <b>Desktop background</b> (Desktop-Hintergrund)</li> <li>• <b>Font smoothing</b> (Schriftglättung)</li> <li>• <b>Desktop composition</b> (Desktopgestaltung)</li> <li>• <b>Show contents of window while dragging</b> (Inhalte des Fensters beim Verschieben anzeigen)</li> <li>• <b>Menu and window animation</b> (Menü- und Fensteranimation)</li> <li>• <b>Themes</b> (Designs)</li> </ul> <p>Die Auswahl von <b>Client Preferred Settings</b> (Vom Client bevorzugte Einstellungen) ermöglicht dem VMware Horizon View-Client die Auswahl der zu verwendenden Optionen.</p> <p>Sie können auch Ihre eigene benutzerdefinierte Kombination von Optionen auswählen.</p>
Ende-zu-Ende Verbindungs-Health-Überwachung	Dient zum Aktivieren der Timeout-Options.
Zeitlimit bei Warnung	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, bevor der Benutzer eine Warnung zur abgebrochenen Verbindung erhält. Diese Funktion kann deaktiviert werden, indem Sie die Option löschen oder die Zeit auf Null setzen.</p> <p>Wenn die Option <b>Show Warning Dialog</b> (Dialogfeld mit Warnung anzeigen) ausgewählt ist, wird ein Warnungsdialogfeld angezeigt, wenn dieses Zeitlimit erreicht ist. Andernfalls wird die Warnung nur in das Verbindungsprotokoll geschrieben.</p> <p><b>TIPP:</b> HP empfiehlt, den Wert des Zeitlimits für Netzwerke, die regelmäßig hoch belastet oder zeitweise überlastet sind bzw. ausfallen, zu erhöhen.</p>
Zeitlimit bei Wiederherstellung	Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client auf die Wiederherstellung der Verbindung wartet, bevor eine bestimmte Maßnahme eingeleitet wird. Am Ende dieser Frist versucht der RDP-Client kurz, erneut eine Verbindung mit der Sitzung aufzubauen.
Zeitlimit bei Fehler	<p>Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client wartet, bevor er aufhört zu versuchen, die Verbindung mit diesem Server wiederherzustellen.</p> <p><b>TIPP:</b> Wählen Sie das Symbol ? neben diesem Feld, um weitere Informationen zu erhalten.</p>

## Advanced (Erweitert)



**HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

---

## VMware Horizon View-Sitzungen mit mehreren Monitoren

VMware Horizon View unterstützt Multi-Monitor-Sitzungen. Zur Verbesserung der Virtualisierungserfahrung verwenden die Standard-VMware Horizon View-Sitzungen Vollbildmodus und umfassen alle Monitore. Zur Auswahl einer anderen Fenstergröße wählen Sie **Full Screen – All Monitors** (Vollbildmodus – Alle Monitore) unter dem Protokolltyp des Desktop-Pools für die Verbindung. Wählen Sie dann eine andere Option aus der Liste für die Fenstergrößen aus. Wenn Sie das nächste Mal eine Verbindung zu einer Sitzung herstellen, wird das Fenster in der ausgewählten Größe geöffnet.

## VMware Horizon View-Tastenkombinationen

### Windows Tastenkombinationen

Zur Unterstützung der Windows-Systemverwaltung unterstützt VMware Horizon View die Tastenkombinationen von Windows. Wenn Sie zum Beispiel **Strg+Alt+Entf** verwenden, zeigt VMware Horizon View eine Meldung mit den folgenden Optionen an:

- Einen Befehl mit **Strg+Alt+Entf** senden.
- Sitzung trennen – Verwenden Sie dies, wenn Sie keine andere Möglichkeit haben, die Sitzung zu beenden.

Die Windows Tastaturkürzel werden an die Remote-Desktop-Sitzung weitergeleitet. Das Ergebnis ist, dass lokale Tastenkombinationen wie **Strg+Alt+Tabulator** und **Strg+Alt+F4** nicht innerhalb der Remote-Sitzung funktionieren.

 **TIPP:** Um Sitzungen umschalten zu können, deaktivieren Sie die Optionen **Obere Menüleiste ausblenden** im VMware Horizon View Connection Manager oder über den Registrierungsschlüssel `root/ConnectionType/view/connections/<UUID>/hideMenuBar`.

### Medientasten

VMware Horizon View verwendet Medientasten zur Steuerung von Optionen wie Lautstärke, Wiedergabe/Pause und Stummschaltung während eines Remote-Desktop-Sitzung. Damit werden Multimediaprogramme wie z. B. Windows Media Player unterstützt.

## VMware Horizon View-Multimedia-Umleitung

VMware Horizon View-Verbindungen unterstützen die MMR-Funktionalität, wenn sie mit dem Microsoft RDP-Protokoll verwendet werden.

Weitere Informationen hierzu finden Sie unter [RDP-Multimedia-Umleitung auf Seite 23](#).

## VMware Horizon View-Geräteumleitung

### VMware Horizon View-USB-Umleitung

Um USBR für VMware Horizon View-Verbindungen zu aktivieren, wählen Sie im USB-Manager **VMware Horizon View** als Remoteprotokoll.

Weitere Informationen zu USBR, einschließlich Geräte- und klassenspezifische Umleitung, finden Sie unter [RDP-USB-Umleitung auf Seite 23](#)

### VMware Horizon View-Massenspeicherumleitung

Sie müssen das RDP-Verbindungsprotokoll verwenden, um die Massenspeicher-Umleitung mit einer VMware Horizon View-Verbindung zu verwenden.

Zur Durchführung einer Laufwerksumleitung von einem USB-Laufwerk oder internen SATA-Laufwerk:

- ▲ Fügen Sie in der Option Befehlszeilenargumente – `xfreerdoptions='/drive:$foldname,shared folder path, share device'` hinzu.

Zum Beispiel gibt in einer VMware Horizon View-Verbindung `-xfreerdoptions='/drive:myfolder,/home/user,/dev/sda2'` den `/home/user` auf dem Laufwerk `/dev/sda2` als `myfolder` frei.

Weitere Einzelheiten finden Sie unter [RDP-Massenspeicherumleitung auf Seite 24](#).

## VMware Horizon View-Druckerumleitung

Für Verbindungen mit dem PCoIP-Protokoll auf x86-Einheiten können unter Verwendung der VMware Horizon View High-Level-Druckerumleitung oder von USB-R Drucker freigegeben werden. PCoIP-Verbindungen auf ARM-Einheiten unterstützen nur die USB-R-Druckerumleitung. Für Verbindungen mit dem RDP-Protokoll, siehe [RDP-Druckerumleitung auf Seite 24](#) für weitere Informationen.

## VMware Horizon View-Audioumleitung

Wenn Sie die Audio-Aufzeichnungsfunktion nicht benötigen, verwenden Sie die High-Level-Audio-Umleitung. Audio wird über die 3,5-mm-Buchse oder standardmäßig über ein USB-Headset abgespielt, wenn dieses eingesteckt ist. Verwenden Sie den lokalen Audio-Manager zum Anpassen der Eingangs-/Ausgangsstufen, zur Auswahl der Wiedergabe und zum Erfassen von Geräten.

Der VMware Horizon View-Client unterstützt die High-Level-Umleitung für Audioaufzeichnungen über den Verbindungstyp PCoIP auf x86-Einheiten nur, wenn er mit einem Server verbunden ist, auf dem VMware Horizon View 5.2 Feature Pack 2 oder höher läuft. Wenn Sie die Unterstützung von Audioaufzeichnung benötigen, und eine andere Konfiguration verwenden, wählen Sie eine der folgenden Methoden:

- Wenn Ihr System den VMware Horizon View-Client 1.7 oder höher verwendet, können Sie mit dem RDP-Protokoll eine High-Level-Audio-Umleitung ermöglichen, entweder durch die 3,5-mm-Buchse oder ein USB-Headset.



**HINWEIS:** Um eine High-Level-Audio-Aufzeichnungsumleitung über das RDP-Protokoll zu verwenden, muss der Server dies unterstützen und so konfiguriert sein, dass die Audio-Aufzeichnung über eine Remotesitzung zulässig ist. Der Server muss Windows 7 oder höher ausführen. Sie müssen außerdem sicherstellen, dass der Registrierungsschlüssel `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\DisableAudioCapture` auf 0 eingestellt ist.

- Wenn Sie ein USB-Headset mit einem Mikrofon haben, können Sie USB-R verwenden. Stellen Sie das USB-Headset so ein, dass es in die Sitzung umgeleitet wird. Das Headset wird dann als Audiogerät angezeigt. Standardmäßig werden USB-Audiogeräte nicht umgeleitet und der VMware Horizon View-Client verwendet eine High-Level-Audioumleitung. Um das USB-Headset umzuleiten, verwenden Sie den USB-Manager des Thin Client und wählen Sie das USB-Headset aus, das umgeleitet werden soll. Stellen Sie sicher, dass die **VMware Horizon View** als USB-R-Protokoll ausgewählt ist, und stellen Sie sicher, dass das Headset unter **Devices** (Geräte) zur Umleitung markiert ist.



**HINWEIS:** VMware und HP empfehlen, kein USB-R für Headsets zu verwenden. Es ist eine sehr hohe Netzwerkbandbreite erforderlich, um Audiodaten über das USB-R-Protokoll zu streamen. Außerdem ist mit dieser Methode die Audioqualität möglicherweise schlecht.

## VMware Horizon View-Smart Card-Umleitung

So verwenden Sie eine Smart Card zur Anmeldung am VMware Horizon View-Server:

1. Stellen Sie sicher, dass die Smart Card-Anmeldung im VMware Horizon View Connection Manager aktiviert ist.

Nach dem Starten der Verbindung zeigt der VMware Horizon View-Client eine Liste der Server-Anmeldeinformationen.

2. Zum Entsperren der Anmeldeinformationen und zum Zugriff auf den VMware Horizon View Manager-Server geben Sie die entsprechende PIN für den Server ein.

---

 **HINWEIS:** Nachdem Sie die korrekte PIN eingegeben haben, werden die Anmeldeinformationen des Benutzers für die Anmeldung am VMware Horizon View Manager-Server verwendet. Weitere Informationen zum Konfigurieren des Servers, damit er die Smart Card-Anmeldung unterstützt, finden Sie in der Dokumentation für VMware Horizon View. Solange der Server konfiguriert ist, um eine Smart Card-Anmeldung zuzulassen, werden die Anmeldeinformationen des Benutzers weitergeleitet und die Anmeldung am Desktop erfolgt ohne erneute Eingabe einer PIN.

 **HINWEIS:** Für eine Anmeldung am VMware Horizon View Manager-Administratorserver mit einer Smart Card muss der lokale Smart Card-Treiber auf dem Thin Client installiert sein. Unter [RDP-Smart Card-Umleitung auf Seite 26](#) finden Sie weitere Informationen zur Smart Card-Treiberinstallation. Nach der Anmeldung am Remote-Host wird die Smart Card über einen virtuellen Kanal und nicht USBR an den Remote-Host übergeben. Diese Umleitung über einen virtuellen Kanal stellt sicher, dass die Smart Card für Aufgaben wie E-Mail-Signaturen, Bildschirmsperren usw. verwendet werden kann, führt aber möglicherweise dazu, dass die Smart Card nicht als Smart Card-Gerät im Geräte-Manager von Windows angezeigt wird.

 **HINWEIS:** Am Remote-Host müssen die richtigen Smart Card-Treiber installiert sein.

---

## VMware Horizon View-Webcam-Umleitung

Der VMware Horizon View-Client unterstützt eine High-Level Webcamumleitung nur über RTAV, unter Verwendung von x86-Einheiten, die an einen Back-End-Server angeschlossen sind, der mit VMware Horizon View 5.2 Feature Pack 2 oder höher ausgestattet ist. Andere Verbindungsarten unterstützen keine High-Level Webcamumleitung und können Webcams nur unter Verwendung von USBR umleiten. Basierend auf internen Tests und Validierungen hat HP festgestellt, dass die Verbindung einer Webcam über eine einfache USBR eine schlechte Leistung erbringt. HP empfiehlt die Verwendung dieser Konfiguration nicht und schlägt vor, dass Kunden, die diese Funktion benötigen, die Verwendung von x86-Einheiten mit RTAV-Technologie ausprobieren, um ein zufriedenstellendes Leistungsniveau zu erreichen. Mit USBR funktioniert die Webcam möglicherweise schlecht oder überhaupt nicht. Weitere Informationen finden Sie unter [RDP-USB-Umleitung auf Seite 23](#).

## Ändern des VMware Horizon View-Protokolls

Der VMware Horizon View-Client kann das PCoIP-, RDP- oder BLAST-Protokoll nutzen.

So ändern Sie das Protokoll:

1. Wählen Sie im VMware Horizon View-Client einen Pool, der eines der unterstützten Protokolle unterstützt.
2. Wählen Sie im Menü **Connection** (Verbindung) **Settings** (Einstellungen) aus.
3. Ändern Sie das Protokoll mithilfe des Dropdown-Feldes neben **Connect Via** (Verbinden über).



**HINWEIS:** Legen Sie im VMware Horizon View Manager fest, welches Protokoll für die einzelnen Desktoppools verwendet werden soll.



**TIPP:** HP empfiehlt, das PCoIP-Protokoll zu verwenden, um die Desktop-Erfahrung zu verbessern. Allerdings bietet das RDP-Protokoll mehr Optionen für die Anpassung und funktioniert möglicherweise bei langsamen Verbindungen besser.

## Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung

VMware Horizon View Client 1.5 und VMware Horizon View Server 5.0 und später erfordern HTTPS. Standardmäßig warnt der VMware Horizon View-Client bei nicht vertrauenswürdigen Serverzertifikaten, wie z. B. selbstsignierte (wie das VMware Horizon View Manager-Standardzertifikat) oder abgelaufene Zertifikate. Falls ein Zertifikat durch eine Zertifizierungsstelle (CA, Certificate Authority) signiert wird und die CA nicht vertrauenswürdig ist, gibt die Verbindung einen Fehler zurück und dem Benutzer wird es nicht gestattet, eine Verbindung herzustellen.

HP empfiehlt, dass ein signiertes Zertifikat, das von einer standardmäßigen, vertrauenswürdigen Stammzertifizierungsstelle überprüft wurde, auf dem VMware Horizon View Manager-Server verwendet wird. Dies stellt sicher, dass der Benutzer eine Verbindung zum Server herstellen kann, ohne dazu aufgefordert zu werden bzw. ohne dass es erforderlich ist, etwas an der Konfiguration zu ändern. Wenn eine interne CA verwendet wird, gibt die VMware Horizon View-Client-Verbindung einen Fehler zurück, bis Sie eine der folgenden Aufgaben ausgeführt haben:

- Verwenden Sie den Zertifikat-Manager, um das Zertifikat aus einer Datei oder URL zu importieren.
- Verwenden Sie eine Remote-Profilaktualisierung zum Importieren eines Zertifikats.
- Stellen Sie im VMware Horizon View Connection Manager **Sicherheitsstufe der Verbindung** auf **Allow all connections** (Alle Verbindungen zulassen).

In der folgenden Tabelle wird die Vertrauensstellung von Zertifikaten beschrieben, wenn die Sicherheitsstufe auf **Refuse insecure connections** (Unsichere Verbindungen ablehnen) festgelegt ist.

Vertrauensstellung des Zertifikats	Ergebnis
Vertrauenswürdig	Vertrauenswürdig
Selbstsigniert	Fehler
Abgelaufen	Fehler
Nicht vertrauenswürdig	Fehler

In der folgenden Tabelle wird die Vertrauensstellung von Zertifikaten beschrieben, wenn die Sicherheitsstufe auf **Warnung** festgelegt ist.

Vertrauensstellung des Zertifikats	Ergebnis
Vertrauenswürdig	Vertrauenswürdig
Selbstsigniert	Warnung
Abgelaufen	Warnung
Nicht vertrauenswürdig	Fehler

In der folgenden Tabelle wird die Vertrauensstellung von Zertifikaten beschrieben, wenn die Sicherheitsstufe auf **Allow all connections** (Alle Verbindungen zulassen) festgelegt ist.

Vertrauensstellung des Zertifikats	Ergebnis
Vertrauenswürdig	Vertrauenswürdig
Selbstsigniert	Nicht vertrauenswürdig
Abgelaufen	Nicht vertrauenswürdig
Nicht vertrauenswürdig	Nicht vertrauenswürdig

In der folgenden Tabelle wird das mit den einzelnen Ergebnissen verknüpfte Verbindungsverhalten beschrieben.

Ergebnis	Beschreibung
Vertrauenswürdig	Stellt ohne den Dialog für eine Zertifikatswarnung eine Verbindung her und zeigt ein grünes Schlosssymbol an.
Nicht vertrauenswürdig	Stellt ohne den Dialog für eine Zertifikatswarnung eine Verbindung her und zeigt ein rotes entsperres Schlosssymbol an.
Warnung	Stellt mit dem Dialog für eine Zertifikatswarnung eine Verbindung her und zeigt ein rotes entsperres Schlosssymbol an.
Fehler	Erlaubt die Verbindung nicht

## Web Browser

### Web Browser – Allgemeine Einstellungen

In der folgenden Tabelle werden die allgemeinen Web Browser-Einstellungen beschrieben.



**HINWEIS:** Diese Einstellungen haben Auswirkungen auf alle Web Browser-Verbindungen.

Option	Beschreibung
Web Browser-Einstellungen	Öffnet das Dialogfeld Firefox-Einstellungen.
Verbindungen erlauben, ihre eigenen Einstellungen zu verwalten	Wenn aktiviert, werden die Firefox-Einstellungen für jede Web Browser-Verbindung gespeichert. Andernfalls werden die Einstellungen jedes Mal zurückgesetzt, wenn die Verbindung gestartet wird.

## Web Browser-Einstellungen pro Verbindung

 **HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

### Configuration (Konfiguration)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer Web Browser-Verbindung in der Kategorie „Configuration“ (Konfiguration) verfügbar sind.

Option	Beschreibung
Name	Der Verbindungsname.
URL	Die URL für die Verbindung.
Beabsichtigte Verwendung	Festlegen der beabsichtigten Verwendung der Verbindung auf <b>Citrix</b> , <b>RDP</b> oder <b>Internet</b> .
Kiosk-Modus aktivieren	Aktiviert den Kioskmodus.
Vollbildmodus aktivieren	Verwendet den Vollbildmodus für die Verbindung.
Druckdialog aktivieren	Aktiviert das Dialogfeld „Drucken“.

### Advanced (Erweitert)

 **HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

## Zusätzliche Verbindungstypen (nur ThinPro)

 **HINWEIS:** Standardmäßig sind diese Verbindungstypen in Smart Zero nicht verfügbar. Weitere Informationen finden Sie unter [Auswählen einer Betriebssystemkonfiguration auf Seite 2](#).

### TeemTalk

 **HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren. Weitere Informationen zu HP TeemTalk finden Sie im *Benutzerhandbuch* für HP TeemTalk.

### Configuration (Konfiguration)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer TeemTalk-Verbindung in der Kategorie „Configuration“ (Konfiguration) verfügbar sind.

Option	Beschreibung
Name	Der Verbindungsname.
Teemtalk-Erstellungsassistent	Zum Öffnen des TeemTalk-Sitzungsassistenten. Weitere Informationen finden Sie in den anderen Tabellen in diesem Abschnitt.
Systemton	Aktiviert den Systemton.

## TeemTalk Session Wizard (TeemTalk-Sitzungsassistent)

In der folgenden Tabelle werden die Einstellungen beschrieben, die im TeemTalk-Sitzungsassistenten in der Kategorie „Connection Information“ (Verbindungsinformationen) verfügbar sind.

Option	Beschreibung
Sitzungsname	Der Name der Sitzung.
Transport	Der Netzwerktransport, der für die Verbindung verwendet werden soll. Gültige Transportoptionen sind: <b>TCP/IP, Seriell, SSH2</b> und <b>SSL</b> .
Verbindung	Die Verbindungsmethode, die verwendet werden soll. Erweiterte Verbindungseinstellungen können über die Schaltfläche konfiguriert werden.
Emulation	Emulationstypen sind: <b>hp70092, IBM 3151, IBM3270 Display, IBM3270 Printer, IBM5250 Display, IBM5250 Printer, MD Prism, TA6530, VT Series</b> und <b>Wyse</b> .

In der folgenden Tabelle werden die Einstellungen beschrieben, die im TeemTalk-Sitzungsassistenten in der Kategorie „Advanced Options“ (Erweiterte Optionen) verfügbar sind.

Option	Beschreibung
Emulationsdrucker	Die Druckereinstellungen für die HP TeemTalk-Emulation.
Automatische Anmeldung	Die Einstellungen für die automatische Anmeldung für HP TeemTalk.
Tastenmakros	Die Einstellungen der Tasten-Makros für HP TeemTalk.
Mausaktionen	Die Einstellungen für Mausaktionen für HP TeemTalk.
SoftButtons	Die Einstellungen der Soft-Tasten für HP TeemTalk.
Attribute	Die HP TeemTalk-Attributeinstellungen.
AUX-Anschlüsse	Die Einstellungen für zusätzliche Ports in HP TeemTalk.
Hotspots	Die Einstellungen für HP TeemTalk-Hotspots.

In der folgenden Tabelle werden die Einstellungen beschrieben, die im TeemTalk-Sitzungsassistenten in der Kategorie „Preferences“ (Einstellungen) verfügbar sind.

Option	Beschreibung
Verbundene Sitzung starten	Startet diese Sitzung verbunden.
Statusleiste anzeigen	Zeigt die Statusleiste für diese Verbindung an.

In der folgenden Tabelle werden die zusätzlichen Einstellungen beschrieben, die im TeemTalk-Sitzungsassistenten in der Kategorie „Preferences“ (Einstellungen) verfügbar sind.

Option	Beschreibung
Konfigurationsleiste anzeigen	Zeigt die Konfigurationsleiste an.
Aktuelle Fensterposition speichern	Speichert die aktuelle Größe und Position des Fensters, wenn Sie <b>Save Preferences</b> (Einstellungen speichern) auswählen. Das Fenster wird beim nächsten Systemstart wiederhergestellt.

Option	Beschreibung
	<b>HINWEIS:</b> Wählen Sie <b>Save Preferences</b> (Einstellungen speichern) bei jeder Änderung der Fenstergröße oder -position, um die neuen Werte zu speichern.
Im Vollbildmodus ausführen	Wählen Sie diese Option aus, damit das Fenster mit voller Bildschirmgröße angezeigt wird. Dies entfernt die Rahmen, die SoftButtons, das Menü und die Konfigurationsleisten.  <b>HINWEIS:</b> Diese Option wird erst beim nächsten Systemstart aktiviert und überschreibt die Optionen <b>Konfigurationsleiste anzeigen</b> und <b>Aktuelle Fensterposition speichern</b> .
Browserbefehl	Geben Sie den Befehl in das Feld ein, mit dem Ihr Internetbrowser ausgeführt wird, wie z. B. :  <code>/ display html links Firefox</code>
Startoptionen für Befehlszeile	Wird verwendet, um einen alternativen Speicherort für die Startoptionen anzugeben.  <b>HINWEIS:</b> Für spezifische Informationen über die HP TeemTalk Befehlszeilen-Startoptionen siehe <i>HP TeemTalk Terminal Emulator Benutzerhandbuch</i> .

## Advanced (Erweitert)

 **HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

## XDMCP

 **HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

## Configuration (Konfiguration)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer XDMCP-Verbindung in der Kategorie „Configuration“ (Konfiguration) verfügbar sind.

Option	Beschreibung
Name	Der Verbindungsname.
Typ	Der Typ der XDMCP-Verbindung. Gültige Optionen sind: <b>chooser</b> (Auswahlfunktion), <b>query</b> (Abfrage) und <b>broadcast</b> (Übertragung).
Adresse	Dieser Wert ist erforderlich, wenn der Wert für <b>Type</b> (Typ) auf <b>Query</b> (Abfrage) eingestellt ist.
Schriftartenserver verwenden	Anstelle der lokal installierten Schriftarten wird ein Remote-X-Fontserver für Schriftartenserver verwendet.
Schriftartenserver	„Font Server“ ist nur aktiviert, wenn die Option <b>Schriftartenserver verwenden</b> aktiviert ist.
Display konfigurieren	Wählen Sie diese Option, um die Anzeigekonfiguration für die Verbindung einzurichten. Wenn Sie keine Konfiguration festlegen, wird die Standardkonfiguration verwendet.

## Advanced (Erweitert)

 **HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

## SSH



**HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

### Configuration (Konfiguration)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer SSH-Verbindung in der Kategorie „Configuration“ (Konfiguration) verfügbar sind.

Option	Beschreibung
Name	Der Verbindungsname.
Adresse	Die IP-Adresse des Remote-Systems.
Port	Der Remote-Port, der für die Verbindung verwendet werden soll.
Benutzername	Der Benutzername, der für die Verbindung verwendet werden soll.
Anwendung ausführen	Die Anwendung, die zum Herstellen der Verbindung ausgeführt werden soll.
Komprimierung	Wählen Sie diese Option aus, wenn die zwischen dem Server und dem Thin Client gesendeten Daten komprimiert werden sollen.
X11 Verbindung leitet weiter	Wählen Sie diese Option aus, wenn auf dem Server ein X-Server aktiv ist, damit der Benutzer die Benutzeroberfläche in der SSH-Sitzung öffnen und lokal auf dem Thin Client anzeigen kann.
TTY Zuordnung erzwingen	Wählen Sie diese Option und geben Sie einen Befehl an, um eine temporäre Sitzung zu starten, die den Befehl ausführt. Sobald der Befehl ausgeführt wird, geht die Sitzung zu Ende. Wenn kein Befehl angegeben wird, wird die Sitzung normal ausgeführt, als wäre die Option nicht ausgewählt worden.
Vordergrundfarbe	Die Standardfarbe für den Text in der SSH-Sitzung.
Hintergrundfarbe	Die Standardfarbe für den Hintergrund in der SSH-Sitzung.
Schriftart	Gültige Optionen sind: <b>7X14, 5X7, 5X8, 6X9, 6X12, 7X13, 8X13, 8X16, 9X15, 10X20</b> und <b>12X24</b> .

### Advanced (Erweitert)



**HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

## Telnet



**HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

### Configuration (Konfiguration)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer Telnet-Verbindung in der Kategorie „Configuration“ (Konfiguration) verfügbar sind.

Option	Beschreibung
Name	Der Name der Verbindung.
Adresse	Die IP-Adresse des Remote-Systems.

Option	Beschreibung
Port	Der Port, der auf dem Remote-System verwendet werden soll.
Vordergrundfarbe	Die Vordergrundfarbe.
Hintergrundfarbe	Die Hintergrundfarbe.
Schriftart	Gültige Optionen sind: <b>7X14, 5X7, 5X8, 6X9, 6X12, 6X13, 7X13, 8X13, 8X16, 9X15, 10X20</b> und <b>12X24</b> .

## Advanced (Erweitert)



**HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

## Custom

Wenn Sie eine benutzerdefinierte Linux®-Anwendung installieren möchten, können Sie die Custom-Verbindung verwenden, um diese Anwendung über Connection Manager zu öffnen.



**HINWEIS:** Diese Einstellungen haben nur Auswirkungen auf die Verbindung, die Sie gerade konfigurieren.

## Configuration (Konfiguration)

In der folgenden Tabelle werden die Einstellungen beschrieben, die beim Bearbeiten einer Custom-Verbindung in der Kategorie „Configuration“ (Konfiguration) verfügbar sind.

Option	Beschreibung
Name	Der Verbindungsname.
Auszuführenden Befehl eingeben	Der Befehl, der zum Herstellen der Remote-Verbindung ausgeführt werden soll.

## Advanced (Erweitert)



**HINWEIS:** Informationen zu den beim Bearbeiten einer Verbindung in der Kategorie „Advanced“ (Erweitert) verfügbaren Einstellungen finden Sie unter [Erweiterte Verbindungseinstellungen auf Seite 8](#).

# 5 Systemsteuerung

Mit der Systemsteuerung können Sie die Systemkonfiguration ändern.



**HINWEIS:** Auf alle Elemente der Systemsteuerung kann im Administratormodus zugegriffen werden. Im Benutzermodus kann nur auf die Elemente der Systemsteuerung zugegriffen werden, die vom Administrator für die Verwendung durch den Benutzer aktiviert wurden.



**TIPP:** Um die Elemente der Systemsteuerung anzugeben, auf die Endbenutzer zugreifen dürfen, wählen Sie die Schaltfläche der Systemsteuerung und dann **Setup** und **Customization Center** (Anpassungszentrum). Aktivieren oder deaktivieren Sie dann Elemente in der Liste **Applications** (Anwendungen).

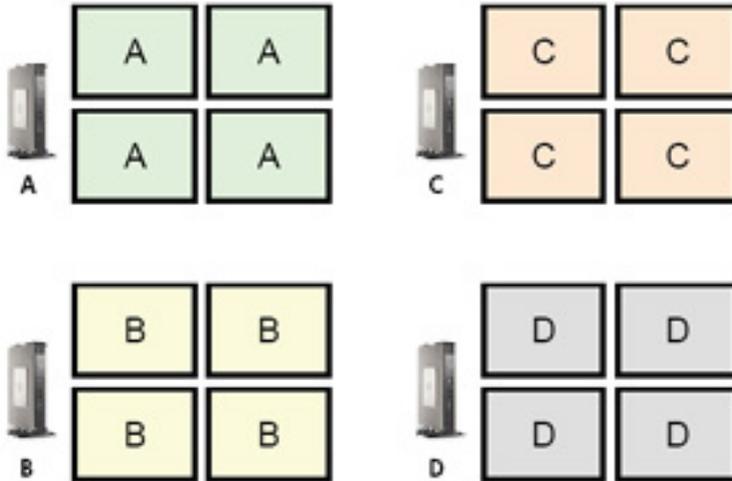
## Peripheriegeräte

Menüoption	Beschreibung
Clientaggregation	Zum Kombinieren von Thin Clients, um einen zusätzlichen Anzeigebereich zu erstellen.  Weitere Informationen finden Sie unter <a href="#">Clientaggregation auf Seite 43</a> .
Anzeige-Einstellungen	Ermöglicht das Konfigurieren und Testen von Optionen für eine primäre und sekundäre Anzeige.  Weitere Informationen finden Sie unter <a href="#">Anzeigeeinstellungen auf Seite 45</a> .
Tastaturlayout	Damit können Sie das Tastaturlayout ändern, um es der Sprache der Tastatur anzupassen.
Audio	Zur Stufenregelung von Audio-Wiedergabe und -Eingang.
Maus	Zum Konfigurieren der Mausgeschwindigkeit und der Mauseingabe für Rechtshänder oder Linkshänder.
Drucker	Zum Einrichten von lokalen und Netzwerkdruckern. Lokale Drucker können im Netzwerk gemeinsam genutzt werden.  Weitere Informationen finden Sie unter <a href="#">Konfigurieren von Druckern auf Seite 46</a> .
Touchscreen	Zum Konfigurieren der Touchscreen-Optionen.
USB Manager	Zum Konfigurieren der Umleitungsoptionen für USB-Geräte.  Weitere Informationen finden Sie unter <a href="#">USB-Geräte umleiten auf Seite 46</a> .
Einrichten der SCIM-Eingabemethode	Zum Konfigurieren der Smart Common Input Method (SCIM) für die Eingabe von Chinesisch, Japanisch und Koreanisch.  Weitere Informationen zu diesem Open-Source-Programm finden Sie unter <a href="http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page">http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page</a> .

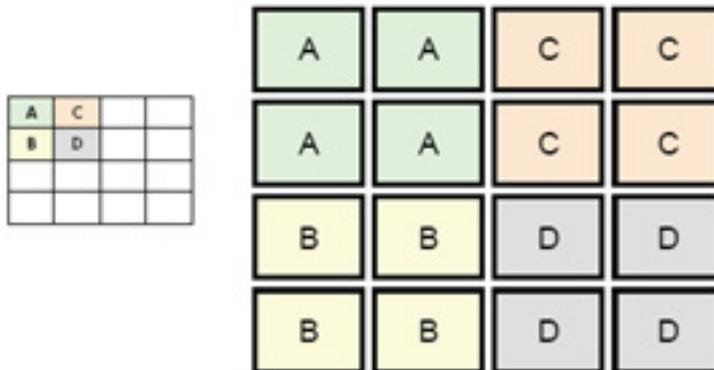
## Clientaggregation

HP ThinPro-basierte Thin Clients unterstützen je nach Hardwaremodell bis zu vier Monitore. Wenn Sie einen zusätzlichen Anzeigebereich benötigen, können mithilfe der Clientaggregation bis zu vier Thin Clients kombiniert werden, sodass es möglich ist, insgesamt 16 Monitore über eine einzige Tastatur und Maus ohne zusätzliche Hardware oder Software zu steuern.

Angenommen, Sie haben vier Thin Clients mit jeweils vier Monitoren, die in einem 2 x 2-Array konfiguriert wurden, wie unten gezeigt.

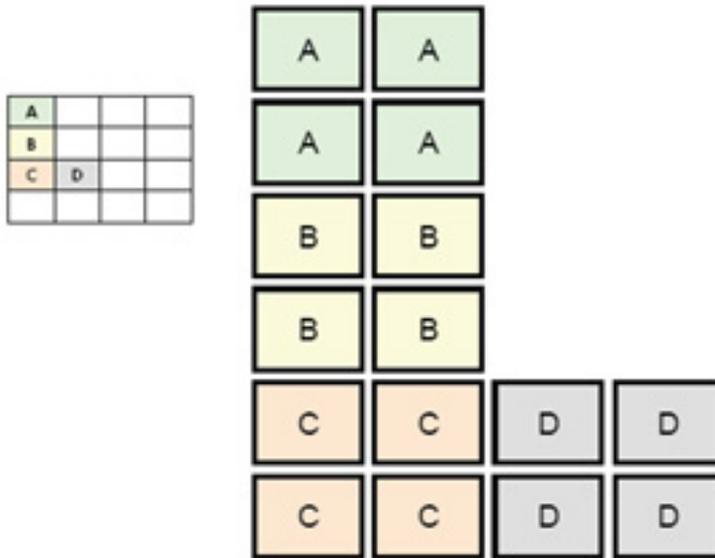


Mithilfe der Clientaggregation können Sie die vier Thin Clients in einem 4 x 4-Raster anordnen. Die folgende Abbildung zeigt eine der möglichen Anordnungen.



Beim Bewegen des Mauszeigers über die rechte Seite der Monitore für den Thin Client A hinaus, erscheint beispielsweise der Mauszeiger auf der linken Seite der Monitore für den Thin Client C. Gleichzeitig wird die Tastatureingabe vom Thin Client A an den Thin Client C umgeleitet.

Die folgende Abbildung zeigt eine weitere mögliche Anordnung.



Wenn Sie bei dieser Konfiguration den Mauszeiger über die rechte Seite der Monitore für den Thin Client A hinaus bewegen, erscheint dieser im oberen Drittel der linken Seite der Monitore für den Thin Client D. Wenn Sie bei dieser Konfiguration den Mauszeiger über die rechte Seite der Monitore für den Thin Client B hinaus bewegen, erscheint dieser im mittleren Drittel der linken Seite der Monitore für den Thin Client D. Wenn Sie schließlich bei dieser Konfiguration den Mauszeiger über die rechte Seite der Monitore für Thin Client C hinaus bewegen, erscheint dieser im unteren Drittel der linken Seite der Monitore für den Thin Client D.

**HINWEIS:** Desktop-Fenster können nicht über die Thin Clients hinweg ausgedehnt oder zwischen ihnen verschoben werden. In der Regel erstellt jeder Thin Client Fenster, die auf der jeweiligen Verbindung zum zugehörigen Remotecomputer basieren, und es sollte kein Bedarf bestehen, die Fenster zwischen den Thin Clients zu verschieben.

Der Thin Client, der physisch mit der Tastatur und der Maus verbunden ist, wird als Aggregation-Server bezeichnet. Die anderen Thin Clients werden als Aggregation-Clients bezeichnet. Wenn sich der Mauszeiger auf einem der Aggregation-Clients befindet, werden die Maus- und Tastatureingaben (vom Aggregation-Server) verschlüsselt und über das Netzwerk an diesen Aggregation-Client gesendet. Der Aggregation-Client entschlüsselt die Maus- und Tastatureingaben und leitet die Eingabedaten an den lokalen Desktop des Aggregation-Clients.

Die Clientaggregation basiert auf einem Open-Source-Softwarepaket mit der Bezeichnung Synergy und die Verschlüsselung erfolgt über ein Paket mit der Bezeichnung Stunnel.

## Konfigurieren der Clientaggregation

Die Konfiguration der Clientaggregation erfolgt in zwei Arbeitsschritten:

1. [Konfigurieren der Aggregation-Clients auf Seite 44](#)
2. [Konfigurieren des Aggregation-Servers auf Seite 45](#)

### Konfigurieren der Aggregation-Clients

Führen Sie diese Prozedur auf jedem der Aggregation-Clients aus:

1. Wählen Sie in der Systemsteuerung **Peripherals > Client Aggregation** (Peripheriegeräte > Clientaggregation).
2. Wählen Sie **Client** aus.

3. Geben Sie den Serverhostnamen oder die IP-Adresse des Aggregation-Servers in das Feld ein.
4. Wählen Sie **Apply** (Übernehmen).

### Konfigurieren des Aggregation-Servers

So konfigurieren Sie den Aggregation-Server:

1. Wählen Sie in der Systemsteuerung **Peripherals > Client Aggregation** (Peripheriegeräte > Clientaggregation).
2. Wählen Sie **Server**.
3. Der Aggregation-Server wird in einem blauen Feld angezeigt, das seinen Hostnamen enthält. Wählen Sie den Aggregation-Server und ziehen Sie ihn an die gewünschte Stelle im 4 x 4-Raster.
4. Wählen Sie die Stelle im 4 x 4-Raster, an der Sie den ersten Aggregation-Client platzieren möchten, geben Sie dessen Hostnamen oder IP-Adresse ein und drücken Sie dann die **Eingabetaste**. Der Aggregation-Client wird in einem grünen Feld angezeigt.
5. Fügen Sie bis zu zwei weitere Aggregation-Clients im 4 x 4-Raster hinzu, falls gewünscht.

Die Anordnung des Aggregation-Servers und der Aggregation-Clients im 4 x 4-Raster kann jederzeit geändert werden, indem Sie auf das entsprechende Kästchen klicken und es an eine neue Position ziehen.

Sobald die Aggregation-Clients und der Aggregation-Server konfiguriert wurden, versuchen sie automatisch, eine verschlüsselte Kommunikation miteinander einzurichten. Wählen Sie **Status**, um den Verbindungsstatus zwischen Computern anzuzeigen.

### Anzeigeeinstellungen

HP ThinPro ermöglicht das Erstellen von Profilen für Anzeigeeinstellungen und die Anwendung verschiedener Profile auf verschiedenen Monitoren. Ein Profil beinhaltet Auflösung, Bildwiederholungsrate, Bittiefe und Ausrichtung.

So konfigurieren Sie Anzeigepprofile:

1. Wählen Sie in der Systemsteuerung **Peripherals > Display Preferences** (Peripheriegeräte > Anzeigeeinstellungen).
2. Konfigurieren Sie die Optionen nach Bedarf und wählen Sie anschließend **Apply** (Übernehmen).



**HINWEIS:** Die Optionen können je nach Hardwaremodell abweichen.

Im Folgenden ein paar Tipps dazu, wann ein Anpassen der Anzeigepprofile nützlich sein kann:

- Einige Anwendungen erfordern unter Umständen eine bestimmte Auflösung oder Bittiefe, damit sie ordnungsgemäß funktionieren.
- Einige Anwendungen erfordern unter Umständen, dass das Display gedreht wird.
- Die Verwendung einer Farbtiefe von 16 Bit kann die Leistung der Citrix- und RDP-Verbindung verbessern, da weniger Daten über das Netzwerk oder an den Grafikchip gesendet werden.
- AMD-basierte Plattformen (t520, t620, t610) bieten nur 32-Bit-Farbtiefe. Die t505 und t510 bieten entweder 16-Bit- oder 32-Bit-Farbtiefe. In allen Fällen verwendet die 32-Bit-Farbtiefe tatsächlich 24 Bit.
- Ein Administrator möchte möglicherweise ein Anzeigeprofil als Standard festlegen, obwohl im Unternehmen viele verschiedene Monitore vorhanden sind.

## Konfigurieren von Druckern

So konfigurieren Sie einen Drucker:

1. Wählen Sie in der Systemsteuerung **Peripherals > Printers** (Peripheriegeräte > Drucker).
2. Wählen Sie im Dialogfeld **Printing** (Drucken) die Option **Add** (Hinzufügen).
3. Wählen Sie im Dialogfeld **New Printer** (Neuer Drucker) den Drucker, den Sie konfigurieren möchten, und wählen Sie dann **Forward** (Weiter).



**HINWEIS:** Wenn Sie einen seriellen Drucker wählen, gehen Sie sicher, dass Sie die richtigen Einstellungen auf der rechten Seite des Dialogfeldes eingeben, da der Drucker ansonsten möglicherweise nicht richtig funktioniert.

4. Wählen Sie das Fabrikat des Druckers. Wenn Sie nicht sicher sind, wählen Sie die Option **Generic (recommended)** (Allgemein (empfohlen)) und dann **Forward** (Weiter).
5. Wählen Sie das Modell und den Treiber für den Drucker und dann **Forward** (Weiter).



**HINWEIS:** Wenn Sie nicht sicher sind, welches Modell oder welchen Treiber Sie verwenden sollen, oder wenn das Modell Ihres Druckers nicht aufgeführt ist, wählen Sie **Back** (Zurück) und versuchen Sie es mit der Option **Generic (recommended)** (Allgemein (empfohlen)) für das Fabrikat des Druckers.

Stellen Sie bei Verwendung der Option **Generic (recommended)** (Allgemein (empfohlen)) sicher, dass Sie für das Modell **text-only (recommended)** (nur-Text (empfohlen)) auswählen, und für den Treiber **Generic text-only printer [en] (recommended)** (Allgemeiner nur-Text-Drucker [en] (empfohlen)) auswählen.

6. Geben Sie optionale Informationen zum Drucker ein, wie z. B. seinen Namen und Ort.



**HINWEIS:** HP empfiehlt, dass Sie den korrekten Treiber-Namen in das Feld **Windows Driver** (Windows Treiber) eingeben. Wenn bei einer Verbindungsherstellung zu einer Remote-Sitzung kein Treiber zugeordnet werden kann, verwendet Windows möglicherweise den falschen Treiber und das Drucken funktioniert nicht. Damit der Drucker ordnungsgemäß funktioniert, muss der Treiber auch auf dem Windows Server installiert werden.

7. Wählen Sie **Apply** (Übernehmen) und drucken Sie dann ggf. eine Testseite.

Wiederholen Sie diesen Vorgang, um bei Bedarf weitere Drucker zu konfigurieren.



**TIPP:** Das häufigste Problem ist, dass der falsche Treiber für den Drucker verwendet wird. Um den Treiber zu ändern, klicken Sie mit der rechten Maustaste auf den Drucker und wählen Sie **Properties** (Eigenschaften), und ändern Sie dann Fabrikat und Modell.

## USB-Geräte umleiten

So leiten Sie USB-Geräte um:

1. Wählen Sie in der Systemsteuerung **Peripherals > USB Manager** (Peripheriegeräte > USB-Manager).
2. Wählen Sie auf der Seite **Protocol** (Protokoll) ein Remote-Protokoll.

Wenn die Einstellung **Local** (Lokal) ist, können Sie auch die Optionen **allow devices to be mounted** (Bereitstellung von Geräten erlauben) und **mount devices read-only** (Geräte schreibgeschützt bereitstellen) angeben.

3. Auf der Seite **Devices** (Geräte) können Sie die Umleitungsoptionen für einzelne Geräte bei Bedarf aktivieren oder deaktivieren.

4. Auf der Seite **Classes** (Klassen) können Sie bestimmte Geräteklassen auswählen, die an Remotesitzungen umgeleitet werden sollen.
5. Wenn Sie fertig sind, wählen Sie **OK**.

## Setup

Menüoption	Beschreibung
Hintergrundeinstellungen	Zum Konfigurieren des Hintergrunddesigns und der dynamischen Anzeige von Systeminformationen (wie Hostname, IP-Adresse, Hardwaremodell und MAC-Adresse des Thin Clients) im Hintergrund.  Weitere Informationen finden Sie im HP ThinPro-Whitepaper <i>Login Screen Customization</i> (nur auf Englisch verfügbar).
Datum und Uhrzeit	Zum Konfigurieren der Zeitzone sowie der Datums- und Uhrzeitoptionen.
Sprache	Zum Anzeigen der HP ThinPro-Oberfläche in einer anderen Sprache.
Netzwerk	Zum Konfigurieren der Netzwerkeinstellungen.  Weitere Informationen finden Sie unter <a href="#">Netzwerkeinstellungen auf Seite 47</a> .
Energieverwaltung	Zum Konfigurieren von Energieverwaltungseinstellungen wie Bildschirmschoner sowie Einstellungen für die Deaktivierung der Anzeige und den Wechsel in den Standbymodus.
Sicherheit	Zum Festlegen und Ändern von Systemkennwörtern für den Thin Client-Administrator und -Benutzer.
Customization Center	Es stehen folgende Aktionen zur Verfügung: <ul style="list-style-type: none"> <li>• Wechseln zwischen den ThinPro- und Smart Zero-Konfigurationen</li> <li>• Konfigurieren der Desktop- und Taskleisten-Optionen</li> <li>• Auswählen der Verbindungstypen und Elemente der Systemsteuerung, auf die Endbenutzer zugreifen können</li> </ul> Weitere Informationen finden Sie unter <a href="#">Anpassungszentrum auf Seite 51</a> .

## Netzwerkeinstellungen

Netzwerkeinstellungen können mit dem Netzwerk Manager konfiguriert werden. So öffnen Sie den Netzwerkmanager:

- ▲ Wählen Sie in der Systemsteuerung **Setup > Network** (Setup > Netzwerk) aus.

In den folgenden Abschnitten finden Sie weitere Informationen über die verschiedenen Registerkarten im Netzwerkmanager:

- [Einstellungen für kabelgebundene Netzwerke](#)
- [WLAN-Einstellungen](#)
- [DNS-Einstellungen](#)

- [IPSec-Regeln](#)
- [Konfigurieren von VPN-Einstellungen](#)
- [Konfigurieren von HP Velocity](#)

## Einstellungen für kabelgebundene Netzwerke

Die folgende Tabelle beschreibt die im Netzwerkmanager unter der Registerkarte **Wired** (Kabelgebunden) verfügbaren Optionen.

Option	Beschreibung
(IPv6 aktivieren)	Aktiviert das IPv6. Standardmäßig wird IPv4 verwendet und es können nicht beide gleichzeitig verwendet werden.
Ethernet-Geschwindigkeit	Zum Festlegen der Ethernet-Geschwindigkeit. Wenn Ihre Switch oder Hub nicht über eine spezielle Anforderung verfügt, lassen Sie dies auf der Standardeinstellung <b>Automatic</b> (Automatisch).
Verbindungsmethode	Zur Auswahl zwischen <b>Automatic</b> (Automatisch) und <b>Static</b> (Statisch). Wenn Ihre Netzwerkumgebung DHCP verwendet, sollte die Option <b>Automatic</b> (Automatisch) ohne weitere Konfigurationen funktionieren.  Wenn <b>Static</b> (Statisch) ausgewählt ist, werden die Einstellungen für <b>Static Address Configuration</b> (Statische Adressenkonfiguration) zur Verfügung stehen. Vergewissern Sie sich, dass Sie diese Werte dementsprechend eingeben, ob Sie IPv4 oder IPv6 verwenden.
MTU	Ermöglicht die Eingabe der maximalen Übertragungseinheit (in Byte ).
Sicherheitseinstellungen	Zum Festlegen der Authentifizierungseinstellung auf eine der folgenden Optionen: <ul style="list-style-type: none"> <li>• None (Keine)</li> <li>• 802.1X-TTLS</li> <li>• 802.1X-PEAP</li> <li>• 802.1X-TLS</li> </ul> Beachten Sie Folgendes über TTLS und PEAP: <ul style="list-style-type: none"> <li>• Die Einstellung der Option <b>Inner Authentication</b> (Innere Authentifizierung) sollte auf das eingestellt werden, was Ihr Server unterstützt.</li> <li>• Die Einstellung <b>CA Certificate</b> (CA-Zertifikat) sollte auf das Zertifikat des Servers auf dem lokalen Thin Client verweisen.</li> <li>• <b>Username</b> (Benutzername) und <b>Password</b> (Kennwort) sind die Anmeldeinformationen des Benutzers.</li> </ul> Beachten Sie Folgendes über TLS: <ul style="list-style-type: none"> <li>• Die Einstellung <b>CA Certificate</b> (CA-Zertifikat) sollte auf das Zertifikat des Servers auf dem lokalen Thin Client verweisen.</li> <li>• Wenn Ihre Datei für den <b>Private Key</b> (Privater Schlüssel) .p12 oder .pfx ist, kann die Einstellung <b>User Certificate</b> (Benutzerzertifikat) leer bleiben.</li> <li>• Die Einstellung der <b>Identity</b> (Identität) sollte der Benutzername sein, der dem Benutzerzertifikat entspricht.</li> <li>• Die Einstellung des <b>Private Key Password</b> (Privates Schlüsselkennwort) ist das Kennwort der privaten Schlüsseldatei des Benutzers.</li> </ul>

## WLAN-E instellungen

Die folgende Tabelle beschreibt die im Netzwerkmanager auf der Registerkarte **Wireless** (Drahtlos) verfügbaren Optionen.



**HINWEIS:** Diese Registerkarte ist nur verfügbar, wenn der Thin Client einen Wireless-Adapter hat.

Option	Beschreibung
AP scannen	Sucht nach verfügbaren WLANs.
SSID	Verwenden Sie dieses Kontrollkästchen, um die SSID des WLAN manuell einzugeben, wenn sie beim Scan nicht erkannt wurde.
SSID ausgeblendet	Aktivieren Sie diese Option, wenn die SSID des WLAN auf „Ausgeblendet“ eingestellt ist (nicht übermitteln).
IPv6 aktivieren	Aktiviert das IPv6. Standardmäßig wird IPv4 verwendet und es können nicht beide gleichzeitig verwendet werden.
Energieverwaltung aktivieren	Aktiviert die Energieverwaltungsfunktion für den Wireless-Adapter.
Verbindungsmethode	<p>Zur Auswahl zwischen <b>Automatic</b> (Automatisch) und <b>Static</b> (Statisch). Wenn Ihre Netzwerkumgebung DHCP verwendet wird, sollte die Option <b>Automatic</b> (Automatisch) ohne weitere Konfigurationen funktionieren.</p> <p>Wenn <b>Static</b> (Statisch) ausgewählt ist, werden die Einstellungen für <b>Static Address Configuration</b> (Statische Adressenkonfiguration) zur Verfügung stehen. Vergewissern Sie sich, dass Sie diese Werte dementsprechend eingeben, ob Sie IPv4 oder IPv6 verwenden.</p>
Sicherheitseinstellungen	<p>Zum Festlegen der Authentifizierungseinstellung auf eine der folgenden Optionen:</p> <ul style="list-style-type: none"><li>• None (Keine)</li><li>• WEP</li><li>• WPA/WPA2-PSK</li><li>• 802.1X-TTLS</li><li>• 802.1X-PEAP</li><li>• 802.1X-TLS</li><li>• EAP FAST</li></ul> <p>Für WEP und WPA/WPA2-PSK müssen Sie nur den Netzwerkschlüssel eingeben und <b>OK</b> auswählen.</p> <p>Stellen Sie für EAP-FAST <b>Anonymous Identity</b> (Anonyme Identität), <b>Username</b> (Benutzername), <b>Password</b> (Kennwort) und <b>Provisioning Method</b> (Bereitstellungsmethode) ein. Die Einstellungen der PAC-Datei müssen Sie nicht ändern.</p> <p>Weitere Informationen über TTLS, PEAP und TLS finden Sie unter <a href="#">Einstellungen für kabelgebundene Netzwerke auf Seite 48</a>.</p>

## DNS-Einstellungen

Die folgende Tabelle beschreibt die im Netzwerkmanager unter der Registerkarte **DNS** verfügbaren Optionen.

Option	Beschreibung
Hostname	Dieser wird entsprechend der MAC-Adresse des Thin Client automatisch generiert. Alternativ können Sie auch einen benutzerdefinierten Hostnamen festlegen.
DNS-Server	Verwenden Sie dieses Feld, um benutzerdefinierte Informationen des DNS-Servers festzulegen.

Option	Beschreibung
Suchbereiche	Verwenden Sie dieses Feld, um die Domänen zu beschränken, die durchsucht werden.
HTTP-Proxy	Verwenden Sie diese Felder, um Proxy-Server-Informationen im folgenden Format einzugeben:
FTP-Proxy	<code>http://Proxyserver:Port</code>
HTTPS-Proxy	HP empfiehlt das Präfix <code>http://</code> für alle drei Proxy-Einstellungen zu verwenden, da es besser unterstützt wird.
	<b>HINWEIS:</b> Die Proxy-Einstellungen sind auf die Umgebungsvariablen <b>http_proxy</b> , <b>ftp_proxy</b> und <b>https_proxy</b> für das System eingestellt.

## IPSec-Regeln

Verwenden Sie diese Registerkarte zum Hinzufügen, Bearbeiten und Löschen von IPSec-Regeln. Eine IPSec-Regel sollte für jedes System identisch sein, das IPSec verwendet, um zu kommunizieren.

Verwenden Sie zum Konfigurieren einer IPSec-Regel die Registerkarte **General** (Allgemein), um Informationen, Adressen und Authentifizierungsmethode für die Regel festzulegen. Die **Source Address** (Quelladresse) ist die IP-Adresse des Thin Client und die Zieladresse ist die IP-Adresse des Systems, mit dem der Thin Client kommunizieren wird.



**HINWEIS:** Es werden nur die Authentifizierungstypen **PSK** und **Certificate** (Zertifikat) unterstützt. Die Kerberos-Authentifizierung wird nicht unterstützt.

Verwenden Sie die Registerkarte **Tunnel**, um Einstellungen für den Tunnelmodus zu konfigurieren.

Verwenden Sie die Registerkarten **Phase I** und **Phase II**, um verbesserte Sicherheitseinstellungen zu konfigurieren. Die Einstellungen sollte für alle Peer-Systeme identisch sein, die miteinander kommunizieren.



**HINWEIS:** Eine IPSec-Regel kann auch verwendet werden, um mit einem Windows Computer zu kommunizieren.

## Konfigurieren von VPN-Einstellungen

HP ThinPro unterstützt zwei Arten von VPN:

- Cisco
- PPTP

Aktivieren Sie die Option **Auto Start** (Automatisch starten), um das VPN automatisch zu starten.

Beachten Sie Folgendes über die Erstellung einer VPN unter Verwendung von Cisco:

- Das **Gateway** ist die IP-Adresse oder der Hostname des Gateway.
- Der **Group name** (Gruppenname) und das **Group password** (Kennwort der Gruppe) sind die IPSec-ID und das IPSec-Kennwort.
- Die Einstellung der **Domain** (Domäne) ist optional.
- Der **User name** (Benutzername) und das **User password** (Benutzerkennwort) sind die Benutzeranmeldeinformationen, die Rechte zum Erstellen einer VPN-Verbindung auf der Serverseite besitzen.
- Der **Security Type** (Sicherheitstyp) sollte identisch eingestellt werden wie auf der Serverseite.
- Die Option **NAT Traversal** (NAT-Traversal) sollte abhängig von Ihrer VPN-Umgebung festgelegt werden.

- Mit der Option **IKE DH Group** (IKE DH-Gruppe) wird die für das VPN zu verwendende Diffie-Hellman-Gruppe festgelegt.
- Mit der Option **PFS Type** (PFS-Typ) wird die für Perfect Forward Secrecy zu verwendende Diffie-Hellman-Gruppe festgelegt.

Beachten Sie Folgendes über die Erstellung einer VPN unter Verwendung von PPTP:

- Das **Gateway** ist die IP-Adresse oder der Hostname des Gateway.
- Die Einstellung der **NT Domain** (NT-Domäne) ist optional.
- Der **User name** (Benutzername) und das **User password** (Benutzerkennwort) sind die Benutzeranmeldeinformationen, die Rechte zum Erstellen einer VPN-Verbindung auf der Serverseite besitzen.

## Konfigurieren von HP Velocity

Verwenden Sie die Registerkarte **HP Velocity**, um HP Velocity-Einstellungen zu konfigurieren. Weitere Informationen zu den HP Velocity-Modi finden Sie auf der Website <http://www.hp.com/go/velocity>.

## Anpassungscenter

So öffnen Sie das Anpassungscenter:

- ▲ Wählen Sie in der Systemsteuerung **Setup > Customization Center** (Setup > Anpassungscenter).

Die Schaltfläche am oberen Rand der **Desktop**-Seite kann verwendet werden, um zwischen ThinPro- und Smart Zero-Konfigurationen zu wechseln. Siehe [Auswählen einer Betriebssystemkonfiguration auf Seite 2](#) für weitere Informationen zu den Unterschieden zwischen den beiden Konfigurationen.



**HINWEIS:** Wenn Sie eine einzige Verbindung konfiguriert haben und von ThinPro zu Smart Zero wechseln, wird diese Verbindung automatisch als Smart Zero-Verbindung verwendet. Wenn Sie mehrere Verbindungen konfiguriert haben, werden Sie aufgefordert, die zu verwendende Verbindung auszuwählen.

Die folgende Tabelle beschreibt die übrigen verfügbaren Optionen auf der **Desktop**-Seite.

Option	Beschreibung
Beim Start den Connection Manager starten	Wenn aktiviert, wird Connection Manager beim Systemstart automatisch gestartet.
Kontextmenü aktivieren	Deaktivieren Sie diese Option, um das Kontextmenü zu deaktivieren, das angezeigt wird, wenn Sie mit der rechten Maustaste auf den Desktop klicken.
Benutzer erlauben, in den Administratormodus zu wechseln	Deaktivieren Sie diese Option, um die Option <b>Administrator/User Mode Switch</b> (Wechsel zwischen Administrator-/Benutzermodus) in der Systemsteuerung im Benutzermodus zu entfernen.
Kennwortschaltfläche anzeigen	Wenn aktiviert, ist die Option <b>Show password</b> (Kennwort anzeigen) im Anmeldedialogfeld für Administratoren verfügbar.
Zugriffssteuerungssicherheit für X-Host aktivieren	Wenn aktiviert, dürfen nur die Systeme, die im Bereich <b>XHost Access Control List</b> (X-Host-Zugriffskontrollliste) aufgeführt werden, den Thin Client über Fernzugriff steuern.
USB-Update aktivieren	Ermöglicht die Installation von Updates über ein USB-Flash-Laufwerk. Weitere Informationen finden Sie unter „ <a href="#">USB-Updates</a> “ auf Seite 76.
USB-Update authentifizieren	Deaktivieren Sie diese Option, um Endbenutzern die Installation von Updates über USB zu erlauben.

Verwenden Sie die Seiten **Connections** (Verbindungen) und **Applications** (Anwendungen), um auszuwählen, welche Verbindungstypen und Anwendungen der Systemsteuerung im Benutzermodus verfügbar sind.

Verwenden Sie die Seite **Taskbar** (Taskleiste), um die Taskleiste zu konfigurieren.

## Verwaltung

Menüoption	Beschreibung
AD/DDNS Manager	<p>Zum Hinzufügen des Thin Client zu einer Organisationseinheit des Active Directory-Servers und zur Aktivierung automatischer Dynamic DNS-Updates der Zuordnung von Namen und IP-Adresse des Thin Client.</p> <p><b>HINWEIS:</b> Dieses Tool aktiviert die Authentifizierung mit der Active Directory-Datenbank nicht.</p>
HPDM Agent	<p>Zum Konfigurieren des HP Device Manager (HPDM) Agent.</p> <p>Weitere Informationen finden Sie im <i>Administratorhandbuch</i> für HPDM.</p>
Automatische Updates	<p>Damit können Sie den Automatic Update-Server manuell zurücksetzen.</p> <p>Weitere Informationen finden Sie unter „<a href="#">HP Smart Client Services</a>“ auf Seite 62.</p>
Komponenten-Manager	<p>Zum Entfernen von Systemkomponenten.</p> <p>Weitere Informationen finden Sie unter <a href="#">Komponenten-Manager</a> auf Seite 53.</p>
Easy Update	<p>Öffnet den Easy Update-Assistenten. Easy Update ist eine Komponente von HP Easy Tools, mit der Sie die neuesten Softwareupdates für den Thin Client installieren können.</p> <p><b>TIPP:</b> Wenn Sie bei der Durchführung eines Image-Updates <b>Thin Client-Konfiguration beibehalten</b> auswählen, werden alle zuvor konfigurierten Einstellungen beibehalten.</p> <p>Weitere Informationen über HP Easy Tools finden Sie im <i>Administratorhandbuch</i> für HP Easy Tools.</p>
Werkseinstellungen	<p>Zum Wiederherstellen der Standard-Werkseinstellungen des Thin Client.</p>
Snapshots	<p>Zum Wiederherstellen eines früheren Zustands oder der Standard-Werkseinstellungen des Thin Client.</p>
SSHD-Manager	<p>Ermöglicht den Zugriff über eine Secure Shell.</p>
ThinState	<p>Mit HP ThinState kann entweder das gesamte Betriebssystem-Image oder nur seine Konfigurationseinstellungen kopiert oder wiederhergestellt werden.</p> <p>Weitere Informationen finden Sie unter <a href="#">HP ThinState</a> auf Seite 54.</p>
VNC-Shadow	<p>Zum Konfigurieren von VNC-Shadowing-Optionen.</p> <p>Weitere Informationen finden Sie unter <a href="#">VNC-Shadowing</a> auf Seite 57.</p>
Wireless-Statistiken	<p>Zum Anzeigen von Informationen zu WLAN-Access Points.</p>

## Komponenten-Manager

Mit dem Komponenten-Manager können Sie Systemkomponenten entfernen, die in Ihrer Umgebung nicht verwendet werden. Dies kann zum Verringern der Image-Größe wünschenswert sein. Wenn in Ihrer Umgebung beispielsweise keine Citrix-Verbindungen verwendet werden, sollten Sie die Citrix-Komponente entfernen.

Wenn Komponenten entfernt wurden, kann die neue Konfiguration getestet werden, bevor Sie die Änderungen dauerhaft übernehmen. Sie können vorgenommene Änderungen auch rückgängig machen, wenn die Änderungen noch nicht dauerhaft angewendet wurden.

---

 **WICHTIG:** Nachdem die neue Konfiguration dauerhaft angewendet wurde, werden alle Schnappschüsse entfernt und ein neuer Schnappschuss der Werkseinstellungen wird erstellt. Jetzt können entfernte Komponenten nicht mehr wiederhergestellt werden.

---

So öffnen Sie den Komponenten-Manager:

- ▲ Wählen Sie in der Systemsteuerung **Management > Component Manager** (Verwaltung > Komponenten-Manager).

## Entfernen von Komponenten

So entfernen Sie Komponenten:

1. Wählen Sie im Komponenten-Manager die gewünschten Komponenten aus.

---

 **TIPP:** Um mehrere Komponenten auszuwählen, verwenden Sie **Strg** oder die **Umschalttaste**.

---

2. Wählen Sie **Remove Component(s)** (Komponenten entfernen) aus.
3. Wenn das Bestätigungsdiaologfeld erscheint, wählen Sie **OK** aus.
4. Nachdem die Komponenten entfernt wurden, testen Sie die neue Konfiguration.

## Rückgängigmachen einer Änderung

Sie können alle Änderungen nacheinander rückgängig machen, wenn die Änderungen noch nicht dauerhaft angewendet wurden. Nach jeder rückgängig gemachten Änderung ist ein Neustart des Thin Client erforderlich.

So machen Sie eine Änderung mit dem Komponenten-Manager rückgängig:

1. Wählen Sie im Komponenten-Manager **Revert Last Change** (Letzte Änderung rückgängig machen) aus.
2. Klicken Sie auf **Ja**, um den Thin Client neu zu starten.

Wiederholen Sie diesen Vorgang für alle Änderungen, die Sie rückgängig machen möchten.

---

 **WICHTIG:** Wenn Sie einen Schnappschuss des Images erstellen, während Sie eine neue Konfiguration testen, können Sie die Änderungen nicht über den Komponenten-Manager rückgängig machen. Diese Änderungen können nur durch das Wiederherstellen eines früheren Schnappschusses über das Tool für Schnappschüsse rückgängig gemacht werden. Dies ist jedoch nicht möglich, wenn die Änderungen bereits dauerhaft angewendet wurden, da diese Funktion alle vorhandenen Schnappschüsse löscht. Wenn Änderungen bereits dauerhaft angewendet wurden, müssen Sie das Betriebssystem neu installieren, um die meisten entfernten Komponenten wiederherzustellen. Einige Komponenten (z. B. Citrix, RDP und VMware Horizon View) können als Add-ons im Internet verfügbar sein und durch eine Neuinstallation wiederhergestellt werden.

---

## Dauerhaftes Anwenden der Änderungen

So wenden Sie mit dem Komponenten-Manager vorgenommene Änderungen dauerhaft an:



---

**WICHTIG:** Nachdem die neue Konfiguration dauerhaft angewendet wurde, werden alle Schnappschüsse entfernt und ein neuer Schnappschuss der Werkseinstellungen wird erstellt. Jetzt können entfernte Komponenten nicht mehr wiederhergestellt werden.

---

1. Wählen Sie im Komponenten-Manager **Apply Component Configuration** (Komponentenkonfiguration anwenden) aus.
2. Wählen Sie **Yes** (Ja).

## HP ThinState

HP ThinState ermöglicht Ihnen das Aufzeichnen und Bereitstellen eines HP ThinPro-Images oder der Konfiguration (Profil) auf einem anderen Thin Client eines kompatiblen Modells mit kompatibler Hardware.

### Verwalten von HP ThinPro-Images

#### Aufzeichnung von HP ThinPro-Images auf einem FTP-Server

So zeichnen Sie ein HP ThinPro-Image auf einem FTP-Server auf:



---

**WICHTIG:** Das Verzeichnis auf dem FTP-Server, in dem Sie das aufgezeichnete Image speichern möchten, muss bereits vorhanden sein, bevor Sie mit der Aufzeichnung beginnen.

---

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie das **HP ThinPro-Image** und anschließend **Next** (Weiter).
3. Wählen Sie **make a copy of the HP ThinPro image** (HP ThinPro-Image kopieren) und anschließend **Next** (Weiter).
4. Wählen Sie **a FTP server** (Einen FTP-Server) und anschließend **Next** (Weiter).
5. Geben Sie die FTP-Server-Informationen in die Felder ein.



---

**HINWEIS:** Die Image-Datei wird standardmäßig nach dem Hostnamen des Thin Client benannt.

---

Wählen Sie **Compress the image** (Image komprimieren), wenn Sie möchten, dass das aufgezeichnete Image komprimiert wird.



---

**HINWEIS:** HP ThinPro-Image-Datei ist ein einfaches Disk-Dump. Die unkomprimierte Größe beträgt etwa 1 GB und ein komprimiertes Image ohne Add-ons hat ungefähr 500 MB.

---

6. Wählen Sie **Finish** (Fertig stellen).

Wenn die Image-Aufzeichnung beginnt, werden alle Anwendungen beendet und es erscheint ein neues Fenster, das den Fortschritt anzeigt. Wenn ein Problem auftritt, wählen Sie **Details**, um weitere Informationen zu erhalten. Der Desktop wird wieder aktiviert, nachdem die Aufzeichnung abgeschlossen ist.

#### Bereitstellung eines HP ThinPro-Images über FTP oder HTTP



---

**WICHTIG:** Wenn Sie eine Bereitstellung abbrechen, wird das vorherige Image nicht wiederhergestellt und der Inhalt des Thin Client-Flash-Laufwerks wird beschädigt.

---

So stellen Sie ein HP ThinPro-Image über FTP oder HTTP bereit:

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie das **HP ThinPro-Image** und anschließend **Next** (Weiter).

3. Wählen Sie **restore an HP ThinPro image** (HP ThinPro-Image wiederherstellen) und anschließend **Next** (Weiter).
4. Wählen Sie entweder das FTP- oder das HTTP-Protokoll und geben Sie die Informationen zum Server in die Felder ein.



**HINWEIS:** Die Felder **Username** (Benutzername) und **Password** (Kennwort) sind nicht erforderlich, wenn Sie das HTTP-Protokoll verwenden.

5. Wählen Sie **Retain HP ThinPro Configuration** (HP ThinPro-Konfiguration beibehalten), wenn Sie alle zuvor konfigurierten Einstellungen beibehalten möchten.
6. Wählen Sie **Finish** (Fertig stellen).

Wenn die Image-Bereitstellung beginnt, werden alle Anwendungen beendet und es erscheint ein neues Fenster, das den Fortschritt anzeigt. Wenn ein Problem auftritt, wählen Sie **Details**, um weitere Informationen zu erhalten. Der Desktop wird wieder aktiviert, nachdem die Bereitstellung abgeschlossen ist.



**HINWEIS:** Eine MD5-Prüfsumme wird nur dann berechnet, wenn die MD5-Datei auf dem Server vorhanden ist.

### Aufzeichnen eines HP ThinPro-Images auf einem USB-Flash-Laufwerk

So zeichnen Sie ein HP ThinPro-Image auf einem USB-Flash-Laufwerk auf:



**WICHTIG:** Machen Sie eine Sicherungskopie aller Daten, die auf dem USB-Flash-Laufwerk vorhanden sind, bevor Sie beginnen. HP ThinState formatiert automatisch das Flash-Laufwerk, um ein bootfähiges USB-Flash-Laufwerk zu erstellen. Dieser Vorgang löscht alle Daten, die derzeit auf dem Flash-Laufwerk vorhanden sind.

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie das **HP ThinPro-Image** und anschließend **Next** (Weiter).
3. Wählen Sie **make a copy of the HP ThinPro image** (HP ThinPro-Image kopieren) und anschließend **Next** (Weiter).
4. Wählen Sie **create a bootable USB flash drive** (Bootfähiges USB-Flash-Laufwerk erstellen) und anschließend **Next** (Weiter).

Der Thin Client wird neu gestartet und Sie werden dann aufgefordert, ein USB-Flash-Laufwerk anzuschließen.

5. Schließen Sie ein USB-Flash-Laufwerk an einen USB-Anschluss am Thin Client an.
6. Wählen Sie das USB-Flash-Laufwerk und anschließend **Finish** (Fertig stellen).

Ein neues Fenster zeigt den Fortschritt an. Wenn ein Problem auftritt, wählen Sie **Details**, um weitere Informationen zu erhalten. Der Desktop wird wieder aktiviert, nachdem die Aufzeichnung abgeschlossen ist.

### Bereitstellung eines HP ThinPro-Images mit einem USB-Flash-Laufwerk

So stellen Sie ein HP ThinPro-Image mit einem USB-Flash-Laufwerk bereit:



**WICHTIG:** Wenn Sie eine Bereitstellung abbrechen, wird das vorherige Image nicht wiederhergestellt und der Inhalt des Thin Client-Flash-Laufwerks wird beschädigt. In diesem Zustand muss für den Thin Client über ein USB-Flash-Laufwerk ein neues Image erstellt werden.

1. Schalten Sie den Ziel-Thin Client aus.
2. Setzen Sie ein USB-Flash-Laufwerk ein.
3. Schalten Sie den Thin Client ein.



**HINWEIS:** Der Bildschirm bleibt für 10 bis 15 Sekunden schwarz, während der Thin Client das USB-Flash-Laufwerk erkennt und über das USB-Flash-Laufwerk startet. Wenn der Thin Client nicht über das USB-Flash-Laufwerk startet, stecken Sie alle anderen USB-Geräte aus und wiederholen Sie das Verfahren.

## Verwalten eines Clientprofils

Ein Clientprofil enthält die Verbindungen, die Einstellungen und die Anpassungen, die mit Connection Manager und der Systemsteuerung konfiguriert wurden. Ein Profil wird in einer Konfigurationsdatei gespeichert, die nur für die Version des HP ThinPro geeignet ist, in der sie erstellt wurde.



**HINWEIS:** Ein Clientprofil kann auch mit Profile Editor und Automatic Update vorkonfiguriert und bereitgestellt werden (weitere Informationen finden Sie unter [„Profile Editor“ auf Seite 67](#) und [„HP Smart Client Services“ auf Seite 62](#)).

## Speichern eines Clientprofils auf einem FTP-Server

So speichern Sie ein Clientprofil auf einem FTP-Server:



**WICHTIG:** Das Verzeichnis auf dem FTP-Server, in dem Sie die Konfiguration speichern möchten, muss bereits vorhanden sein, bevor Sie mit dem Speichervorgang beginnen.

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie die **HP ThinPro-Konfiguration** und anschließend **Next** (Weiter).
3. Wählen Sie **save the configuration** (Konfiguration speichern) und anschließend **Next** (Weiter).
4. Wählen Sie **on a FTP server** (Auf einem FTP-Server) und anschließend **Next** (Weiter).
5. Geben Sie die FTP-Server-Informationen in die Felder ein.
6. Wählen Sie **Finish** (Fertig stellen).

## Wiederherstellen eines Clientprofils über FTP oder HTTP

So stellen Sie ein Clientprofil über FTP oder HTTP wieder her:

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie die **HP ThinPro-Konfiguration** und anschließend **Next** (Weiter).
3. Wählen Sie **restore a configuration** (Konfiguration wiederherstellen) und anschließend **Next** (Weiter).
4. Wählen Sie **on a remote server** (Auf einem Remoteserver) und anschließend **Next** (Weiter).
5. Wählen Sie entweder das FTP- oder das HTTP-Protokoll und geben Sie die Informationen zum Server in die Felder ein.



**HINWEIS:** Die Felder **Username** (Benutzername) und **Password** (Kennwort) sind nicht erforderlich, wenn Sie das HTTP-Protokoll verwenden.

6. Wählen Sie **Finish** (Fertig stellen).

## Speichern eines Clientprofils auf einem USB-Flash-Laufwerk

So speichern Sie ein Clientprofil auf einem USB-Flash-Laufwerk:

1. Schließen Sie ein USB-Flash-Laufwerk an einen USB-Anschluss am Thin Client an.
2. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
3. Wählen Sie die **HP ThinPro-Konfiguration** und anschließend **Next** (Weiter).
4. Wählen Sie **save the configuration** (Konfiguration speichern) und anschließend **Next** (Weiter).
5. Wählen Sie **on a USB key** (Auf einem USB-Stick) und anschließend **Next** (Weiter).
6. Wählen Sie ein USB-Flash-Laufwerk aus.
7. Wählen Sie **Durchsuchen**.
8. Navigieren Sie zu dem gewünschten Speicherort auf dem USB-Flash-Laufwerk und weisen Sie dem Profil einen Dateinamen zu.
9. Wählen Sie **Speichern**.
10. Wählen Sie **Finish** (Fertig stellen).

## Wiederherstellen eines Clientprofils von einem USB-Flash-Laufwerk

So stellen Sie ein Clientprofil von einem USB-Flash-Laufwerk wieder her:

1. Schließen Sie das USB-Flash-Laufwerk, das die Konfigurationsdatei enthält, an einen USB-Anschluss am Ziel-Thin Client an.
2. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
3. Wählen Sie die **HP ThinPro-Konfiguration** und anschließend **Next** (Weiter).
4. Wählen Sie **restore a configuration** (Konfiguration wiederherstellen) und anschließend **Next** (Weiter).
5. Wählen Sie **on a USB key** (Auf einem USB-Stick) und anschließend **Next** (Weiter).
6. Wählen Sie den USB-Stick aus.
7. Wählen Sie **Durchsuchen**.
8. Doppelklicken Sie auf die gewünschte Konfigurationsdatei auf dem USB-Stick.
9. Wählen Sie **Finish** (Fertig stellen).

## VNC-Shadowing

Virtual Network Computing (VNC) ist ein Remote-Desktop-Protokoll, mit dem Sie den Desktop eines Remote-Computers sehen und auch mit Ihrer lokalen Maus und Tastatur steuern können.

So greifen Sie auf das VNC Shadow-Tool zu:

- ▲ Wählen Sie in der Systemsteuerung **Verwaltung > VNC-Shadow** aus.



**HINWEIS:** Der Thin Client muss neu gestartet werden, bevor Änderungen an den VNC-Shadowing-Optionen wirksam werden.

Die folgende Tabelle beschreibt die Optionen, die im VNC Shadow-Tool verfügbar sind.

Option	Beschreibung
VNC-Shadow aktivieren	Ermöglicht das VNC-Shadowing.

Option	Beschreibung
VNC Schreibgeschützt	Öffnet die VNC-Sitzung als schreibgeschützt.
VNC: Kennwort verwenden	Macht beim Zugriff auf den Thin Client über VNC ein Kennwort erforderlich. Wählen Sie <b>Set Password</b> (Kennwort festlegen), um das Kennwort festzulegen.
VNC: Benutzer benachrichtigen, um Ablehnung zuzulassen	Ermöglicht ein Benachrichtigungs-Dialogfeld auf dem Remote-System, das den Remote-Benutzer informiert, wenn jemand versucht eine Verbindung über VNC herzustellen. Der Benutzer kann den Zugriff entweder zulassen oder verweigern.
VNC-Zeitlimit für Benachrichtigung anzeigen	Legt die Dauer der Anzeige des Benachrichtigungs-Dialogfelds in Sekunden fest.
Benutzerbenachrichtigung	Ermöglicht Ihnen, eine Nachricht im Dialogfeld für die Benachrichtigung an den Remote-Benutzer anzuzeigen.
Verbindungen standardmäßig verweigern	Wenn aktiviert, wird die VNC-Verbindung standardmäßig verweigert, sobald die Zeit abgelaufen ist.
VNC-Server jetzt zurücksetzen	Setzt den VNC-Server zurück, nachdem die neuen Einstellungen angewendet wurden.

## Advanced (Erweitert)

Menüoption	Beschreibung
Zertifikate	Öffnet den Zertifikat-Manager, mit dem man ganz einfach Zertifikate importieren, anzeigen oder entfernen kann.  Weitere Informationen finden Sie unter <a href="#">Zertifikat-Manager auf Seite 59</a> .
Prozessormanager	Zur Auswahl der Prozessorleistung zwischen <b>Balanced</b> (Ausgeglichen) und <b>High Performance</b> .
DHCP-Optionen	Zum Konfigurieren der DHCP-Optionen.  Weitere Informationen finden Sie unter <a href="#">DHCP-Optionen auf Seite 59</a> .
HP Lizenz	Zum Anzeigen des HP Endbenutzer-Lizenzvertrags (EULA).
SCEP Manager	Ermöglicht die netzwerkbasierete Zertifikatsverwaltung.
Serial Manager	Zur Konfiguration serieller Geräte.
Tastenkombinationen	Zum Erstellen, Ändern und Löschen von Tastenkombinationen.
Snipping Tool	Zum Aufnehmen eines Schnappschusses einer rechteckigen Auswahl des Bildschirms, eines bestimmten Fensters oder des gesamten Bildschirms.
Task-Manager	Zum Überwachen der CPU-Auslastung und des Verlaufs der CPU-Auslastung für den Thin Client.
Text-Editor	Öffnet einen einfachen Texteditor zum Anzeigen und Bearbeiten von Textdateien.
X-Terminal	Zum Ausführen von Linux-Befehlen.

## Zertifikate



**HINWEIS:** Weitere Informationen über die Verwendung der Zertifikate unter Linux finden Sie auf der Website <http://www.openssl.org/docs/apps/x509.html>.

### Zertifikat-Manager

So öffnen Sie den Zertifikat-Manager:

- ▲ Wählen Sie in der Systemsteuerung **Advanced > Certificates** (Erweitert > Zertifikate).

Verwenden Sie den Zertifikat-Manager, um manuell ein Zertifikat von einer Zertifizierungsstelle (CA) zu installieren. Dieser Vorgang kopiert das Zertifikat zum lokalen Zertifikatsspeicher des Benutzers (`/usr/local/share/ca-certificates`) und konfiguriert OpenSSL, um das Zertifikat zur Verbindungsverifizierung zu verwenden.

Falls gewünscht, können Sie Profile Editor verwenden, um das Zertifikat einem Profil zuzuweisen, wie unter [Hinzufügen von Zertifikaten zu einem Clientprofil auf Seite 69](#) beschrieben.



**HINWEIS:** Im Allgemeinen funktioniert ein selbstsigniert Zertifikat, so lange es gemäß der Spezifikationen gültig ist und von OpenSSL überprüft werden kann.

### SCEP Manager

So öffnen Sie den SCEP Manager:

- ▲ Wählen Sie in der Systemsteuerung **Advanced > SCEP Manager** (Erweitert > SCEP-Manager).

Verwenden Sie den SCEP Manager, wenn Sie auf der Client-Seite Zertifikate von einer Zertifizierungsstelle registrieren oder erneuern müssen.

Während einer Registrierung oder Erneuerung generiert der SCEP Manager den privaten Schlüssel und die Zertifikatsanforderung des Thin Client und sendet anschließend die Anforderung an die Zertifizierungsstelle auf dem SCEP-Server. Wenn die Zertifizierungsstelle das Zertifikat ausgibt, wird das Zertifikat zurückgesendet und im Zertifikatsspeicher des Thin Client abgelegt. OpenSSL verwendet das Zertifikat zur Verbindungsverifizierung.



**HINWEIS:** Stellen Sie vor der Registrierung sicher, dass der SCEP-Server richtig konfiguriert ist.

Verwenden Sie die Registerkarte **Identifying** (Identifizierung) im SCEP Manager, um ggf. Informationen über den Benutzer einzugeben.



**HINWEIS:** Der **Common Name** (Allgemeiner Name) ist erforderlich – standardmäßig ist dies der vollständig qualifizierte Domänenname (Fully-Qualified Domain Name, FQDN) des Thin Client. Alle anderen Informationen sind optional. **Country or Region** (Land bzw. Region) wird als zwei Buchstaben, z. B. US für die Vereinigten Staaten oder CN für China, eingegeben.

Verwenden Sie die Registerkarte **Servers** (Server) im SCEP Manager, um SCEP-Server hinzuzufügen und zum Registrieren oder Erneuern von Zertifikaten.



**TIPP:** Speichern Sie bei der Eingabe eines neuen SCEP-Servers zuerst die Informationen zum Server und wählen Sie dann die Schaltfläche **Settings** (Einstellungen), um zurückzukehren und eine Registrierung durchzuführen.

### DHCP-Optionen

So öffnen Sie den DHCP Option Manager:

- ▲ Wählen Sie in der Systemsteuerung **Advanced > DHCP Options** (Erweitert > DHCP-Optionen).

Der DHCP Option Manager zeigt Details zu den DHCP-Optionen an, die vom Thin Client angefordert werden.

---

 **TIPP:** Die Dropdown-Liste in der linken unteren Ecke des DHCP Option Managers erlaubt es Ihnen zu filtern, welche DHCP-Tags angezeigt werden.

---

So weisen Sie den Thin Client an, bestimmte DHCP-Optionen anzufordern oder zu ignorieren:

- ▲ Aktivieren oder deaktivieren Sie die Kontrollkästchen in der Spalte **Requested** (Angefordert).

Wenn in der Spalte **DHCP Code** ein Stift angezeigt wird, kann die Codenummer geändert werden, für den Fall, dass zu einer bestimmten Codenummer auf Ihrem DHCP-Server ein Konflikt aufgetreten ist.

So ändern Sie einen DHCP-Code:

- ▲ Doppelklicken Sie auf den DHCP-Code und geben Sie eine neue Nummer ein.

---

 **HINWEIS:** Veränderbare DHCP-Codes können nur geändert werden, wenn diese DHCP-Option in der Spalte **Requested** (Angefordert) aktiviert ist.

---

So erhalten Sie weitere Informationen über die Verwendung einer DHCP-Option auf dem Thin Client und auf dem DHCP-Server:

- ▲ Wählen Sie das Symbol in der Spalte **Info** dieser Option.

## 6 Systeminformationen

Wählen Sie auf der Taskleiste die Schaltfläche **Systeminformationen** aus, um System-, Netzwerk- und Softwareinformationen anzuzeigen. In der folgende Tabelle werden die Informationen beschrieben, die in den einzelnen Bereichen angezeigt werden.

Bereich	Beschreibung
Allgemein	Zeigt Informationen über BIOS, Betriebssystem, CPU und Speicher an.
Netzwerk	Zeigt Informationen über Netzwerkschnittstelle, Gateway und DNS-Einstellungen an.
Net-Tools	Bietet die folgenden Tools zur Überwachung und Problembhebung: <ul style="list-style-type: none"><li>• <b>Ping</b> – Spezifizieren einer IP-Adresse von einem anderen Gerät im Netzwerk, um eine Verbindung aufzubauen.</li><li>• <b>DNS-Lookup</b> – Zum Auflösen eines Domännennamens in eine IP-Adresse.</li><li>• <b>Route verfolgen</b> – Zum Nachverfolgen des Pfades, auf dem ein Netzwerkpaket von einem Gerät zum anderen gesendet wird.</li></ul>
Softwareinformationen	Zeigt eine Liste der installierten Add-ons auf der Registerkarte <b>Service Packs</b> (Service-Pakete) an, sowie Informationen zur Software-Version auf der Registerkarte <b>Installierte Software</b> . <b>TIPP:</b> Sie können auch das Administrator-Handbuch (dieses Dokument) über diesen Bildschirm aufrufen.
Systemprotokolle	Zeigt folgende Protokolle an: <ul style="list-style-type: none"><li>• Netzwerkmanager</li><li>• Smart Client Services</li><li>• DHCP Wired Leases</li><li>• DHCP Wireless Leases</li><li>• Kernel</li><li>• X Server</li><li>• Connection Manager</li></ul> <p>Die Debugstufe kann geändert werden, um weitere Informationen anzuzeigen, die möglicherweise vom HP Support bei der Problembhebung angefragt werden.</p> <p>Wählen Sie <b>Diagnostic</b> (Diagnose), um eine Diagnosedatei zu speichern. Weitere Informationen finden Sie unter <a href="#">Verwenden der Systemdiagnose für die Fehlerbeseitigung auf Seite 74</a>.</p>



**HINWEIS:** Siehe [SystemInfo auf Seite 150](#) für Informationen über die Registrierungsschlüssel, die zum Ausblenden von Systeminformationen verwendet werden können.

---

# 7 HP Smart Client Services

HP Smart Client Services besteht aus einer Reihe serverseitiger Tools, mit denen Sie Client-Profilen konfigurieren können, die auf eine große Anzahl Thin Clients verteilt werden können. Diese Funktion wird als Automatic Update (Automatische Updates) bezeichnet.

HP ThinPro erkennt einen Automatic Update-Server beim Hochfahren und konfiguriert Einstellungen entsprechend. Dies vereinfacht die Geräteinstallation und Wartung.

## Unterstützte Betriebssysteme

HP Smart Client Services unterstützt die folgenden Betriebssysteme:

- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2003
- Windows Vista®
- Windows XP



---

**HINWEIS:** Der Installer ist zwar nur ein 32-Bit-Programm, wird jedoch von der 32-Bit- als auch der 64-Bit-Version des Windows Betriebssystems unterstützt.

---

## Voraussetzungen für HP Smart Client Services

Überprüfen Sie vor der Installation von HP Smart Client Services, den Konfigurations- und Installationsstatus der folgenden Komponenten:

- **Internet Information Services (IIS)**
- **.NET Framework 3.5**

Informationen zur Installation oder Aktivierung dieser Komponenten auf dem Betriebssystem, das Sie für den Server verwenden, finden Sie unter <http://www.microsoft.com>.

## Abrufen von HP Smart Client Services

So rufen Sie die HP Smart Client Services ab:

1. Navigieren Sie zur Webseite <http://www.hp.com/support>.
2. Suchen Sie nach dem Thin Client-Modell. Sie finden HP Smart Client Services unter der Kategorie **Software - System Management** (Software - Systemsteuerung) auf der Seite **Drivers, Software & Firmware** (Treiber, Software und Firmware).

## Anzeigen der Automatic Update-Website

1. Wählen Sie auf dem Serverdesktop **Start > Systemsteuerung** und dann **Verwaltung**.
2. Doppelklicken Sie auf **Internet Information Services (IIS) Manager**.
3. Erweitern Sie im linken Bereich des IIS-Manager die folgenden Elemente:  
**Servername > Sites (Standorte) > HP Automatic Update > auto-update**



**HINWEIS:** Der physische Speicherort für die Automatic Update-Dateien lautet wie folgt:

```
C:\Program Files (x86)\Hewlett-Packard\HP Smart Client Service\auto-update
```

## Erstellen eines Automatic Update-Profiles

Automatic Update verwendet Profile zum Verteilen einer Konfiguration an Thin Clients. Wenn Sie ein Profil mit Profile Editor erstellen (siehe „[Profile Editor](#)“ auf [Seite 67](#)), können Sie es standardmäßig im folgenden Ordner speichern:

```
C:\Program Files (x86) Hewlett-Packard\HP Smart Client Service\autoupdate  
\PersistentProfile\
```

Sie können auch ein vorhandenes Profil von einem Thin Client mit HP ThinState exportieren und in diesen Speicherort kopieren.

Bei der Suche nach Updates prüft HP ThinPro diesen Ordner und wendet das dort gespeicherte Profil an. So wird sichergestellt, dass auf allen Thin Clients die gleiche Konfiguration verwendet wird.

## Profile für bestimmte MAC-Adressen

Automatic Update-Profile können für eine einzelne MAC-Adresse erstellt werden. Dies kann nützlich sein, wenn für einige Thin Clients eine andere Konfiguration erforderlich ist.

Profile für eine einzelne MAC-Adresse müssen auf dem Automatic Update-Server im folgenden Ordner gespeichert werden:

```
C:\Program Files (x86) Hewlett-Packard\HP Smart Client Service\autoupdate  
\PersistentProfile\MAC\
```

Bei der Suche nach Updates prüft HP ThinPro zuerst auf das generische Profil und dann auf ein Profil, das auf einer MAC-Adresse basiert. Diese Profile werden zusammengeführt und gemeinsam auf dem Thin Client installiert. Das auf der MAC-Adresse basierende Profil hat Vorrang. Wenn also ein Registrierungsschlüssel in beiden Dateien unterschiedliche Werte aufweist, wird der Wert aus dem auf der MAC-Adresse basierenden Profil verwendet.

Dadurch wird sichergestellt, dass auf allen Thin Clients eine gemeinsame Konfiguration bereitgestellt werden kann, bei Bedarf jedoch bestimmte Anpassungen ergänzt werden können.

In diesem Abschnitt wird beschrieben, wie Sie ein Automatic Update-Profil für eine einzelne MAC-Adresse erstellen.

1. Ermitteln Sie die MAC-Adresse des Thin Client über die Systeminformationen. In den folgenden Schritten wird z. B. die MAC-Adresse `00fcab8522ac` verwendet.
2. Verwenden Sie Profile Editor zum Erstellen oder Ändern eines Clientprofils (siehe [„Profile Editor“ auf Seite 67](#)), bevor Sie das Clientprofil speichern.
3. Wählen Sie in **Profile Editor** im linken Bereich **Finish** (Fertig stellen), um auf den Bereich **Current profile** (Aktuelles Profil) zuzugreifen.
4. Wählen Sie **Save profile as** (Profil speichern unter) aus, um das Clientprofil wie folgt zu speichern:  

```
C:\Program Files (x86) Hewlett-Packard\HP Smart Client Service\auto-update\PersistentProfile\MAC\00fcab8522ac.xml
```
5. Wählen Sie im Bereich **Current profile** (Aktuelles Profil) die Schaltfläche **Finish** (Fertig stellen) aus, um Profile Editor zu schließen.
6. Starten Sie den Thin Client neu, der die angegebene MAC-Adresse verwendet, um die automatische Aktualisierung einzuleiten.

## Aktualisieren von Thin Clients

### Verwenden der Methode zur Aktualisierung per Übertragung

Um eine Aktualisierung per Übertragung vorzunehmen, verbinden Sie den Thin Client mit demselben Netzwerk wie den Aktualisierungsserver. Eine Aktualisierung per Übertragung stützt sich auf HP Smart Client Services, das mittels IIS automatisch Aktualisierungen auf den Thin Client überträgt.

 **HINWEIS:** Aktualisierungen per Übertragung funktionieren nur, wenn sich der Thin Client im gleichen Subnetz befindet wie der Server.

 **TIPP:** Um zu überprüfen, ob die Aktualisierung per Übertragung funktioniert, führen Sie Profile Editor aus und nehmen Sie einige Änderungen vor. Schließen Sie den Thin Client an und überprüfen Sie, ob das neue Profil heruntergeladen wurde. Falls nicht, siehe [„Fehlerbeseitigung“ auf Seite 73](#).

### Verwenden der Methode zur Aktualisierung per DHCP-Kennung

Auf Windows Server 2003- und Windows Server 2008-Systemen kann ein Thin Client über die DHCP-Kennung aktualisiert werden. Verwenden Sie diese Methode, um bestimmte Thin Clients zu aktualisieren. Wenn Sie jedoch nur einen oder zwei Clients aktualisieren möchten, sollten Sie stattdessen die manuelle Aktualisierungsmethode verwenden. Generell empfiehlt HP die Methode zur Aktualisierung per Übertragung.

### Beispiel für die Durchführung DHCP-Kennung

Das Beispiel in diesem Bereich zeigt, wie die DHCP-Kennung auf einem Windows 2008 R2-Server durchgeführt wird.

 **HINWEIS:** Zum Verwenden der DHCP-Kennung lesen Sie Ihre DHCP-Serverdokumentation.

1. Auf dem Server-Desktop wählen Sie **Start > Administrative Tools > DHCP** (Start > Verwaltungstools > DHCP).
2. Wählen Sie im linken Bereich des Bildschirms **DHCP** die Domäne aus, mit der die Thin Clients verbunden sind.

- Erweitern Sie im rechten Bereich des Bildschirms **DHCP** den Eintrag **IPv4**, klicken Sie mit der rechten Maustaste darauf und wählen Sie dann **Vordefinierte Optionen einstellen** aus.
- Wählen Sie im Dialogfeld **Vordefinierte Optionen und Werte** die Option **Hinzufügen** aus.
- Im Feld **Option Type** (Optionstyp) konfigurieren Sie die Optionen wie in der folgenden Tabelle beschrieben.

Feld	Eintrag
Name	Geben Sie <code>auto-update</code> ein.
Datentyp	Wählen Sie <b>Einstellungen</b> aus.
Code	Geben Sie <code>137</code> ein.
Beschreibung	Geben Sie <code>HP Automatic Update</code> ein.

- Wählen Sie **OK**.
- Geben Sie im Dialogfeld **Vordefinierte Optionen und Werte** unter **Wert > Zeichenfolge** die Adresse des Aktualisierungsservers im folgenden Format ein:  
`http://auto-update.dominio.com:18287/auto-update`
- Um das Setup abzuschließen, wählen Sie **OK**. Die DHCP-Kennung kann jetzt für die Aktualisierung bestimmter Thin Clients verwendet werden.

## Verwenden der Methode zur Aktualisierung per DNS-Alias

Während des Systemstarts versucht die automatische Aktualisierung den DNS-Alias **auto-update** aufzulösen. Wenn dieser Host-Name aufgelöst wird, versucht er, unter **http://auto-update:18287** zu prüfen, ob neue Aktualisierungen verfügbar sind. Diese Aktualisierungsmethode ermöglicht es Thin Clients, auf einen einzelnen Aktualisierungsserver in der gesamten Domäne zuzugreifen. Daher wird die Verwaltung von Bereitstellungen mit vielen Subnetzen und DHCP-Servern vereinfacht.

So konfigurieren Sie die Aktualisierungsmethode mit DNS Alias:

- ▲ Ändern Sie den Hostnamen des Servers, der HP Smart Client Services hostet, zu **auto-update** (Automatisch aktualisieren) oder erstellen Sie einen DNS-Alias von **auto-update** (Automatisch aktualisieren) für diesen Server.

## Verwenden der Methode zur manuellen Aktualisierung

Verwenden Sie die Methode zur manuellen Aktualisierung, um einen Thin Client für eine Aktualisierung mit einem bestimmten Server zu verbinden. Verwenden Sie diese Methode auch, wenn Sie eine Aktualisierung auf einem einzelnen Thin Client testen möchten, bevor Sie die Aktualisierung auf viele Thin Clients übertragen oder wenn bestimmte Aktualisierungen auf nur ein oder zwei Thin Clients installiert werden sollen.

 **HINWEIS:** Sie müssen den Hostnamen des manuellen Servers in dem Profil angeben, das Sie aktualisieren. Andernfalls werden die Einstellungen beim Herunterladen des Profils auf die automatischen Einstellungen zurückgesetzt. Verwenden Sie **Profile Editor** zum Ändern dieser Einstellungen im Stammverzeichnis bzw. für die automatische Aktualisierung.

 **HINWEIS:** Wenn mehrere Thin Clients bestimmte Aktualisierungen benötigen, verwenden Sie die Methode mit der DHCP-Kennung.

Wenn keine Differenzierung erforderlich ist, empfiehlt sich die Aktualisierung per Übertragung.

## Durchführen einer manuellen Aktualisierung

1. Wählen Sie in der Systemsteuerung **Management > Automatic Update** (Verwaltung > Automatic Update).
2. Wählen Sie **Enable manual configuration** (Manuelle Konfiguration aktivieren).
3. Stellen Sie das **Protocol** (Protokoll) auf **http** ein.
4. Geben Sie im Feld **Server** Hostname und Port des Aktualisierungsservers im folgenden Format ein:  
*HostName:18287*
5. Geben Sie im Feld **Path** (Pfad) Folgendes ein:  
*auto-update*
6. Wählen Sie **Preserve thin client configuration** (Thin Client-Konfiguration beibehalten) aus, wenn Sie alle zuvor konfigurierten Einstellungen beibehalten möchten.
7. Wählen Sie **OK** und der Thin Client ruft die Aktualisierungen ab.

## 8 Profile Editor

Zu HP Smart Client Services gehört Profile Editor, mit dem Administratoren Clientprofile erstellen und auf den Automatic Update-Server hochladen können.

 **TIPP:** Zusätzlich zur Erstellung eines neuen Clientprofils, können Sie ein vorhandenes Profil bearbeiten, das mithilfe von HP ThinState exportiert wurde.

Ein Clientprofil enthält die Verbindungen, die Einstellungen und die Anpassungen, die mit Connection Manager und verschiedenen Elementen der Systemsteuerung konfiguriert wurden. Ein Clientprofil wird in einer Konfigurationsdatei gespeichert, die nur für die Version von HP ThinPro geeignet ist, in der sie erstellt wurde.

### Öffnen von Profile Editor

▲ Wählen Sie **Start > Alle Programme > Hewlett-Packard > HP Automatic Update Server > Profile Editor**.

### Laden eines Clientprofils

Der Name des gerade geladenen Profils wird auf dem Startbildschirm von Profile Editor angezeigt.

So laden Sie ein anderes Clientprofil:

1. Wählen Sie auf dem Startbildschirm von Profile Editor den Link, auf dem der Name des gerade geladenen Clientprofils angezeigt wird.
2. Navigieren Sie zu einem Clientprofil und wählen Sie dann **Open** (Öffnen).

### Anpassung von Clientprofilen

#### Auswählen der Plattform für ein Clientprofil

Verwenden Sie den Bildschirm **Plattform** (Plattform) in Profile Editor, um die folgenden Aufgaben durchzuführen:

- Auswählen der gewünschten HP ThinPro-Image-Version, die mit Ihrer Hardware kompatibel ist
- Wählen zwischen ThinPro und Smart Zero
- Anzeigen der installierten Client-Kits, die zusätzliche Registrierungseinstellungen zur Verfügung stellen



**HINWEIS:** Client-Kits sollten im folgenden Verzeichnis gespeichert werden:

```
C:\Program Files (x86)\Hewlett-Packard\HP Smart Client Service\auto-update\Packages
```

So konfigurieren Sie die Plattformeinstellungen eines Clientprofils:

1. Wählen Sie auf dem Bildschirm **Plattform** (Plattform) in Profile Editor eine **OS-Build-ID** (Betriebssystem-Build-ID), die der gewünschten Image-Version entspricht.



**WICHTIG:** Stellen Sie sicher, dass Sie für jeden Hardwaretyp ein anderes Clientprofil erstellen.

 **HINWEIS:** Wenn ein Client-Kit installiert ist, wird es automatisch im Feld für Client-Kits angezeigt und zusätzliche Registrierungseinstellungen stehen auf dem Registrierungsbildschirm zur Verfügung.

---

2. Stellen Sie die Konfiguration entweder auf **Standard** (ThinPro) oder **Zero** (Null) (Smart Zero) ein.

 **HINWEIS:** Für ältere Image-Versionen ist diese Einstellung ausgegraut und automatisch auf „Zero“ (Null) eingestellt.

---

## Konfigurieren einer Standardverbindung für ein Clientprofil

So konfigurieren Sie eine Standardverbindung für ein Clientprofil:

1. Wählen Sie auf dem Bildschirm **Connection** (Verbindung) in Profil Editor den gewünschten Verbindungstyp aus der Dropdown-Liste **Type** (Typ).

 **HINWEIS:** Die verfügbaren Verbindungstypen sind davon abhängig, ob Sie ThinPro oder Smart Zero auf dem Bildschirm „Plattform“ (Plattform) ausgewählt haben.

---

2. Geben Sie im Feld **Server** den Namen oder die IP-Adresse des Servers ein.

## Ändern von Registrierungseinstellungen eines Clientprofils

So ändern Sie die Standard-Registrierungseinstellungen für ein Clientprofil:

1. Erweitern Sie auf dem Bildschirm **Registry** (Registrierung) in Profile Editor die Ordner in der Baumstruktur **Registry settings** (Registrierungseinstellungen), um nach den Registrierungseinstellungen zu suchen, die Sie ändern möchten.
2. Wählen Sie den Registrierungsschlüssel aus und geben Sie dann den gewünschten Wert im Feld **Value** (Wert) ein.

 **HINWEIS:** Siehe „[Registrierungsschlüssel](#)“ auf [Seite 79](#) für eine umfassende Liste und Beschreibung der Registrierungsschlüssel.

---

## Hinzufügen von Dateien zu einem Clientprofil

Verwenden Sie den Bildschirm **Files** (Dateien) in Profile Editor, um Konfigurationsdateien hinzuzufügen, die automatisch auf dem Thin Client installiert werden, wenn das Clientprofil installiert ist. Dies wird normalerweise aus folgenden Gründen verwendet:

- Zum Hinzufügen von Zertifikaten
- Zum Ändern von Geräteeinstellungen, wenn keine Registrierungseinstellung für die Änderung verfügbar ist.
- Um das Verhalten des Systems zu ändern, indem Sie benutzerdefinierten Skripte einfügen oder vorhandene Skripte ändern.

Sie können auch eine symbolische Verknüpfung angeben, die auf eine Datei verweist, die bereits auf dem Thin Client installiert ist. Gehen Sie so vor, wenn von mehr als einem Verzeichnis auf die Datei zugegriffen werden muss.

## Hinzufügen einer Konfigurationsdatei zu einem Clientprofil

1. Wählen Sie auf dem Bildschirm **Files** (Dateien) in Profile Editor **Add a file** (Datei hinzufügen).
2. Wählen Sie **Import File** (Datei importieren) aus, um nach der zu importierenden Datei zu suchen, und klicken Sie dann auf **Open** (Öffnen).

---

 **HINWEIS:** Dateien können auch über die Schaltfläche **Export File** (Datei exportieren) exportiert werden, wenn weitere Einzelheiten über die Datei erforderlich sind.

---

3. Geben Sie im Feld **Path** (Pfad) den Pfad ein, in dem die Datei auf dem Thin Client installiert werden soll.
4. Legen Sie im Abschnitt **File details** (Dateidetails) die Felder **Owner** (Besitzer), **Group** (Gruppe) und **Permissions** (Berechtigungen) auf die entsprechenden Werte fest.

---

 **HINWEIS:** Normalerweise reicht es aus, den Besitzer und die Gruppe als **root** und die Berechtigungen als **644** festzulegen. Wenn besondere Besitzer, Gruppen oder Berechtigungen erforderlich sind, finden Sie in den standardmäßigen Unix®-Dateiberechtigungen Hinweise zum Ändern der Dateidetails.

---

5. Wählen Sie **Save** (Speichern) aus, um das Hinzufügen der Konfigurationsdatei zum Clientprofil abzuschließen.

---

 **HINWEIS:** Eine Datei, die als Teil eines Profils installiert wurde, wird automatisch jede vorhandene Datei auf dem Dateisystem im Zielpfad überschreiben. Außerdem wird ein zweites Profil ohne die angehängte Datei zuvor angehängte Dateien nicht wiederherstellen. Alle Dateien, die über einen Profilanhang installiert wurden, sind dauerhaft und müssen manuell oder über die Werkseinstellungen wiederhergestellt werden.

---

## Hinzufügen von Zertifikaten zu einem Clientprofil

Client-Profile enthalten automatisch Zertifikate, die auf einen Standard-Client-Zertifikatsspeicher für die folgenden Anwendungen importiert werden:

- VMware Horizon View, Citrix, RDP
- Automatic Update
- HP Smart Client Services
- Web Browser-Speicher

So importieren Sie andere Zertifikate zu einem Client-Profil:

1. Wählen Sie auf dem Bildschirm **Files** (Dateien) in Profile Editor **Add a file** (Datei hinzufügen).
2. Wählen Sie **Import File** (Datei importieren) aus, ermitteln Sie das Zertifikat und wählen Sie auf **Open** (Öffnen) aus.

---

 **HINWEIS:** Das Zertifikat sollte als `.pem`- oder `.crt`-Datei formatiert sein.

---

3. Stellen Sie im Feld **Path** (Pfad) den Pfad auf Folgendes ein:

```
/usr/local/share/ca-certificates
```

4. Wählen Sie **Save** (Speichern), um das Hinzufügen des Zertifikats zum Clientprofil abzuschließen.
5. Verwenden Sie nach der Installation des Clientprofils den **Zertifikat-Manager**, um zu überprüfen, ob das Zertifikat ordnungsgemäß importiert wurde.

## Hinzufügen eines symbolischen Links zu einem Clientprofil

1. Wählen Sie auf dem Bildschirm **Files** (Dateien) in Profile Editor **Add a file** (Datei hinzufügen).
2. Wählen Sie in der Dropdown-Liste **Type** (Typ) die Option **Link**.
3. Legen Sie im Abschnitt **Symbolic link details** (Details des symbolischen Links) das Feld **Link** auf den Pfad der gewünschten Datei fest, die bereits auf dem Thin Client installiert ist.
4. Wählen Sie **Save** (Speichern) aus, um das Hinzufügen des symbolischen Links abzuschließen.

## Speichern des Clientprofils

1. Wählen Sie in **Profile Editor** im linken Bereich **Finish** (Fertig stellen), um auf den Bildschirm **Current profile** (Aktuelles Profil) zuzugreifen.
2. Wählen Sie **Save Profile** (Profil speichern), um das aktuelle Clientprofil zu speichern, oder wählen Sie **Save Profile As** (Profil speichern unter), um es als ein neues Clientprofil zu speichern.



---

**HINWEIS:** Wenn **Save Profile** (Profil speichern) deaktiviert ist, wurde Ihr Clientprofil seit dem letzten Speichern nicht geändert.

---

3. Wählen Sie auf dem Bildschirm **Current profile** (Aktuelles Profil) die Schaltfläche **Finish** (Fertig stellen), um Profile Editor zu schließen.

## Konfiguration eines seriellen oder parallelen Druckers

Sie können mit Profile Editor die Anschlüsse für den seriellen oder parallelen Drucker einrichten. Ein USB-Drucker wird beim Anschließen automatisch zugeordnet.

### Abrufen der Druckereinstellungen

Rufen Sie vor der Konfiguration der Druckeranschlüsse die Druckereinstellungen ab. Falls verfügbar, überprüfen Sie die Druckerdokumentation bevor Sie fortfahren. Gehen Sie wie folgt vor, wenn diese Option nicht verfügbar ist:

1. Bei den meisten Druckern drücken und halten Sie die Taste **Feed** (Papierzufuhr) gedrückt, während das Gerät eingeschaltet wird.
2. Nach einigen Sekunden lassen Sie die **Feed** (Papierzufuhr)-Taste los. So kann der Drucker in einen Testmodus wechseln und die erforderlichen Informationen ausdrucken.



---

**TIPP:** Zum Beenden des Testdruckmodus müssen Sie den Drucker eventuell wieder ausschalten oder die **Feed** (Papierzufuhr)-Taste nochmals drücken, damit die Diagnosesseite gedruckt wird.

---

### Einrichten von Druckeranschlüssen

1. Wählen Sie in **Profile Editor** die Option **Registry** (Registrierung) und aktivieren Sie dann das Kontrollkästchen **Show all settings** (Alle Einstellungen anzeigen).
2. Aktivieren Sie die Druckerportzuordnung für Ihren Verbindungstyp:

- Citrix – Es sind keine Aktionen erforderlich.
  - RDP – Navigieren Sie zu **root > ConnectionType > freerdp**. Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **New connection** (Neue Verbindung) und dann **OK**. Legen Sie den Registrierungsschlüssel **portMapping** auf 1 fest, um die Zuordnung des Druckeranschlusses zu aktivieren.
  - VMware Horizon View – Navigieren Sie zu **root > ConnectionType > view**. Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **New connection** (Neue Verbindung) und dann **OK**. Legen Sie im Ordner **xfreerdpOptions** den Registrierungsschlüssel **portMapping** auf 1 fest, um die Zuordnung des Druckeranschlusses zu aktivieren.
3. Navigieren Sie zu **root > Serial**. Klicken Sie mit der rechten Maustaste auf den Ordner **Serial** und wählen Sie **New UUID** (Neue UUID) und dann **OK**.
  4. Stellen Sie unter dem neuen Verzeichnis die Werte **baud** (Baud), **dataBits** (Datenbits), **flow** (Fluss) und **parity** (Parität) gemäß der Werte unter [Abrufen der Druckereinstellungen auf Seite 70](#) ein.  
Stellen Sie den Wert **device** (Gerät) auf den Port ein, an dem der Drucker angeschlossen wird. So wäre beispielsweise der erste serielle Port `/dev/ttyS0`, der zweite serielle Port wäre `/dev/ttyS1` usw. Verwenden Sie für serielle USB-Drucker das Format `/dev/ttyUSB#`, wobei # die Nummer des Ports ist, beginnend mit 0.

## Installieren von Druckern auf dem Server

1. Auf dem Windows Desktop wählen Sie **Start > Drucker und Faxgeräte**.
  2. Wählen Sie **Drucker hinzufügen** und dann **Weiter**.
  3. Wählen Sie **Lokaler Drucker, der an den Computer angeschlossen ist** und bei Bedarf deaktivieren Sie **Plug & Play-Drucker automatisch ermitteln und installieren**.
  4. Klicken Sie dann auf **Weiter**.
  5. Wählen Sie im Menü einen Anschluss.
- 
-  **HINWEIS:** Der Port, den Sie benötigen, befindet sich im Bereich mit den als **TS###** gekennzeichneten Ports, wobei ### eine Zahl von 000 bis 009 oder von 033 bis 044 ist. Welcher Port der Richtige ist, hängt von Ihrem Host-Namen und von dem zu installierenden Drucker ab. Wenn der Host-Name ZTAHENAKOS lautet und Sie einen seriellen Drucker installieren möchten, wählen Sie den Port mit der Bezeichnung **ZTAHENAKOS:COM1**. Für einen parallelen Drucker wählen Sie (**ZTAHENAKOS:LPT1**). Die Kennzeichnung **TS###** wird vom Server zugewiesen und kann sich daher jedes Mal ändern.
- 
6. Wählen Sie den Hersteller und den Treiber für Ihren Drucker aus.
- 
-  **TIPP:** Falls gewünscht, verwenden Sie die Treiber-Disc **Windows Update** zum Installieren des Treibers.
-  **HINWEIS:** Für einfache oder Testdrucke funktioniert normalerweise der Drucker **Generic Manufacturer** (Allgemeiner Hersteller) oder **Generic/Text Only** (Allgemein / Nur Text).
- 
7. Wenn Sie dazu aufgefordert werden, den vorhandenen funktionsfähigen Treiber beizubehalten, tun Sie es und wählen Sie dann **Weiter** aus.
  8. Weisen Sie dem Drucker einen Namen zu. Wählen Sie **Ja**, um ihn als Standarddrucker zu verwenden, und wählen Sie dann **Weiter**.

9. Um den Drucker freizugeben, wählen Sie **Freigabename** und weisen Sie ihm einen Freigabennamen zu. Wählen Sie andernfalls **Weiter**.
10. Auf der nächsten Seite können Sie einen Testdruck anfordern. HP empfiehlt dies, weil Sie dadurch überprüfen können, ob der Drucker korrekt eingerichtet ist. Falls der Drucker nicht korrekt eingerichtet ist, überprüfen Sie die Einstellungen und versuchen Sie es erneut.



**HINWEIS:** Wenn der Thin Client vom Server getrennt wird, muss der Drucker erneut eingerichtet werden, wenn der Thin Client das nächste Mal eine Verbindung herstellt.

---

# 9 Fehlerbeseitigung

## Fehlerbeseitigung bei der Netzwerkverbindung

1. Führen Sie den Ping-Befehl für den gewünschten Server mit den folgenden Schritten aus:
  - a. Wählen Sie die Schaltfläche „Systeminformationen“ auf der Taskleiste und dann die Registerkarte **Net Tools** (Netzwerktools).
  - b. Unter **Tool auswählen** wählen Sie **Ping**.
  - c. Geben Sie im Feld **Zielhost** die Serveradresse ein und wählen Sie dann **Prozess starten**.

Wenn der Ping erfolgreich ausgeführt wird, zeigt das System die folgende Ausgabe:

```
PING 10.30.8.52 (10.30.8.52) 56(84) bytes of data.
```

```
64 bytes from 10.30.8.52: icmp_seq=1 ttl=64 time=0.815 ms
64 bytes from 10.30.8.52: icmp_seq=2 ttl=64 time=0.735 ms
```

Wenn der Ping-Befehl nicht erfolgreich ist, ist der Thin Client möglicherweise vom Netzwerk getrennt und es entsteht eine lange Verzögerung ohne Systemausgabe.

2. Wenn der Thin Client nicht auf den Ping-Befehl reagiert, gehen Sie wie folgt vor:
  - a. Überprüfen Sie das Netzkabel und die Netzwerkeinstellungen in der Systemsteuerung.
  - b. Versuchen Sie, den Ping-Befehl für andere Server oder Thin Clients auszuführen.
  - c. Wenn Sie andere Thin Clients erreichen können, überprüfen Sie, ob Sie die richtige Serveradresse eingegeben haben.
  - d. Führen Sie einen Ping unter Verwendung der IP-Adresse durch anstelle des Domänennamens oder umgekehrt.
3. Überprüfen Sie die Systemprotokolle indem Sie Folgendes durchführen:
  - a. Wählen Sie die Schaltfläche „Systeminformationen“ auf der Taskleiste und dann die Registerkarte **Systemprotokolle**.
  - b. Überprüfen Sie die Protokolle auf Fehler.
  - c. Wenn ein Fehler aufgetreten ist, wird die Benachrichtigung **Server is not set up** (Server ist nicht eingerichtet) angezeigt. Stellen Sie sicher, dass der Server richtig eingerichtet ist und dass HP Smart Client Services ausgeführt wird.

## Fehlerbeseitigung bei abgelaufenen Citrix-Kennwörtern

Wenn Benutzer nicht dazu aufgefordert werden, abgelaufene Citrix-Kennwörter zu ändern, stellen Sie sicher, dass für die XenApp Services-Site (PNAgent-Site) die Authentifizierungsmethode **Prompt** (Auffordern) festgelegt ist, um Benutzern das Ändern abgelaufener Kennwörter zu ermöglichen. Wenn Sie es Benutzern ermöglichen, ihre Kennwörter zu ändern, indem sie eine direkte Verbindung mit dem Domänencontroller herstellen, stellen Sie sicher, dass die Uhrzeit des Thin Clients mit der des Domänencontrollers synchron ist und dass bei der Eingabe von Citrix-Anmeldeinformationen der vollständige Domänenname (z. B. `domain_name.com`) verwendet wird. Weitere Informationen finden Sie in der Citrix-Dokumentation.

## Verwenden der Systemdiagnose für die Fehlerbeseitigung

Die Systemdiagnose erstellt einen Schnappschuss vom Thin Client, der dazu genutzt werden kann, ohne physischen Zugriff auf den Thin Client Probleme zu lösen. Dieser Schnappschuss enthält Protokolldateien der BIOS-Informationen und die Prozesse, die zum Zeitpunkt der Ausführung der Systemdiagnose aktiv waren.

 **TIPP:** Sie können die Einstellung **Debugstufe** der Registerkarte **Systemprotokolle** im Fenster **Systeminformationen** ändern, um den Umfang der Informationen anzugeben, die in den Diagnosebericht aufgenommen werden sollen. Diese Informationen werden möglicherweise für die Fehlerbeseitigung von HP angefordert. Da das System Protokolldateien beim Neustart zurücksetzt, sollten Sie darauf achten, Protokolldateien vor einem Neustart zu erfassen.

### Speichern von Systemdiagnosedaten

1. Schließen Sie ein USB-Flash-Laufwerk am Thin Client an.
2. Wählen Sie die Schaltfläche „Systeminformationen“ auf der Taskleiste und dann die Registerkarte **Systemprotokolle**.
3. Wählen Sie **Diagnostic** (Diagnose) und speichern Sie die komprimierte Diagnosedatei **Diagnostic.tgz** dann auf dem USB-Flash-Laufwerk.

### Dekomprimieren der Systemdiagnosedateien

Die Systemdiagnosedatei **Diagnostic.tgz** ist komprimiert und muss dekomprimiert werden, bevor Sie die Diagnosedateien anzeigen können.

### Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen

1. Laden Sie eine Kopie der Windows Version von **7-Zip** herunter und installieren Sie diese.  
 **HINWEIS:** Eine kostenlose Kopie von 7-Zip für Windows erhalten Sie unter <http://www.7-zip.org/download.html>.
2. Stecken Sie das USB-Flash-Laufwerk, das die gespeicherte Systemdiagnosedatei enthält, ein, und kopieren Sie anschließend **Diagnostic.tgz** auf den Desktop.
3. Klicken Sie mit der rechten Maustaste auf **Diagnostic.tgz** und wählen Sie **7-Zip > Extract files** (Dateien entpacken ...).
4. Öffnen Sie den neu erstellten Ordner mit der Bezeichnung **Diagnostic** (Diagnose) und führen Sie Schritt 3 in **Diagnostic.tar** aus.

### Dekomprimieren der Systemdiagnosedateien auf Linux- oder Unix-basierten Systemen

1. Stecken Sie das USB-Flash-Laufwerk, das die gespeicherte Systemdiagnosedatei enthält, ein, und kopieren Sie anschließend **Diagnostic.tgz** zum Startverzeichnis.
2. Öffnen Sie ein Terminal und navigieren Sie zum Startverzeichnis.
3. Geben Sie in der Befehlszeile `tar xvfz Diagnostic.tgz` ein.

### Anzeigen der Systemdiagnosedateien

Die Systemdiagnosedateien werden in die Ordner **Commands** (Befehle), **/var/log** und **/etc** unterteilt.

## Anzeigen von Dateien im Ordner Befehle

Diese Tabelle beschreibt die Dateien, die Sie im Ordner **Commands** (Befehle) finden können.

Datei	Beschreibung
Demidecode.txt	Diese Datei enthält Informationen zum System-BIOS und Grafiken.
dpkg_--list.txt	Diese Datei listet die Pakete auf, die zum Zeitpunkt des Ausführens der Systemdiagnose ausgeführt wurden.
ps_-ef.txt	Diese Datei listet die aktiven Prozesse auf, die zum Zeitpunkt des Ausführens der Systemdiagnose ausgeführt wurden.

## Anzeigen von Dateien im Ordner /var/log

Diese nützliche Datei im Ordner **/var/log** lautet **Xorg.0.log**.

## Anzeigen von Dateien im Ordner /etc

Der Ordner **/etc** enthält das Dateisystem zu dem Zeitpunkt, als die Systemdiagnose ausgeführt wurde.

---

# A USB-Updates

Wenn die USB-Updates aktiviert sind (siehe [Anpassungszentrum auf Seite 51](#)), können Sie ein USB-Flash-Laufwerk verwenden, um gleichzeitig mehrere Add-ons und Zertifikate zu installieren oder zum Bereitstellen eines Profils.

So führen Sie USB-Updates durch:

1. Speichern Sie die gewünschten Dateien auf einem USB-Flash-Laufwerk.



**HINWEIS:** Die Dateien können in das Root-Verzeichnis oder in Unterordnern abgelegt werden.

2. Schließen Sie das USB-Flash-Laufwerk an den Thin Client an.

Updates werden automatisch erkannt und im **USB Update**-Dialog angezeigt, in dem Sie Einzelheiten zu den erkannten Updates suchen und anzeigen können.

3. Aktivieren Sie die Kontrollkästchen neben den Updates, die Sie installieren möchten, und wählen Sie dann **Installieren**.
4. Starten Sie den Thin Client nach der Installation neu, wenn Sie dazu aufgefordert werden.

## HP ThinUpdate

Mit HP ThinUpdate können Sie Images und Add-ons von HP herunterladen und bootfähige USB-Flash-Laufwerke für die Image-Bereitstellung erstellen. Weitere Informationen finden Sie im *Administratorhandbuch* für HP ThinUpdate.

## B BIOS-Tools

Es gibt zwei Arten von BIOS-Tools für HP ThinPro:

- BIOS-Tool für Einstellungen – Zum Abrufen oder Ändern von BIOS-Einstellungen
- BIOS Flashing-Tool – Zum Aktualisieren des BIOS

Diese Tools können über einen X-Terminal ausgeführt werden.

### BIOS-Tool für Einstellungen

Die folgende Tabelle beschreibt die Syntax für das BIOS-Tool für Einstellungen.



**HINWEIS:** Änderungen werden erst beim nächsten Neustart wirksam.

Syntax	Beschreibung
<code>hptc-bios-cfg -G FileName</code>	Ruft die aktuellen BIOS-Einstellungen ab und speichert sie in der angegebenen Datei, sodass sie angezeigt oder geändert werden können (standardmäßig CPQSETUP.TXT).
<code>hptc-bios-cfg -S FileName</code>	Schreibt die BIOS-Einstellungen aus der angegebenen Datei (standardmäßig CPQSETUP.TXT) ins BIOS.
<code>hptc-bios-cfg -h</code>	Zeigt eine Liste der Optionen an.

### BIOS Flashing-Tool

Die folgende Tabelle beschreibt die Syntax für das BIOS Flashing-Tool.



**HINWEIS:** Änderungen werden erst beim nächsten Neustart wirksam.

Syntax	Beschreibung
<code>hptc-bios-flash ImageName</code>	Bereitet das System so vor, dass das BIOS beim nächsten Neustart aktualisiert wird. Mit diesem Befehl werden die Dateien automatisch in den richtigen Speicherort kopiert und Sie werden zum Neustart des Thin Clients aufgefordert.  <b>HINWEIS:</b> Für diesen Befehl muss die Option <b>Tool-less update</b> (Update ohne Tools) in den BIOS-Einstellungen auf <b>Auto</b> (Automatisch) festgelegt sein.
<code>hptc-bios-flash -h</code>	Zeigt eine Liste der Optionen an.

# C Ändern der Größe der Flash-Laufwerk-Partition

 **WICHTIG:** HP Thin Clients, die mit HP ThinPro ausgeliefert werden, verwenden das gesamte Flash-Laufwerk. Die Image-Aufzeichnungsmethoden zeichnen ein möglichst kleines Image auf. Dadurch können Images von größeren Flash-Laufwerken auf kleineren Flash-Laufwerken bereitgestellt werden, die über ausreichend Speicherplatz für das aufgezeichnete Image verfügen. Eine Änderung der Größe der Partition des Flash-Laufwerks sollte für HP Thin Clients nicht mehr erforderlich sein, die mit HP ThinPro ausgeliefert werden. Beachten Sie für Thin Clients mit HP ThinPro, die aus einem bestimmten Grund nicht das gesamte Flash-Laufwerk verwenden, die folgenden Informationen.

Um den gesamten Speicherplatz des Flash-Laufwerks zu verwenden, müssen Sie die Größe der Partition anpassen und das Dateisystem erweitern, sodass es diesen zusätzlichen Platz aufnimmt. Dies können Sie mit dem Skript `resize-image` über einen X-Terminal erreichen.

 **HINWEIS:** Wenn ein Image über HPDM, HP ThinState oder Automatic Update bereitgestellt wurde, wird das Dateisystem automatisch angepasst, um den gesamten verfügbaren Speicherplatz auf dem Flash-Laufwerk zu verwenden.

Die folgende Tabelle beschreibt die Syntax des Skripts `resize-image`.

Syntax	Beschreibung
<code>resize-image</code>	Wenn dieses Skript ohne Parameter aufgerufen wird, zeigt es die aktuelle Größe der Partition und die Größe des verfügbaren Speicherplatzes auf dem Flash-Laufwerk an. Das Skript fordert Sie auf, die Ziel-Partitionsgröße einzugeben und die Änderung zu bestätigen. Die Änderung wird nach dem nächsten Neustart des Thin Clients wirksam.  <b>HINWEIS:</b> Es ist nicht möglich, die Größe der Partition zu verringern. Der eingegebene Wert muss größer als die aktuelle Partitionsgröße sein.
<code>resize-image --size <i>SizeinMB</i></code> Beispiel: <code>resize-image --size 1024</code>	Mit dieser Syntax können Sie die Ziel-Partitionsgröße in Megabyte (MB) als Parameter angeben und die Änderung anschließend bestätigen.
<code>resize-image --no-prompt</code> – oder – <code>resize-image --no-prompt --size <i>SizeinMB</i></code> Beispiel: <code>resize-image --no-prompt --size 1024</code>	Mit dieser Syntax wird das Skript automatisch ausgeführt, ohne dass ein Benutzereingriff erforderlich ist.  Wenn keine bestimmte Größe gleichzeitig als Parameter eingegeben wurde, wird die Größe der Partition auf die Maximalgröße erhöht.  <b>TIPP:</b> Dieser nicht-interaktive Modus ist nützlich für die Skripterstellung und das Durchführen dieses Vorgangs über ein Remote-Verwaltungstool, wie z. B. den HP Device Manager.

# D Registrierungsschlüssel

Die HP ThinPro-Registrierungsschlüssel sind in Ordnern gruppiert und können auf unterschiedliche Arten geändert werden:

- Verwenden einer **\_File and Registry** -Task in HPDM
- Mithilfe der Komponente Registry Editor von Profile Editor und der anschließenden Bereitstellung des neuen Profils
- Mithilfe des Registrierungs-Editors der HP ThinPro-Benutzeroberfläche, der durch die Eingabe `regeditor` in einem X-Terminal geöffnet wird

Jeder Abschnitt der obersten Ebene in diesem Anhang entspricht einem Registrierungsordner der obersten Ebene.

 **HINWEIS:** Einige Registrierungsschlüssel gelten möglicherweise nur für ThinPro oder Smart Zero.

## Audio

Registrierungsschlüssel	Beschreibung
<code>root/Audio/AdjustSoundPath</code>	Legt den vollständigen Pfad auf den wiedergegebenen Sound fest, wenn die Wiedergabelautstärke über die Lautstärkereglung geändert wird.
<code>root/Audio/JackRetask</code>	Dieser Registrierungsschlüssel gilt nur für t730. Damit kann der Audiobuchse bei Bedarf eine neue Funktion zugewiesen werden. Wenn der Wert 0 ist, gibt es keine Änderung. Wenn der Wert 1 ist, funktioniert die Buchse als Headsetbuchse. Wenn der Wert 2 ist, funktioniert die Buchse als Kopfhörer- und Mikrofonbuchse. Möglicherweise müssen Sie das System zweimal neu starten oder herunterfahren, damit die neue Einstellung funktioniert.
<code>root/Audio/OutputMute</code>	Wenn der Wert 1 ist, sind die internen Lautsprecher und die Kopfhörerbuchse stumm geschaltet.
<code>root/Audio/OutputScale</code>	Bestimmt die Lautstärke-Skalierung für die internen Lautsprecher und die Kopfhörerbuchse, die zwischen 1 und 400 liegt.
<code>root/Audio/OutputScaleAuto</code>	Wenn der Wert 1 ist, wird der <code>OutputScale</code> -Wert automatisch basierend auf dem Thin Client-Modell gesetzt.
<code>root/Audio/OutputVolume</code>	Legt die Lautstärke für die internen Lautsprecher und die Kopfhörerbuchse fest, die zwischen 1 bis 100 liegt.
<code>root/Audio/PlaybackDevice</code>	Legt fest, dass das Gerät für die Wiedergabe verwendet wird.
<code>root/Audio/RecordDevice</code>	Legt fest, dass das Gerät für die Aufzeichnung verwendet wird.
<code>root/Audio/RecordMute</code>	Wenn auf 1 gesetzt, ist das Mikrofon stumm geschaltet.
<code>root/Audio/RecordScale</code>	Legt die Lautstärkekalierung für die Mikrofonbuchse fest, die zwischen 1 und 400 liegt.
<code>root/Audio/RecordScaleAuto</code>	Wenn der Wert 1 ist, wird der <code>RecordScale</code> -Wert automatisch basierend auf dem Thin Client-Modell gesetzt.

Registrierungsschlüssel	Beschreibung
root/Audio/RecordVolume	Legt die Lautstärke für die Mikrofonbuchse fest, die zwischen 1 bis 100 liegt.
root/Audio/VisibleInSystray	Wenn der Wert 1 ist, dann ist ein Lautsprechersymbol in der Taskleiste sichtbar.

## CertMgr

Diese Kategorie wird intern verwendet und muss keine benutzerdefinierten Einträge aufweisen.

## ConnectionManager

Registrierungsschlüssel	Beschreibung
root/ConnectionManager/customLogoPath	
root/ConnectionManager/defaultConnection	Um eine Verbindung beim Start ordnungsgemäß zu starten, muss dies als eine gültige Verbindung im Format <i>Type: Label</i> festgelegt werden, wie im folgenden Beispiel gezeigt: <code>xen:DefaultConnection</code>
root/ConnectionManager/minHeight	
root/ConnectionManager/minWidth	
root/ConnectionManager/splashLogoPath	Zeigt den vollständigen Pfad zum Standard-Image an, während eine Verbindung geladen wird.
root/ConnectionManager/useKioskMode	
root/ConnectionManager/useSplashOnConnectionStartup	Bei Einstellung des Werts auf 1 wird das durch <code>splashLogoPath</code> festgelegte Image aktiviert. Standardmäßig wird dies für ThinPro aktiviert und für Smart Zero deaktiviert.

## ConnectionType

### custom

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/authorizations/user/add	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/custom/authorizations/user/general	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/custom/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/custom/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/custom/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/custom/connections/<UUID>/autoReconnect	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/custom/connections/<UUID>/autoReconnectDelay	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
root/ConnectionType/custom/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/custom/connections/<UUID>/autostartDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
root/ConnectionType/custom/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/custom/connections/<UUID>/command	Gibt den Hauptbefehl für die benutzerdefinierte Verbindung an.
root/ConnectionType/custom/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/custom/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/custom/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/custom/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/custom/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/custom/connections/&lt;UUID&gt;/waitForNetwork</code>	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
<code>root/ConnectionType/custom/coreSettings/USBrelevant</code>	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
<code>root/ConnectionType/custom/coreSettings/appName</code>	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/custom/coreSettings/className</code>	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/custom/coreSettings/editor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/custom/coreSettings/generalSettingsEditor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/custom/coreSettings/icon16Path</code>	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
<code>root/ConnectionType/custom/coreSettings/icon32Path</code>	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
<code>root/ConnectionType/custom/coreSettings/icon48Path</code>	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
<code>root/ConnectionType/custom/coreSettings/label</code>	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmü der Verbindungstypen angezeigt wird.
<code>root/ConnectionType/custom/coreSettings/priorityInConnectionLists</code>	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
<code>root/ConnectionType/custom/coreSettings/serverRequired</code>	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
<code>root/ConnectionType/custom/coreSettings/stopProcess</code>	Das Verhalten, das auftreten sollte, wenn <code>connection_mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/gui/CustomManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/gui/CustomManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/gui/CustomManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget <b>Automatische Verbindungswiederherstellung</b> in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/autostart	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/command	Zum Einstellen des Status für das Widget <b>Auszuführenden Befehl eingeben</b> in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget <b>Alternative Verbindung</b> in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget <b>Symbol auf Desktop anzeigen</b> in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/label	Zum Einstellen des Status für das Widget <b>Name</b> in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das

Registrierungsschlüssel	Beschreibung
	Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/custom/gui/CustomManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget <b>Vor der Anmeldung auf Netzwerkverbindung warten</b> in Custom Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

## firefox

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/firefox/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/firefox/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/address</code>	Legt die URL- oder IP-Adresse für die Verbindung an.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/autoReconnectDelay</code>	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/autostartDelay</code>	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
<code>root/ConnectionType/firefox/connections/&lt;UUID&gt;/beforeStartingCommand</code>	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/connections/<UUID>/enablePrintDialog	Wenn der Wert 1 ist, kann der Dialog „Drucken“ des Webbrowsers verwendet werden.
root/ConnectionType/firefox/connections/<UUID>/enableSmartCard	Wenn der Wert 1 ist, ist die Smart Card-Anmeldung für Citrix-Verbindungen aktiviert, die über den Internetbrowser erstellt werden.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/firefox/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/firefox/connections/<UUID>/forbiddenFiles	Dieser Registrierungsschlüssel funktioniert nur, wenn <b>Allow connections to manage their own settings</b> (Verbindungen die Verwaltung der eigenen Einstellungen ermöglichen) im Web Browser Connection General Settings Manager aktiviert ist. Die Dateien, die im Wert dieses Registrierungsschlüssels aufgeführt sind, werden entfernt, sobald eine Web Browser-Verbindung beendet wurde. Die Dateinamen sollte durch Kommas getrennt werden und ein Platzhalter wird unterstützt. Beispiel: *.rdf,cookies.sqlite
root/ConnectionType/firefox/connections/<UUID>/fullscreen	Wenn der Wert 1 ist, startet der Webbrowser im Vollbildmodus. Wenn <code>KioskMode</code> deaktiviert ist, ist die Benutzeroberfläche des Browsers im Vollbildmodus zugänglich.
root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/intendedUse	Legt die vorgesehene Nutzung dieser Web Browser-Verbindung auf Citrix, RDP oder Internet fest.
root/ConnectionType/firefox/connections/<UUID>/kioskMode	Wenn der Wert 1 ist, wird der Internetbrowser im Kioskmodus gestartet, was bedeutet, dass der Internetbrowser im Vollbildmodus gestartet wird, (selbst wenn <code>fullscreen</code> auf 0 eingestellt ist) und die Benutzeroberfläche des Browsers nicht zur Verfügung steht.
root/ConnectionType/firefox/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/firefox/connections/<UUID>/showBackForwardButton	Wenn der Wert 1 ist, werden die Schaltflächen „Zurück“ und „Vorwärts“ des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showHomeButton	Wenn der Wert 1 ist, wird die Schaltfläche „Startseite“ des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/connections/<UUID>/showSearchBar	Wenn der Wert 1 ist, wird die Suchleiste des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showTabsBar	Wenn der Wert 1 ist, werden Registerkarten des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showTaskBar	Wenn der Wert 1 ist, wird die Taskleiste des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/showUrlBarRefreshButton	Wenn der Wert 1 ist, werden die URL-Leiste und die Schaltfläche „Aktualisieren“ des Internetbrowsers angezeigt, wenn der Kioskmodus aktiviert ist.
root/ConnectionType/firefox/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/firefox/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/firefox/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/firefox/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/firefox/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/firefox/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/firefox/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/firefox/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der

Registrierungsschlüssel	Beschreibung
	Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/firefox/coreSettings/restartIdleTime	Legt die Zeit in Minuten fest, bevor der Webbrowser neu gestartet wird, wenn das System keine Benutzereingabe erhält. Wenn der Wert 0 ist, ist Neustart deaktiviert.
root/ConnectionType/firefox/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/firefox/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/firefox/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/general/enableUserChanges	Wenn der Wert 1 ist, werden die Einstellungen, die im Dialog Firefox-Einstellungen konfiguriert sind, nach jeder Sitzung gespeichert.
root/ConnectionType/firefox/gui/FirefoxManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Zum Einstellen des Status für das Widget <b>URL</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget <b>Automatische Verbindungswiederherstellung</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung

Registrierungsschlüssel	Beschreibung
	<code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog</code>	Zum Einstellen des Status für das Widget <b>Druckdialog aktivieren</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection</code>	Zum Einstellen des Status für das Widget <b>Alternative Verbindung</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget <b>Symbol auf Desktop anzeigen</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/kioskMode</code>	Zum Einstellen des Status für das Widget <b>Kiosk-Modus aktivieren</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/label</code>	Zum Einstellen des Status für das Widget <b>Name</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/showBackForwardButton</code>	Zum Einstellen des Status für das Widget <b>Schaltfläche „Zurück“ und „Vorwärts“ anzeigen</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/showHomeButton</code>	Zum Einstellen des Status für das Widget <b>Schaltfläche „Startseite“ anzeigen</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/showSearchBar</code>	Zum Einstellen des Status für das Widget <b>Suchleiste anzeigen</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung

Registrierungsschlüssel	Beschreibung
	<code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/showTabsBar</code>	Zum Einstellen des Status für das Widget <b>Registerkartenleiste anzeigen</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/showTaskBar</code>	Zum Einstellen des Status für das Widget <b>Taskleiste anzeigen</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/showUrlBarRefreshButton</code>	Zum Einstellen des Status für das Widget <b>URL-Leiste und Aktualisierungsschaltfläche anzeigen</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/startMode</code>	Zum Einstellen des Status für das Widget <b>Vollbildmodus aktivieren</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/firefox/gui/FirefoxManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget <b>Vor der Anmeldung auf Netzwerkverbindung warten</b> in Web Browser Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

## freerdp

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/freerdp/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/freerdp/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/ExtraArgs</code>	Gibt zusätzliche Argumente zum Xfreerdp-Client an. Führen Sie <code>xfreerdp -help</code> über ein X-Terminal aus, um alle verfügbaren Argumente zu sehen.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/SingleSignOn</code>	
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/address</code>	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll. Die Portnummer kann nach einem Doppelpunkt am Ende angehängt werden. Beispiel: <code>servername:3389</code>
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/application</code>	Gibt eine alternative Shell oder Anwendung an, die ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/attachToConsole</code>	
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/audioLatency</code>	Legt den durchschnittlichen Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln fest.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/autoReconnectDelay</code>	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/autostartDelay</code>	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/bandwidthLimitation</code>	Wenn der Wert größer als 0 ist, stellt der Wert eine ungefähre Bandbreitenbegrenzung für das Herunter- und Hochladen in Kilobytes pro Sekunde dar. Ist der Wert 0 (Standardwert), gibt es keine Begrenzung.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/beforeStartingCommand</code>	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/clipboardExtension</code>	Bei Einstellung des Werts auf 1, ist die Zwischenablage sowohl zwischen verschiedenen RDP-Sitzungen als auch zwischen RDP-Sitzungen und dem lokalen System aktiviert.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/compression</code>	Bei Einstellung des Werts auf 1, wird die Komprimierung von RDP-Daten zwischen dem Client und dem Server aktiviert.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/freerdp/connections/<UUID>/directory	Gibt das Systemstart-Verzeichnis an, in dem eine alternative Shell-Anwendung ausgeführt wird.
root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX	Wenn die Einstellung 1 ist, wird die Multimedia-Umleitung deaktiviert, wenn eine gültige RemoteFX-Sitzung aufgebaut wurde.
root/ConnectionType/freerdp/connections/<UUID>/domain	Legt die Standarddomäne fest, die während der Anmeldung für den Remote-Host benötigt wird. Wenn keine Domäne angegeben ist, wird die Standarddomäne für den Remote-Host verwendet.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/freerdp/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount	Legt die Anzahl der Videoframes fest, die der Server pushen kann, ohne auf eine Bestätigung vom Client zu warten. Niedrigere Zahlen führen zu einem schneller reagierenden Desktop, jedoch auch zu einer niedrigeren Bildfrequenz. Bei Einstellung des Werts auf 0 wird die Frame-Bestätigung bei den Client-Server-Interaktionen nicht verwendet.
root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress	Legt den RD-Gateway-Servernamen oder die Adresse fest.
root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain	Legt die Standarddomäne fest, die während der Anmeldung vom RD-Gateway benötigt wird. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn <code>GatewayUsesSameCredentials</code> auf 1 eingestellt ist, wird dieser Wert deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled	Bei Einstellung des Werts auf 1 wird die Verwendung des RD-Gateway erwartet.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword	Gibt das Standardkennwort an, das vom RD-Gateway während der Anmeldung benötigt wird. Dieser Wert ist normalerweise verschlüsselt. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn <code>GatewayUsesSameCredentials</code> auf 1 eingestellt ist, wird dieser Wert deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPort	Gibt die Portnummer an, die bei Kontaktaufnahme mit den RDP-Server zu verwenden ist. Dieser Schlüssel kann leer gelassen werden. Der am häufigsten verwendete Wert ist 443.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUser	Gibt den Standard-Benutzernamen an, der vom Gateway während der Anmeldung benötigt wird. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn <code>GatewayUsesSameCredentials</code> auf 1 eingestellt ist, wird dieser Wert deaktiviert.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/gatewayUsesSameCredentials	Bei Einstellung des Werts auf 1 verwendet das Gerät zur Herstellung einer Verbindung zum RD-Gateway dieselben Anmeldeinformationen, die auch zur Verbindung mit dem endgültigen Server verwendet werden.
root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo	Dieser Wert ist der Lastenausgleich-Cookie, der zu Vermittlungszwecken beim Herstellen einer Verbindung an den Server gesendet wird und entspricht dem Feld <code>Loadbalanceinfo</code> in der Datei <code>.rdp</code> . Der Standardwert ist leer.
root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection	Bei Einstellung des Werts auf 1 werden die lokalen nicht-USB-Speicherpartitionen über die <code>Storage</code> zum Remote-Host umgeleitet. Wenn der Wert 0 ist, ist die Erweiterung für nicht-USB-Speicher Partitionen deaktiviert, die nicht von HP ThinPro verwendet werden.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld <b>Domain</b> (Domäne) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/password	Wenn der Wert 1 ist, wird das Feld <b>Password</b> (Kennwort) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen <b>Remember me</b> (Anmeldedaten merken) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/showpassword	Wenn der Wert 1 ist, wird die Schaltfläche <b>Show password</b> (Kennwort anzeigen) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird die Schaltfläche angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird die Schaltfläche ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/smartcard	Wenn der Wert 1 ist, wird das Kontrollkästchen <b>Smart card login</b> (Smart Card-Anmeldung) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet. Dieses Kontrollkästchen wird möglicherweise nicht angezeigt, wenn keine Smart Card erkannt wird, auch wenn diese Option aktiviert ist.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/username	Wenn der Wert 1 ist, wird das Feld <b>User Name</b> (Benutzername) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/mouseMotionEvents	Bei Einstellung des Werts auf 0 werden Mausbewegungsereignisse nicht an den Server gesendet. Dies kann dazu führen, dass einige Benutzerfeedbacks, wie z. B. Quickinfos, nicht richtig funktionieren.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/offScreenBitmaps	Bei Einstellung des Werts auf 0 werden Off-Screen-Bitmaps deaktiviert. Dies kann die Leistung etwas erhöhen, bewirkt aber, dass die Bildschirmblöcke asynchron aktualisiert werden, wodurch auch Übergänge nicht gleichmäßig aktualisiert werden.
root/ConnectionType/freerdp/connections/<UUID>/password	Legt das Standardkennwort fest, das der Remote-Host während der Anmeldung benötigt. Dieser Wert ist normalerweise verschlüsselt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagDesktopComposition	Die Einstellung des Werts 1 ermöglicht die Desktopgestaltung, wie z. B. durchsichtige Rahmen, wenn dies vom Server unterstützt wird. Das Ausschalten der Desktopgestaltung kann die Leistung für Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagFontSmoothing	Die Einstellung des Werts 1 ermöglicht eine Schriftglättung, wenn dies vom Server unterstützt wird und aktiviert ist. Das Ausschalten dieser Option kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorSettings	Die Einstellung des Werts 1 deaktiviert das Blinken des Cursors, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorShadow	Die Einstellung des Werts 1 schaltet den Mauscursor-Schatten aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoMenuAnimations	Die Einstellung des Werts 1 schaltet Menüanimationen aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoTheming	Die Einstellung des Werts 1 schaltet die Designs der Benutzeroberfläche aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWallpaper	Die Einstellung des Werts 1 schaltet die Desktop-Hintergrundbilder aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWindowDrag	Die Einstellung des Werts 1 schaltet die Option zum Ziehen von Fenstern mit vollem Inhalt aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Stattdessen werden die Fensterumrisse verwendet. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/portMapping	Wenn der Wert 1 ist, werden alle seriellen und parallelen Anschlüsse über die Erweiterung der Ports zum Remote-Host weitergeleitet. Durch die Einstellung 0 wird die Erweiterung deaktiviert.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/printerMapping</code>	Wenn der Wert 1 ist, werden alle lokal über CUPS definierten Drucker über die <code>Printers</code> zum Remote-Host weitergeleitet werden. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Wenn der Wert 2 ist, werden USB-Drucker entsprechend der Konfiguration im USB-Manager weitergeleitet.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdWebFeed/autoDisconnectTimeout</code>	Legt die Anzahl von Minuten fest, die ohne Ausführung einer RemoteApp- und Desktop-Ressource verstreichen kann, bevor die Verbindung automatisch beendet wird. Ein Countdown-Zähler wird während der letzten 20 Sekunden angezeigt, sodass der Benutzer die Möglichkeit hat, den Timer zu deaktivieren. Ist der Wert 0 (Standardwert), ist der Timer deaktiviert.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdWebFeed/autoStartSingleResource</code>	Wenn der Wert 1 ist und wenn nur eine einzige veröffentlichte Ressource (RemoteApp-Programm oder virtueller Desktop) vom Server zurückgegeben wird, wird diese Ressource automatisch gestartet.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdWebFeed/filter/&lt;UUID&gt;/alias</code>	Gibt den Alias einer Ressource für den Ressourcenfilter an. RemoteApp- und Desktopressourcen mit einem passenden Alias sind für Benutzer verfügbar.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdWebFeed/filter/&lt;UUID&gt;/name</code>	Gibt den Namen einer Ressource für den Ressourcenfilter an. RemoteApp- und Desktopressourcen mit einem passenden Namen sind für Benutzer verfügbar.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdWebFeed/keepResourcesWindowOpened</code>	Wenn der Wert 0 ist, wird das Ressourcenauswahlfenster automatisch geschlossen, nachdem eine Ressource gestartet wurde. Wenn der Wert 1 ist, bleibt das Ressourcenauswahlfenster geöffnet, nachdem Ressourcen gestartet wurden. Dies ermöglicht es dem Benutzer, mehrere Ressourcen zu starten, bevor das Ressourcenauswahlfenster geschlossen wird.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdWebFeed/trustedPublisherSha1Thumbprints</code>	Gibt eine durch Kommas getrennte Liste der SHA1-Fingerabdrücke vertrauenswürdiger Herausgeber von Ressourcen an. Beachten Sie, dass ein Zertifikat nicht überprüft wird, das mit einem dieser Fingerabdrücke übereinstimmt. Importieren Sie zur Erhöhung der Sicherheit die Stamm-CA des Herausgebers. Weitere Informationen finden Sie unter dem Registrierungsschlüssel <code>verifyPublisherSignature</code> und im Zertifikat-Manager in der Systemsteuerung.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdWebFeed/verifyPublisherSignature</code>	Wenn der Wert 1 ist, wird die Signatur des Herausgebers überprüft, sofern sie in veröffentlichten RDP-Dateien verfügbar ist. Nur Ressourcen mit einer gültigen Signatur von einem vertrauenswürdigen Herausgeber können ausgeführt werden. Wenn der Wert 0 ist, wird die Signatur nicht überprüft. Weitere Informationen finden Sie unter dem Registrierungsschlüssel <code>trustedPublisherSha1Thumbprints</code> .
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdp6Buffering</code>	Wenn der Wert 1 ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdp8Codecs</code>	Wenn der Wert 1 ist, werden RDP 8-Codecs verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der RDP 8-Codecs deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdpEncryption</code>	Bei Einstellung des Werts auf 1 wird die Standard-RDP-Verschlüsselung zum Verschlüsseln aller Daten zwischen dem Client und Server verwendet.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdpH264Codec</code>	Wenn der Wert 1 ist, werden RDP 8 H.264-Codecs verwendet, wenn verfügbar. Für diese Einstellung gibt es bekannte visuelle

Registrierungsschlüssel	Beschreibung
	Fehler, insbesondere bei Konfigurationen mit mehreren Monitoren, daher sollte sie als experimentell und nicht unterstützt betrachtet werden. Durch Aktivieren dieser Einstellung wird einfach der Server darauf hingewiesen, dass der Thin Client H.264 für die Desktopanzeige unterstützt. Der Server muss auch H.264 unterstützen und der Server trifft die endgültige Entscheidung darüber, welche Codecs verwendet werden. Diese Einstellung wirkt sich nur auf die Desktop-Codecs aus. Codecs für die Multimedia-Umleitung sind davon nicht betroffen.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdpProgressiveCodec</code>	Wenn der Wert 1 ist, werden progressive RDP 8-Codecs verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der progressiven RDP 8-Codecs deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/redirectPreference</code>	Zur Umleitung erhält der RDP-Client verschiedene mögliche Ziele. Diese werden normalerweise in der folgenden Reihenfolge ausprobiert: FQDN, primäre IP, IP-Liste, NetBIOS. Wenn FQDN nicht gewünscht ist, kann eine der Alternativen zuerst ausprobiert werden, indem dieser Registrierungsschlüssel festgelegt wird. Wenn diese Methode nicht funktioniert, wird auf dem RDP-Client wieder die ursprüngliche Reihenfolge herangezogen. Mit der Einstellung <code>auto</code> wird die ursprüngliche Reihenfolge erzwungen.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/remoteApp</code>	Gibt den Namen einer verfügbaren Anwendung an, die im RAIL-Modus (Remote Application Integrated Locally) ausgeführt werden soll.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/remoteDesktopService</code>	Wenn der Wert <code>Remote Computer</code> ist, wird eine direkte RDP-Verbindung mit einem Remotecomputer hergestellt. Wenn der Wert <code>RD Web Access</code> ist, wird zuerst eine Verbindung mit einem RD Web Access-Dienst hergestellt, um einen Feed der veröffentlichte RemoteApp-Ressourcen abzurufen.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/remoteFx</code>	Wenn der Wert 1 ist, wird RemoteFX in der Form von RDP 7.1 verwendet, wenn verfügbar. Diese Einstellung ist veraltet und ist möglicherweise in einer zukünftigen Version von HP ThinPro nicht mehr enthalten. Diese Einstellung sollte nur bei einem Fehler des RemoteFX-Protokolls deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/seamlessWindow</code>	Bei Einstellung des Werts auf 1 sind die Fensterdekorationen deaktiviert. Dies kann in einer Konfiguration mit mehreren Monitoren wünschenswert sein, um die Einstellung der Verbindung auf die Größe des primären Monitors zu ermöglichen.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/securityLevel</code>	Legt die Sicherheitsstufen von Zertifikaten fest. Wenn der Wert 0 ist, sind alle Verbindungen zulässig. Wenn der Wert 1 ist, werden beibehaltene Hosts überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 2 ist, werden beibehaltene Hosts nicht überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 3 ist, werden alle unsichere Verbindungen verweigert.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/sendHostname</code>	Legt den Thin Client-Hostnamen fest, der an den Remote-Host gesendet wird. Wenn keine Eintragung vorgenommen wird, wird der System-Host-Namen gesendet. Der Registrierungsschlüssel <code>root/ConnectionType/freerdp/general/sendHostname</code> muss auf <code>hostname</code> eingestellt sein, damit dieser Schlüssel verwendet wird.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/showConnectionGraph	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, wird beim Starten der Sitzung ein separates Programm gestartet, um den Verbindungszustand grafisch darzustellen.
root/ConnectionType/freerdp/connections/<UUID>/showRDPDashboard	Ist der Wert 1, wenn die Sitzung gestartet wird, werden in einem gesonderten Fenster RDP-Leistung und -Status angezeigt.
root/ConnectionType/freerdp/connections/<UUID>/smartcard	Wenn der Wert 1 ist, ist die lokale Smart Card-Authentifizierung zum Remote-Host zulässig. Zurzeit wird dadurch Network Level Authentication (NLA) deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/sound	Durch die Einstellung 1 werden die Wiedergabe- und Aufnahmegereäte über die Erweiterung von Audio zum Remote-Host umgeleitet. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Wenn der Wert 2 ist, werden USB-Audiogeräte entsprechend der Konfiguration im USB-Manager weitergeleitet. In der Regel, empfiehlt HP, dass dieser Wert auf 1 gesetzt wird, sodass High-Level-Audio-Umleitung verwendet wird. Dadurch wird die Audioqualität verbessert und sichergestellt, dass Client-Audio, das mittels anderer Methoden umgeleitet wird (wie zum Beispiel <code>Multimedia Redirection</code> ), den lokalen Audioeinstellungen entspricht.
root/ConnectionType/freerdp/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/freerdp/connections/<UUID>/timeoutError	Legt die Anzahl von Millisekunden fest, die nach dem Verlust einer Verbindung gewartet werden, bevor der Versuch, eine Verbindung mit dem Server herzustellen, aufgegeben wird. Wenn der Wert 0 ist, dann wird immer wieder versucht, die Verbindung wieder herzustellen.
root/ConnectionType/freerdp/connections/<UUID>/timeoutRecovery	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung für die Wiederherstellung des Netzwerkbetriebs vergehen, bevor versucht wird eine erneute Verbindung zu erzwingen.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarning	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung mit dem Server vergehen, bevor der Benutzer gewarnt wird, dass die Verbindung getrennt wurde.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarningDialog	Wenn der Wert 1 ist, dann wird ein Dialogfeld angezeigt, wenn ein Abfallen einer Ende-zu-Ende-Verbindung erkannt wird, und das Display wird grau. Andernfalls werden Nachrichten in das Verbindungsprotokoll geschrieben und die Sitzung fährt sich fest.
root/ConnectionType/freerdp/connections/<UUID>/timeoutsEnabled	Wenn der Wert 1 ist, dann sind die Health-Tests der Ende-zu-Ende-Verbindung abgeschlossen.
root/ConnectionType/freerdp/connections/<UUID>/tlsVersion	Legt die Transport Layer Security-Version fest, die in den Anfangsphasen der Aushandlung mit dem RDP-Server verwendet wird. Legen Sie diese Option auf die TLS-Version Ihres RDP-Servers fest oder verwenden Sie <code>auto</code> .  <b>HINWEIS:</b> Durch einige Serverfehler auf einigen ungepatchten RDP-Servern kann die automatische Einstellung zu einem Fehler führen, deshalb ist es nicht die Standardeinstellung.
root/ConnectionType/freerdp/connections/<UUID>/usbMiscRedirection	Bei Einstellung des Werts auf 0 ist die Umleitung für alle USB-Geräte deaktiviert, ausgenommen jener, die über <code>sound</code> , <code>printerMapping</code> , <code>portMapping</code> , <code>usbStorageRedirection</code> und

Registrierungsschlüssel	Beschreibung
	<code>localPartitionRedirection</code> gehandhabt werden. Wenn der Wert 2 ist, werden alle anderen USB-Geräte zum Remotehost umgeleitet, wie im USB-Manager konfiguriert.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/usbStorageRedirection</code>	Wenn der Wert 1 ist, werden alle USB-Speichergeräte über die Storage-Erweiterung zum Remote-Host weitergeleitet werden. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Wenn der Wert 2 ist, werden USB-Speichergeräte entsprechend der Konfiguration im USB-Manager weitergeleitet.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/username</code>	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/waitForNetwork</code>	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/windowMode</code>	Bei einer Einstellung auf <code>Remote Application</code> wird RDP im Remote Application Integrated Local (RAIL) ausgeführt. Dies erfordert, dass der RemoteApp-Server die gewünschte Anwendung als Remoteanwendung ausführen kann. Die Anwendung wird in einem separaten Fenster innerhalb der Desktop-Umgebung angezeigt, sodass es wirkt, als wäre die Anwendung Teil des lokalen Systems. Siehe auch den Registrierungsschlüssel <code>RemoteApp</code> . Bei einer Einstellung auf <code>Alternate Shell</code> wird eine nicht-standardmäßige Shell aufgerufen. Siehe auch die Registrierungsschlüssel <code>application</code> und <code>directory</code> .
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/windowSizeHeight</code>	
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/windowSizePercentage</code>	
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/windowSizeWidth</code>	
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/windowType</code>	
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/x11Capture</code>	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, werden X11-Vorgänge für eine spätere Wiedergabe aufgezeichnet.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/x11CaptureDir</code>	Dies ist eine Diagnosefunktion. Mit diesem Wert wird das Verzeichnis für X11-Aufzeichnungsdateien festgelegt.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/x11LogAutoflush</code>	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, wird die X11-Protokolldatei häufiger auf den Datenträger übertragen.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/x11Logfile</code>	Dies ist eine Diagnosefunktion. Mit dem Wert wird der Pfad der X11-Protokolldatei festgelegt.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/x11Logging</code>	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, werden X11-Vorgänge protokolliert.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/x11Synchronous</code>	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, werden X11-Vorgänge nicht gepuffert.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/xkbLayoutId</code>	Legt eine XKB-Layout-ID für die Umgehung der Systemtastatur fest. Um Zugriff auf die Liste der verfügbaren IDs zu erhalten, geben Sie Folgendes in ein X-Terminal ein: <code>xfreerdp --kbd-list</code> .
<code>root/ConnectionType/freerdp/coreSettings/USBrelevant</code>	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
<code>root/ConnectionType/freerdp/coreSettings/appName</code>	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/freerdp/coreSettings/className</code>	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning</code>	Wenn der Wert 1 ist, generiert das Betriebssystem keinen Dialog, der angibt, dass das Netzwerk ausgefallen ist, da das Verbindungsprotokoll solche Situationen bearbeitet.
<code>root/ConnectionType/freerdp/coreSettings/editor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manger für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/freerdp/coreSettings/generalSettingsEditor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/freerdp/coreSettings/icon16Path</code>	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
<code>root/ConnectionType/freerdp/coreSettings/icon32Path</code>	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
<code>root/ConnectionType/freerdp/coreSettings/icon48Path</code>	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
<code>root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout</code>	Legt die Anzahl der Sekunden fest, die gewartet werden, um eine erste Reaktion vom RDP-Server zu erhalten, bis der Versuch aufgegeben wird.
<code>root/ConnectionType/freerdp/coreSettings/label</code>	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
<code>root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists</code>	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
<code>root/ConnectionType/freerdp/coreSettings/stopProcess</code>	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch

Registrierungsschlüssel	Beschreibung
	<code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
<code>root/ConnectionType/freerdp/coreSettings/watchPid</code>	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/freerdp/coreSettings/wrapperScript</code>	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/freerdp/general/autoReconnectDialogTimeout</code>	Wenn <code>AutoReconnect</code> aktiviert ist, ist dies die Anzahl der Sekunden, bevor Fehlerdialoge für die Verbindung ein Zeitlimit erreichen. Wenn der Wert 0 ist, warten die Dialogen unbegrenzt auf eine Benutzerinteraktion.
<code>root/ConnectionType/freerdp/general/disablePasswordChange</code>	Wenn eine Remote-Anmeldung aufgrund fehlerhafter Anmeldeinformationen fehlschlägt, wird dem Benutzer eine Schaltfläche angezeigt, die ein Dialogfeld öffnet, um das Kennwort zu aktualisieren. Wenn diese Taste auf 1 eingestellt ist, werden die Schaltfläche und das Dialogfeld nicht angezeigt.
<code>root/ConnectionType/freerdp/general/enableMMR</code>	Bei Einstellung des Werts auf 1 wird die <code>Multimedia Redirection</code> aktiviert, sodass unterstützte Codecs, die über den Windows Media Player abgespielt werden, an den Client umgeleitet werden. Dies verbessert erheblich die Videowiedergabe im Vollbild- und High-Definition-Modus für Codecs wie z. B. WMV9, VC1 und MPEG4.
<code>root/ConnectionType/freerdp/general/preferredAudio</code>	Legt das Standard-Audio-Backend für High-Level-Audio-Umleitung (sowohl Ein- als auch Ausgang) fest.
<code>root/ConnectionType/freerdp/general/rdWebFeedUrlPattern</code>	Legt das Muster fest, das verwendet wird, um die RD Web-Access-URL zu erstellen. Der Host der URL, z. B. <code>myserver.com</code> , wird durch den Wert im Feld <b>Address</b> (Adresse) der Verbindung ersetzt. Dieses Muster wird nicht verwendet, wenn die Adresse bereits eine URL ist.
<code>root/ConnectionType/freerdp/general/sendHostname</code>	Wenn <code>hostname</code> eingestellt ist, wird der System-Hostname an den Remote-Host gesendet. Dies wird in der Regel verwendet, um den mit einer bestimmten RDP-Sitzung verknüpften Thin Client zu identifizieren. Der gesendete Host-Name kann mit <code>sendHostname</code> in den verbindungs-spezifischen Einstellungen außer Kraft gesetzt werden. Bei der Einstellung <code>mac</code> wird die MAC-Adresse des ersten verfügbaren Netzwerkadapters anstelle des Hostnamen gesendet.
<code>root/ConnectionType/freerdp/general/serialPortsDriver</code>	Diese Einstellung sorgt für eine bessere Kompatibilität mit der erwarteten zugrunde liegenden Windowstreiber <code>SerCx2.sys</code> , <code>SerCx.sys</code> oder <code>Serial.sys</code> .
<code>root/ConnectionType/freerdp/general/serialPortsPermissive</code>	Wenn der Wert 1 ist, dann werden Fehler für nicht unterstützte Funktionen ignoriert.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/ssh/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/ssh/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/address</code>	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/application</code>	Gibt die Anwendung an, die ausgeführt werden soll.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/autoReconnectDelay</code>	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/autostartDelay</code>	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/backgroundColor</code>	Gibt die Hintergrundfarbe der Verbindung an.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/beforeStartingCommand</code>	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/compression</code>	Aktiviert die Komprimierung für eine SSH-Verbindung.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/connectionEndAction</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/ssh/connections/&lt;UUID&gt;/coord</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/ssh/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/ssh/connections/<UUID>/font	Gibt die Schriftgröße für die Verbindung an.
root/ConnectionType/ssh/connections/<UUID>/foregroundColor	Gibt die Vordergrundfarbe der Verbindung an.
root/ConnectionType/ssh/connections/<UUID>/fork	Wenn die Auswahl 1 ist, dann ist die Option <b>Fork into background</b> (Prozess in den Hintergrund verschieben) für die Verbindung aktiviert.
root/ConnectionType/ssh/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/ssh/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/ssh/connections/<UUID>/port	Gibt die Portnummer an, die bei der Verbindungsherstellung mit dem SSH-Server verwendet wird. Die Standardeinstellung ist 22.
root/ConnectionType/ssh/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/ssh/connections/<UUID>/tty	Wenn die Auswahl 1 ist, dann ist die Option <b>TTY Zuordnung erzwingen</b> für die Verbindung aktiviert ist.
root/ConnectionType/ssh/connections/<UUID>/username	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/ssh/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/ssh/connections/<UUID>/x11	Wenn der Wert 1 ist, dann ist die Option <b>X11 Verbindung leitet weiter</b> für die Verbindung aktiviert.
root/ConnectionType/ssh/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/ssh/coreSettings/appName</code>	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/ssh/coreSettings/className</code>	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/ssh/coreSettings/editor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/ssh/coreSettings/icon16Path</code>	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
<code>root/ConnectionType/ssh/coreSettings/icon32Path</code>	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
<code>root/ConnectionType/ssh/coreSettings/icon48Path</code>	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
<code>root/ConnectionType/ssh/coreSettings/label</code>	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
<code>root/ConnectionType/ssh/coreSettings/priorityInConnectionLists</code>	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
<code>root/ConnectionType/ssh/coreSettings/serverRequired</code>	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
<code>root/ConnectionType/ssh/coreSettings/stopProcess</code>	Das Verhalten, das auftreten sollte, wenn <code>connection_mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
<code>root/ConnectionType/ssh/coreSettings/watchPid</code>	Wenn der Wert 1 ist, wird die unter dem Namen <code>appName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/ssh/coreSettings/wrapperScript</code>	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/ssh/gui/SshManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/ssh/gui/SshManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/gui/SshManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/gui/SshManager/widgets/address	Zum Einstellen des Status für das Widget <b>Address</b> (Adresse) in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/application	Zum Einstellen des Status für das Widget <b>Anwendung ausführen</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget <b>Automatische Verbindungswiederherstellung</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/autostart	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor	Zum Einstellen des Status für das Widget <b>Hintergrundfarbe</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/compression	Zum Einstellen des Status für das Widget <b>Komprimierung</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget <b>Alternative Verbindung</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/font	Zum Einstellen des Status für das Widget <b>Schriftart</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird

Registrierungsschlüssel	Beschreibung
	das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/foregroundColor</code>	Zum Einstellen des Status für das Widget <b>Vordergrundfarbe</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/fork</code>	Zum Einstellen des Status für das Widget <b>In den Hintergrund verschieben</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget <b>Symbol auf Desktop anzeigen</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/isInMenu</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/label</code>	Zum Einstellen des Status für das Widget <b>Name</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/port</code>	Zum Einstellen des Status für das Widget <b>Port</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/tty</code>	Zum Einstellen des Status für das Widget <b>TTY Zuordnung erzwingen</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/ssh/gui/SshManager/widgets/username</code>	Zum Einstellen des Status für das Widget <b>Benutzername</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/gui/SshManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget <b>Vor der Anmeldung auf Netzwerkverbindung warten</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/x11	Zum Einstellen des Status für das Widget <b>X11 Verbindung leitet weiter</b> in Secure Shell Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

## teemtalk

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/authorizations/user/add	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/teemtalk/authorizations/user/general	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/teemtalk/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/teemtalk/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/teemtalk/connections/<UUID>/autoReconnect	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/teemtalk/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/teemtalk/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/teemtalk/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/teemtalk/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/teemtalk/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/teemtalk/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/teemtalk/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/teemtalk/connections/<UUID>/systembeep	Wenn der Wert 1 ist, dann sind Systemsignale für die Verbindung aktiviert.
root/ConnectionType/teemtalk/connections/<UUID>/ttsName	Gibt den TeemTalk-Profilnamen an.
root/ConnectionType/teemtalk/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/teemtalk/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/teemtalk/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/teemtalk/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/teemtalk/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/teemtalk/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstin­stallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/teemtalk/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/teemtalk/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/teemtalk/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/gui/TeemtalkManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/gui/TeemtalkManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/gui/TeemtalkManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget <b>Automatische Verbindungswiederherstellung</b> in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autostart	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung

Registrierungsschlüssel	Beschreibung
	<code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget <b>Symbol auf Desktop anzeigen</b> in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/isInMenu</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/label</code>	Zum Einstellen des Status für das Widget <b>Name</b> in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget <b>Vor der Anmeldung auf Netzwerkverbindung warten</b> in TeemTalk Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

## telnet

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/telnet/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/telnet/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/telnet/connections/&lt;UUID&gt;/address</code>	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll.
<code>root/ConnectionType/telnet/connections/&lt;UUID&gt;/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/telnet/connections/&lt;UUID&gt;/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/telnet/connections/&lt;UUID&gt;/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/telnet/connections/&lt;UUID&gt;/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/telnet/connections/&lt;UUID&gt;/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
root/ConnectionType/telnet/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/telnet/connections/<UUID>/backgroundColor	Gibt die Hintergrundfarbe der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/telnet/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/telnet/connections/<UUID>/font	Gibt die Schriftgröße für die Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/foregroundColor	Gibt die Vordergrundfarbe der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/telnet/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/telnet/connections/<UUID>/locale	Gibt das Gebietsschema der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/port	Gibt die Portnummer an, die bei der Verbindungsherstellung mit dem Server verwendet wird. Die Standardeinstellung ist 23.
root/ConnectionType/telnet/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/telnet/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/telnet/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/telnet/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/telnet/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/telnet/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmü der Verbindungstypen angezeigt wird.
root/ConnectionType/telnet/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/telnet/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/telnet/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection_mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/telnet/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/gui/TelnetManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/telnet/gui/TelnetManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/telnet/gui/TelnetManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/address</code>	Zum Einstellen des Status für das Widget <b>Adresse</b> in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/autoReconnect</code>	Zum Einstellen des Status für das Widget <b>Automatische Verbindungswiederherstellung</b> im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor</code>	Zum Einstellen des Status für das Widget <b>Hintergrundfarbe</b> im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection</code>	Zum Einstellen des Status für das Widget <b>Alternative Verbindung</b> in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor</code>	Zum Einstellen des Status für das Widget <b>Vordergrundfarbe</b> im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget <b>Symbol auf Desktop anzeigen</b> im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/label</code>	Zum Einstellen des Status für das Widget <b>Name</b> in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer

Registrierungsschlüssel	Beschreibung
	kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/port</code>	Zum Einstellen des Status für das Widget <b>Port</b> im Telnet-Verbindungs-Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget <b>Vor der Anmeldung auf Netzwerkverbindung warten</b> in Telnet Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

## view

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/view/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/view/authorizations/user/commandLineBox</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Eingeben von Befehlszeilenargumenten in VMware Horizon View Connection Manager.
<code>root/ConnectionType/view/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/ExtraArgs</code>	Gibt zusätzliche Argumente zum VMware Horizon View-Client an. Führen Sie <code>view_client --help</code> oder <code>vmware-view --help</code> über ein X-Terminal aus, um alle verfügbaren Argumente anzuzeigen.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/SingleSignOn</code>	
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/appInMenu</code>	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung im Menü der Taskleiste angezeigt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/appOnDesktop</code>	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung auf dem Desktop angezeigt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/applicationSize</code>	Legt die Größe fest, in der VMware Horizon View-Client Anwendungen startet.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/attachToConsole</code>	

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/view/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/view/connections/<UUID>/autoReconnect	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/view/connections/<UUID>/autoReconnectDelay	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
root/ConnectionType/view/connections/<UUID>/automaticLogin	Wenn der Wert 1 ist, dann wird der VMware Horizon View-Client versuchen, sich automatisch anzumelden, wenn alle Felder zur Verfügung stehen. Wenn der Wert 0 ist, müssen Benutzer im VMware Horizon View-Client manuell <b>Connect</b> (Verbinden) auswählen, sich anmelden und einen Desktop auswählen.
root/ConnectionType/view/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/view/connections/<UUID>/autostartDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.
root/ConnectionType/view/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/view/connections/<UUID>/closeAfterDisconnect	Bei Einstellung des Werts auf 1 wird die Verbindung beendet, nachdem der erste Desktop geschlossen wurde. Bei Einstellung des Werts auf 0 wird der VMware Horizon View-Client zum Desktop-Auswahl-Bildschirm zurückkehren. Dies ist standardmäßig aktiviert, um zu verhindern, dass Benutzer versehentlich die Verbindung auf dem Desktop-Auswahl-Bildschirm bestehen lassen, nachdem sie sich abgemeldet haben.
root/ConnectionType/view/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/view/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/view/connections/<UUID>/desktop	Wenn angegeben, wird der benannte Desktop beim Anmelden automatisch gestartet. Standardmäßig wird, wenn nur ein Desktop verfügbar ist, dieser Desktop automatisch gestartet, ohne dass er angegeben werden muss.
root/ConnectionType/view/connections/<UUID>/desktopSize	Legt die Größe fest, in der der VMware Horizon View-Client den Desktop startet.
root/ConnectionType/view/connections/<UUID>/directory	
root/ConnectionType/view/connections/<UUID>/disableMaximizedApp	Wenn der Wert 1 ist, dann sind die Einstellungen für die Fenstergröße bei maximierten Anwendungen deaktiviert.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/<UUID>/domain	Legt die Domäne fest, die dem View Connection Server zur Verfügung gestellt wird. Wenn keine Domäne angegeben ist, wird die Standarddomäne für den Server verwendet.
root/ConnectionType/view/connections/<UUID>/enableSingleMode	
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/view/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/view/connections/<UUID>/fullscreen	Wenn der Wert 1 ist, dann startet der VMware Horizon View-Client im Vollbildmodus, wenn er gestartet wird.
root/ConnectionType/view/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/view/connections/<UUID>/hideMenuBar	Bei Einstellung des Werts auf 1 wird die obere Menüleiste innerhalb des Desktops ausgeblendet. Diese Leiste wird zur Verwaltung von Remote-Geräten und zum Starten anderer Desktops verwendet.
root/ConnectionType/view/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/view/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/view/connections/<UUID>/lockServer	Wenn der Wert 1 ist, können Endbenutzer die Serveradresse nicht ändern.
root/ConnectionType/view/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld <b>Domain</b> (Domäne) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/password	Wenn der Wert 1 ist, wird das Feld <b>Password</b> (Kennwort) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen <b>Remember me</b> (Anmeldedaten merken) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/showpassword	Wenn der Wert 1 ist, wird die Schaltfläche <b>Show password</b> (Kennwort anzeigen) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird die Schaltfläche angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird die Schaltfläche ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/smartcard	Wenn der Wert 1 ist, wird das Kontrollkästchen <b>Smart card login</b> (Smart Card-Anmeldung) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das

Registrierungsschlüssel	Beschreibung
	Kontrollkästchen ausgeblendet. Dieses Kontrollkästchen wird möglicherweise nicht angezeigt, wenn keine Smart Card erkannt wird, auch wenn diese Option aktiviert ist.
root/ConnectionType/view/connections/<UUID>/loginfields/username	Wenn der Wert 1 ist, wird das Feld <b>User Name</b> (Benutzername) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/view/connections/<UUID>/password	Legt das Standardkennwort fest, das der Remote-Host während der Anmeldung benötigt. Dieser Wert ist normalerweise verschlüsselt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/view/connections/<UUID>/preferredProtocol	Legt das bevorzugte Protokoll fest.
root/ConnectionType/view/connections/<UUID>/saveCredentials	
root/ConnectionType/view/connections/<UUID>/server	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll. In der Regel ist dies eine URL, wie z. B. <code>http://server.domain.com</code> .
root/ConnectionType/view/connections/<UUID>/sessionEndAction	
root/ConnectionType/view/connections/<UUID>/singleDesktop	
root/ConnectionType/view/connections/<UUID>/smartCardModules/CoolKeyPK11	Legt das Coolkey PKCS #11-Modul fest.
root/ConnectionType/view/connections/<UUID>/smartCardModules/GemaltoDotNet	Legt das Gemalto .NET-Modul fest,
root/ConnectionType/view/connections/<UUID>/smartcard	Wenn der Wert 1 ist, dann werden hierdurch alle lokal angeschlossenen Smart Cards an den Remote-Host weitergeleitet, damit sie von Anwendungen auf dem Remote-Host verwendet werden können. Dies ermöglicht nur Smart Card-Anmeldungen für den Remote-Host, nicht für View Connection Server.
root/ConnectionType/view/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/view/connections/<UUID>/username	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/view/connections/<UUID>/viewSecurityLevel	Wenn der Standard <code>Refuse insecure connections</code> eingestellt ist, erlaubt der VMware Horizon View-Client dem Benutzer nicht, sich mit dem Server zu verbinden, wenn das SSL-Zertifikat des Servers ungültig ist. Wenn <code>Warn</code> eingestellt ist, gibt der VMware Horizon View-Client eine Warnung aus, wenn das Zertifikat des Servers nicht überprüft werden kann und wenn es selbstsigniert oder abgelaufen ist. Dem Benutzer wird weiterhin keine Verbindung erlaubt. Wenn die Einstellung <code>Allow all connections</code> ist, wird das Serverzertifikat nicht überprüft und Verbindungen zu jedem beliebigen Server werden zugelassen.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/attachToConsole	
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/audioLatency	Legt den durchschnittlichen Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln fest.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/clipboardExtension	Wenn der Wert 1 ist, ist die Zwischenablage sowohl zwischen verschiedenen RDP-Sitzungen als auch zwischen RDP-Sitzungen und dem lokalen System aktiviert.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/colorDepth	Diese Einstellung ist veraltet. Sie wird verwendet, um die Farbtiefe der Verbindung zu reduzieren, sodass sie unterhalb der nativen Desktopauflösung liegt. Häufig wurde diese verwendet, um die Netzwerkbandbreite zu reduzieren. Die Verringerung der Farbtiefe auf eine Stufe, die nicht vom Videotreiber unterstützt wird, führt möglicherweise zu Bildschirmstörungen oder zu Startfehlern.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/compression	Bei Einstellung des Werts auf 1, wird die Komprimierung von RDP-Daten zwischen dem Client und dem Server aktiviert.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/disableMMRwithRFX	Wenn die Einstellung 1 ist, wird die Multimedia-Umleitung deaktiviert, wenn eine gültige RemoteFX-Sitzung aufgebaut wurde.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/frameAcknowledgeCount	Legt die Anzahl der Videoframes fest, die der Server pushen kann, ohne auf eine Bestätigung vom Client zu warten. Niedrigere Zahlen führen zu einem schneller reagierenden Desktop, jedoch auch zu einer niedrigeren Bildfrequenz. Bei Einstellung des Werts auf 0 wird die Frame-Bestätigung bei den Client-Server-Interaktionen nicht verwendet.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/enableMMR	Bei Einstellung des Werts auf 1 wird die <b>Multimedia Redirection</b> aktiviert, sodass unterstützte Codecs, die über den Windows Media Player abgespielt werden, an den Client umgeleitet werden. Dies verbessert erheblich die Videowiedergabe im Vollbild- und High-Definition-Modus für Codecs wie z. B. WMV9, VC1 und MPEG4.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname	Wenn <code>hostname</code> eingestellt ist, wird der System-Hostname an den Remote-Host gesendet. Dies wird in der Regel verwendet, um den mit einer bestimmten RDP-Sitzung verknüpften Thin Client zu identifizieren. Der gesendete Host-Name kann mit <code>sendHostname</code> in den verbindungspezifischen Einstellungen außer Kraft gesetzt werden. Bei der Einstellung <code>mac</code> wird die MAC-Adresse des ersten verfügbaren Netzwerkadapters anstelle des Hostnamen gesendet.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo	Dieser Wert ist der Lastenausgleich-Cookie, der zu Vermittlungszwecken beim Herstellen einer Verbindung an den Server gesendet wird und entspricht dem Feld <code>Loadbalanceinfo</code> in der Datei <code>.rdp</code> . Der Standardwert ist leer.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents	Bei Einstellung des Werts auf 0 werden Mausbewegungsereignisse nicht an den Server gesendet. Dies kann dazu führen, dass einige Benutzerfeedbacks, wie z. B. Quickinfos, nicht richtig funktionieren.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/offScreenBitmaps</code>	Bei Einstellung des Werts auf 0 werden Off-Screen-Bitmaps deaktiviert. Dies kann die Leistung etwas erhöhen, bewirkt aber, dass die Bildschirmblöcke asynchron aktualisiert werden, wodurch auch Übergänge nicht gleichmäßig aktualisiert werden.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagDesktopComposition</code>	Die Einstellung des Werts 1 ermöglicht die Desktopgestaltung, wie z. B. durchsichtige Rahmen, wenn dies vom Server unterstützt wird. Das Ausschalten der Desktopgestaltung kann die Leistung für Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagFontSmoothing</code>	Die Einstellung des Werts 1 ermöglicht eine Schriftglättung, wenn dies vom Server unterstützt wird und aktiviert ist. Das Ausschalten dieser Option kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagNoCursorSettings</code>	Die Einstellung des Werts 1 deaktiviert das Blinken des Cursors, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagNoCursorShadow</code>	Die Einstellung des Werts 1 schaltet den Mauscursor-Schatten aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagNoMenuAnimations</code>	Die Einstellung des Werts 1 schaltet Menüanimationen aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagNoTheming</code>	Die Einstellung des Werts 1 schaltet die Designs der Benutzeroberfläche aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagNoWallpaper</code>	Die Einstellung des Werts 1 schaltet die Desktop-Hintergrundbilder aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/perfFlagNoWindowDrag</code>	Die Einstellung des Werts 1 schaltet die Option zum Ziehen von Fenstern mit vollem Inhalt aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Stattdessen werden die Fensterumrisse verwendet. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/portMapping</code>	Bei Einstellung des Werts auf 1 werden die folgenden lokalen seriellen und parallelen Ports zum Remote-Host umgeleitet: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/printerMapping</code>	Wenn der Wert 1 ist, werden alle lokal über CUPS definierten Drucker zum Remote-Host weitergeleitet.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdp6Buffering</code>	Wenn der Wert 1 ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdp8Codecs</code>	Wenn der Wert 1 ist, werden RDP 8-Codex verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der RDP 8-Codex deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codex deaktiviert werden.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/rdpEncryption</code>	Bei Einstellung des Werts auf 1 wird die Standard-RDP-Verschlüsselung zum Verschlüsseln aller Daten zwischen dem Client und Server verwendet.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdpH264Codec</code>	Wenn der Wert 1 ist, werden RDP H.264-Codex verwendet, wenn verfügbar. Für diese Einstellung gibt es bekannte visuelle Fehler, insbesondere bei Konfigurationen mit mehreren Monitoren, daher sollte sie als experimentell und nicht unterstützt betrachtet werden. Durch Aktivieren dieser Einstellung wird einfach der Server darauf hingewiesen, dass der Thin Client H.264 für die Desktopanzeige unterstützt. Der Server muss auch H.264 unterstützen und der Server trifft die endgültige Entscheidung darüber, welche Codex verwendet werden. Diese Einstellung wirkt sich nur auf die Desktop-Codex aus. Codex für die Multimedia-Umleitung sind davon nicht betroffen.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/rdpProgressiveCodec</code>	Wenn der Wert 1 ist, werden progressive RDP 8-Codex verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der progressiven RDP 8-Codex deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codex deaktiviert werden.
<code>root/ConnectionType/freerdp/connections/&lt;UUID&gt;/redirectPreference</code>	Zur Umleitung erhält der RDP-Client verschiedene mögliche Ziele. Diese werden normalerweise in der folgenden Reihenfolge ausprobiert: FQDN, primäre IP, IP-Liste, NetBIOS. Wenn FQDN nicht gewünscht ist, kann eine der Alternativen zuerst ausprobiert werden, indem dieser Registrierungsschlüssel festgelegt wird. Wenn diese Methode nicht funktioniert, wird auf dem RDP-Client wieder die ursprüngliche Reihenfolge herangezogen. Mit der Einstellung <code>auto</code> wird die ursprüngliche Reihenfolge erzwungen.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/remoteFx</code>	Wenn der Wert 1 ist, dann wird RemoteFX verwendet, wenn verfügbar.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/securityLevel</code>	Legt die Sicherheitsstufen von Zertifikaten fest. Wenn der Wert 0 ist, sind alle Verbindungen zulässig. Wenn der Wert 1 ist, werden beibehaltene Hosts überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 2 ist, werden beibehaltene Hosts nicht überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 3 ist, werden alle unsichere Verbindungen verweigert.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/sendHostname</code>	Legt den Thin Client-Hostnamen fest, der an den Remote-Host gesendet wird. Wenn keine Eintragung vorgenommen wird, wird der System-Host-Namen gesendet. Der Registrierungsschlüssel <code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/general/sendHostname</code> muss auf <code>hostname</code> eingestellt sein, damit diese Taste verwendet werden kann.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/sound</code>	Durch die Standardeinstellung <code>Bring to this computer</code> wird der Sound mithilfe eines virtuellen Kanals vom Remote-Host zum Client umgeleitet. Durch die Einstellung <code>Leave at remote computer</code> verbleibt der Sound am Remote-Host. Dies kann nützlich sein, wenn ein USB-umgeleitetes Audiogerät verwendet wird. Durch die Einstellung auf irgendeinen anderen Wert, wird Audio deaktiviert. In der Regel empfiehlt HP, den Wert <code>Bring to this computer</code> einzustellen und USB-

Registrierungsschlüssel	Beschreibung
	Wiedergabegeräte nicht zum Remote-Host umzuleiten. Dadurch wird die Audioqualität verbessert und sichergestellt, dass Client-Audio, das mittels anderer Methoden umgeleitet wird (wie zum Beispiel <code>Multimedia Redirection</code> ), den lokalen Audioeinstellungen entspricht.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/timeoutError</code>	Legt die Anzahl von Millisekunden fest, die nach dem Verlust einer Verbindung gewartet werden, bevor der Versuch eine Verbindung mit dem Server herzustellen aufgegeben wird. Wenn der Wert 0 ist, dann wird immer wieder versucht, die Verbindung wieder herzustellen.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/timeoutRecovery</code>	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung für die Wiederherstellung des Netzwerkbetriebs vergehen, bevor versucht wird eine erneute Verbindung zu erzwingen.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/timeoutWarning</code>	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung mit dem Server vergehen, bevor der Benutzer gewarnt wird, dass die Verbindung getrennt wurde.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/timeoutWarningDialog</code>	Wenn der Wert 1 ist, dann wird ein Dialogfeld angezeigt, wenn ein Abfallen einer Ende-zu-Ende-Verbindung erkannt wird, und das Display wird grau. Andernfalls werden Nachrichten in das Verbindungsprotokoll geschrieben und die Sitzung fährt sich fest.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/timeoutsEnabled</code>	Wenn der Wert 1 ist, dann sind die Health-Tests der Ende-zu-Ende-Verbindung abgeschlossen.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/tlsVersion</code>	Legt die Transport Layer Security-Version fest, die in den Anfangsphasen der Aushandlung mit dem RDP-Server verwendet wird. Legen Sie diese Option auf die TLS-Version Ihres RDP-Servers fest oder verwenden Sie „auto“.  <b>HINWEIS:</b> Durch einige Serverfehler auf einigen ungepatchten RDP-Servern kann die automatische Einstellung zu einem Fehler führen, deshalb ist es nicht die Standardeinstellung.
<code>root/ConnectionType/view/connections/&lt;UUID&gt;/xfreerdpOptions/xkbLayoutId</code>	Legt eine XKB-Layout-ID für die Umgehung der Systemtastatur fest. Um Zugriff auf die Liste der verfügbaren IDs zu erhalten, geben Sie Folgendes in ein X-Terminal ein: <code>xfreerdp --kbd-list</code> .
<code>root/ConnectionType/view/coreSettings/USBrelevant</code>	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
<code>root/ConnectionType/view/coreSettings/appName</code>	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/view/coreSettings/className</code>	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/view/coreSettings/editor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/view/coreSettings/icon16Path</code>	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
<code>root/ConnectionType/view/coreSettings/icon32Path</code>	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/view/coreSettings/icon48Path</code>	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
<code>root/ConnectionType/view/coreSettings/label</code>	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmü der Verbindungstypen angezeigt wird.
<code>root/ConnectionType/view/coreSettings/priorityInConnectionLists</code>	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinatation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
<code>root/ConnectionType/view/coreSettings/serverRequired</code>	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
<code>root/ConnectionType/view/coreSettings/stopProcess</code>	Das Verhalten, das auftreten sollte, wenn <code>connection_mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
<code>root/ConnectionType/view/coreSettings/watchPid</code>	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/view/coreSettings/wrapperScript</code>	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/view/general/rdpOptions</code>	Die hier angegebenen Optionen werden direkt an den RDP-Client weitergeleitet, wenn RDP als Anzeigeprotokoll für die VMware Horizon View-Verbindung verwendet wird. Um eine vollständige Liste der Optionen anzuzeigen, geben Sie den folgenden Befehl in ein X-Terminal ein: <code>rdesktop --help</code>
<code>root/ConnectionType/view/gui/viewManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/view/gui/viewManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/view/gui/viewManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/view/gui/viewManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in VMware Horizon View Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung

Registrierungsschlüssel	Beschreibung
	<code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection</code>	Zum Einstellen des Status für das Widget <b>Alternative Verbindung</b> in VMware Horizon View Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/view/gui/viewManager/widgets/label</code>	Zum Einstellen des Status für das Widget <b>Name</b> in VMware Horizon View Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

## xdmcp

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xdmcp/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/xdmcp/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/address</code>	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/beforeStartingCommand</code>	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/color</code>	Legt die Farbtiefe für die Anzeige der Verbindung fest.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/xdmcp/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/xdmcp/connections/<UUID>/fontServer	Legt die Adresse des zu verwendenden Schriftartenservers fest. Der Registrierungsschlüssel <code>useFontServer</code> muss auch auf 1 eingestellt werden.
root/ConnectionType/xdmcp/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/xdmcp/connections/<UUID>/refreshRate	Legt die Bildwiederholungsrate für das Display der Verbindung fest.
root/ConnectionType/xdmcp/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/xdmcp/connections/<UUID>/type	Gibt den XDMCP-Verbindungstyp an. Durch die Einstellung <code>chooser</code> werden alle verfügbaren Hosts aufgelistet und der Benutzer kann wählen, zu welchem eine Verbindung hergestellt werden soll. Durch die Einstellung <code>query</code> wird eine XDMCP-Anforderung direkt zum angegebenen Host gesendet. Durch die Einstellung <code>broadcast</code> werden alle verfügbaren Hosts aufgelistet und es wird automatisch eine Verbindung mit dem erste Host hergestellt.
root/ConnectionType/xdmcp/connections/<UUID>/useFontServer	Bei Einstellung des Werts auf 1 wird der Schriftartenserver aktiviert. Bei Einstellung des Werts auf 0 wird die lokale Schriftart verwendet.
root/ConnectionType/xdmcp/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xdmcp/connections/&lt;UUID&gt;/windowSize</code>	Gibt die Fenstergröße für die Verbindung an.
<code>root/ConnectionType/xdmcp/coreSettings/USBrelevant</code>	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
<code>root/ConnectionType/xdmcp/coreSettings/appName</code>	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xdmcp/coreSettings/audio</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xdmcp/coreSettings/className</code>	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xdmcp/coreSettings/desktopButton</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xdmcp/coreSettings/editor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xdmcp/coreSettings/icon16Path</code>	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
<code>root/ConnectionType/xdmcp/coreSettings/icon32Path</code>	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
<code>root/ConnectionType/xdmcp/coreSettings/icon48Path</code>	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
<code>root/ConnectionType/xdmcp/coreSettings/label</code>	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
<code>root/ConnectionType/xdmcp/coreSettings/priorityInConnectionLists</code>	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungs-Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Ersteinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
<code>root/ConnectionType/xdmcp/coreSettings/serverRequired</code>	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
<code>root/ConnectionType/xdmcp/coreSettings/stopProcess</code>	Das Verhalten, das auftreten sollte, wenn <code>connection-mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch

Registrierungsschlüssel	Beschreibung
	<code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
<code>root/ConnectionType/xmcp/coreSettings/watchPid</code>	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xmcp/coreSettings/wrapperScript</code>	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xmcp/gui/XmcpManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xmcp/gui/XmcpManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xmcp/gui/XmcpManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/address</code>	Zum Einstellen des Status für das Widget <b>Adresse</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/autoReconnect</code>	Zum Einstellen des Status für das Widget <b>Automatische Verbindungswiederherstellung</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/color</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/fontServer</code>	Zum Einstellen des Status für das Widget <b>Schriftartenserver</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget <b>Symbol auf Desktop anzeigen</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung

Registrierungsschlüssel	Beschreibung
	<code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/isInMenu</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/label</code>	Zum Einstellen des Status für das Widget <b>Name</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/refreshRate</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/type</code>	Zum Einstellen des Status für das Widget <b>Typ</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/useFontServer</code>	Zum Einstellen des Status für das Widget <b>Schriftartenserver verwenden</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget <b>Vor der Anmeldung auf Netzwerkverbindung warten</b> in XDMCP Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xmcp/gui/XmcpManager/widgets/windowSize</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

## xen

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/authorizations/user/add</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/xen/authorizations/user/general</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über Connection Manager. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/SingleSignOn</code>	Wenn der Wert 1 ist, verwendet die Verbindung die gleichen Anmeldeinformationen wie der Bildschirmschoner.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/address</code>	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll. In der Regel ist dies eine URL, wie z. B. <code>http://server.domain.com</code> .
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/afterStartedCommand</code>	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/afterStoppedCommand</code>	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/anonymousLogin</code>	Wenn der Wert 1 ist, dann ist eine anonyme Anmeldung für PNAgent und direkte Verbindungen zulässig.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/appInMenu</code>	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung im Menü der Taskleiste angezeigt.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/appOnDashboard</code>	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung in der Taskleiste angezeigt.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/appOnDesktop</code>	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung auf dem Desktop angezeigt.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/authorizations/user/edit</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/authorizations/user/execution</code>	Wenn der Wert 1 ist, hat ein Endbenutzer die Berechtigung zum Ausführen dieser Verbindung.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autoLaunchSingleApp</code>	Wenn der Wert 1 ist und wenn nur eine einzige veröffentlichte Anwendung oder Desktop vom Citrix-Server zurückgegeben wird, wird diese Ressource automatisch gestartet.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autoReconnect</code>	Wenn der Wert 1 ist, wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autoReconnectAppsOnLogin</code>	Bei Einstellung des Werts auf 1 versucht das System nach einer Erstanmeldung alle aktiven oder getrennten Citrix-Sitzungen wiederherzustellen.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autoReconnectDelay</code>	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> auf 1 eingestellt ist.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autoRefreshInterval</code>	Steuert die Zeit in Sekunden, bevor die Ressourcen gelöscht und vom Server erneut aktualisiert werden. Stellen Sie zum Deaktivieren den Wert -1 ein. Es ist in der Regel nicht erforderlich, die Ressourcen häufig vom Server zu aktualisieren.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autoStartDesktop</code>	Wenn der Wert 1 und <code>autoStartResource</code> leer ist, wird der erste Desktop, der beim Starten der Verbindung zur Verfügung steht, automatisch geöffnet.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autoStartResource</code>	Legt den Namen des Desktops oder der Anwendung fest, der oder die automatisch startet, wenn die Verbindung gestartet wird.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autostart</code>	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/autostartDelay</code>	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn <code>autostart</code> auf 1 eingestellt ist.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/beforeStartingCommand</code>	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/connectionEndAction</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/connectionMode</code>	Legt den Citrix-Verbindungsmodus für die Verbindung fest.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/coord</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/dependConnectionId</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/disableSaveCredentials</code>	
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/domain</code>	Die Domäne, die für den XenDesktop-Server bereitgestellt wird. Wenn keine Domäne angegeben ist, wird die Standarddomäne für den Server verwendet.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/enableRSAToken</code>	<b>ACHTUNG:</b> Diese Funktionalität wird nicht unterstützt. Wenn der Wert 1 ist, wird der Benutzer vor dem Verbindungsaufbau aufgefordert, den Wert des Sicherheits-Tokens anzugeben, der beim Authentifizieren mit NetScaler Gateway verwendet werden soll.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/extraEnvValues/&lt;UUID&gt;/key</code>	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/extraEnvValues/&lt;UUID&gt;/value</code>	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/fallBackConnection</code>	Legt die alternative Verbindung über seine UUID fest.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/folder</code>	
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/forceHttps</code>	Wenn der Wert 1 ist, dann sind nur HTTPS-Verbindungen zulässig.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/fullscreen</code>	Wenn der Wert 1 ist, dann wird der Citrix-Client beim Starten im Vollbildmodus geöffnet.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/hasDesktopIcon</code>	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/ignoreCertCheck</code>	Bei Einstellung des Werts auf 1 wird die Überprüfung von Zertifikaten diese Verbindung ignoriert.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/label</code>	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf <code>Default Connection</code> eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/logOnMethod</code>	
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/loginfields/domain</code>	Wenn der Wert 1 ist, wird das Feld <b>Domain</b> (Domäne) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist,

Registrierungsschlüssel	Beschreibung
	wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/password	Wenn der Wert 1 ist, wird das Feld <b>Password</b> (Kennwort) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen <b>Remember me</b> (Anmeldedaten merken) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/showpassword	Wenn der Wert 1 ist, wird die Schaltfläche <b>Show password</b> (Kennwort anzeigen) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird die Schaltfläche angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird die Schaltfläche ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/smartcard	Wenn der Wert 1 ist, wird das Kontrollkästchen <b>Smart card login</b> (Smart Card-Anmeldung) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet. Dieses Kontrollkästchen wird möglicherweise nicht angezeigt, wenn keine Smart Card erkannt wird, auch wenn diese Option aktiviert ist.
root/ConnectionType/xen/connections/<UUID>/loginfields/username	Wenn der Wert 1 ist, wird das Feld <b>User Name</b> (Benutzername) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/password	Legt das Standardkennwort fest, das der Remote-Host während der Anmeldung benötigt. Dieser Wert ist normalerweise verschlüsselt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/xen/connections/<UUID>/requireCredentialsDirectConnect	Wenn der Wert 0 ist, dann werden Anmeldeinformationen nicht benötigt, um eine direkte Verbindung zu initiieren. Jedoch sind Anmeldeinformationen benötigt, um eine Anwendung zu starten.
root/ConnectionType/xen/connections/<UUID>/resListRequest	Wenn der Wert 1 ist, listet eine Verbindung nur die Ressource auf, ohne sie zu starten oder Symbole herunterzuladen.
root/ConnectionType/xen/connections/<UUID>/saveNewUrl	Dies ist ein interner Wert. Wenn der Wert <code>ToBeAsked</code> ist, fragt das Skript den Benutzer. Wenn der Wert <code>Auto</code> ist, fragt das Skript den Benutzer nicht. Ob die URL gespeichert wird, ist fallabhängig. Wenn der Wert <code>Yes</code> ist, hat der Benutzer das Speichern der neuen URL angefordert. Wenn der Wert <code>No</code> ist, hat der Benutzer angefordert, die neue URL nicht zu speichern.
root/ConnectionType/xen/connections/<UUID>/savePassword	
root/ConnectionType/xen/connections/<UUID>/smartCardModuleKey	Gibt das Sicherheitsmodul an, das für eine Smart Card-Verbindung verwendet werden soll.
root/ConnectionType/xen/connections/<UUID>/startMode	Wenn die Standardeinstellung <code>Focus</code> eingestellt ist und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/subscribedOnly</code>	Wenn der Wert 1 ist, werden nur abonnierte Ressourcen für die neue Verbindung angezeigt.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/unplugSmartCardAction</code>	Legt die Aktion fest, die durchgeführt werden soll, wenn eine Smart Card während einer Verbindung ausgesteckt wird. Mit <code>logoff</code> wird die aktuelle Sitzung abgemeldet. Mit <code>close</code> werden alle geöffneten Ressourcen geschlossen. Mit <code>noaction</code> wird keine Aktion ausgeführt.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/username</code>	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
<code>root/ConnectionType/xen/connections/&lt;UUID&gt;/waitForNetwork</code>	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
<code>root/ConnectionType/xen/coreSettings/USBrelevant</code>	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
<code>root/ConnectionType/xen/coreSettings/appName</code>	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch</code>	Diese Einstellung gilt für Citrix-Server mit mehreren veröffentlichten Ressourcen. Bei einem Wert unter 0 wird keine automatische Abmeldung ausgeführt. Andernfalls legt diese Einstellung die Anzahl der Sekunden festgelegt, die zur Verfügung stehen zwischen dem Schließen der letzten von Xen veröffentlichten Ressource und dem automatischen Abmelden des Benutzers und Zurückkehren zum Anmeldebildschirm. Citrix-Prozessverzögerungen können die Zeit bis zur automatischen Abmeldung verlängern.
<code>root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch</code>	Diese Einstellung gilt für Citrix-Server mit mehreren veröffentlichten Ressourcen. Bei einem Wert unter 0 wird keine automatische Abmeldung ausgeführt. Andernfalls legt diese Einstellung die Anzahl der Sekunden festgelegt, die ohne das Starten neuer Anwendungen vergehen bis zum automatischen Abmelden des Benutzers und Zurückkehren zum Anmeldebildschirm. Citrix-Prozessverzögerungen können die Zeit bis zur automatischen Abmeldung verlängern.
<code>root/ConnectionType/xen/coreSettings/className</code>	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xen/coreSettings/editor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn Connection Manager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xen/coreSettings/generalSettingsEditor</code>	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/ConnectionType/xen/coreSettings/icon16Path</code>	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/xen/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/xen/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmü der Verbindungstypen angezeigt wird.
root/ConnectionType/xen/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese in Connection Manager angezeigt wird, und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter in Connection Manager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/xen/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse <code>unused</code> , <code>optional</code> oder <code>required</code> für diesen Verbindungstyp ist.
root/ConnectionType/xen/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn <code>connection_mgr stop</code> für diese Verbindung angefordert wird. Standardmäßig ist dies <code>close</code> , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn <code>kill</code> eingestellt ist, wird der durch den <code>appName</code> angegebene Prozess zum Abbruch gezwungen. Wenn <code>custom</code> eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch <code>wrapperScript</code> , mit dem Argument <code>stop</code> ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/xen/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen <code>AppName</code> angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/CGPTimeout	Legt den Zeitraum in Sekunden fest, in dem der Client versucht, eine CGP-Verbindung erneut herzustellen. Durch das Kopieren einer großen Datei auf oder von einem USB-Laufwerk bleibt die Sitzung für den Zeitraum der CGP-Zeitüberschreitung aktiv. Wenn der Zeitraum der CGP-Zeitüberschreitung zu kurz ist, wird die Sitzung getrennt, während eine große Datei kopiert wird. Bei einem Netzwerkproblem wird während des Zeitraums der CGP-Zeitüberschreitung keine Fehlermeldung angezeigt. Zudem dauert es länger als üblich, bis die Aufforderung zum erneuten Verbindungsaufbau angezeigt wird.
root/ConnectionType/xen/general/TWIMode	Steuert den nahtlosen Modus für veröffentlichte Anwendungen. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>TWIMode</code> direkt zugeordnet.
root/ConnectionType/xen/general/TWIModeResizeType	Diese Einstellung ist der Citrix INI-Dateieinstellung <code>TWIMoveResizeType</code> direkt zugeordnet.
root/ConnectionType/xen/general/allowReadOnA ... allowReadOnZ	Wenn der Wert 1 ist, kann ein Benutzer das zugeordnete Laufwerk lesen.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/ allowWriteOnA ... allowWriteOnZ	Wenn der Wert 1 ist, kann ein Benutzer im zugeordneten Laufwerk auch schreiben.
root/ConnectionType/xen/general/async	Wenn der Wert 1 ist, ist die asynchrone Abfrage aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>CommPollSize</code> direkt zugeordnet.
root/ConnectionType/xen/general/autoReconnect	Bei Einstellung des Werts auf 1 ist das automatische Neuverbinden der Sitzung aktiviert. Dies ist nicht identisch mit dem verbindungs-spezifischen "autoReconnect" (automatisches Neuverbinden). Diese Neuverbindung findet intern statt, innerhalb des Citrix-Clients, ohne Neustart der Verbindung. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>TransportReconnectEnabled</code> direkt zugeordnet.
root/ConnectionType/xen/general/ bitmapCacheSize	Legt die minimale Größe für die Bitmap-Zwischenspeicherung fest. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>PersistentCacheMinBitmap</code> direkt zugeordnet.
root/ConnectionType/xen/general/bottomMonitor	Legt fest, dass auf dem Bildschirmbereich des unteren Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/colorDepth	Erzwingt die Verwendung einer bestimmten Farbtiefe für alle Verbindungen. Dies erfolgt in der Regel entweder in speziellen Umgebungen, in denen die automatische Tiefenauswahl fehlschlägt, oder in sehr langsam Netzwerken, um eine Überlastung zu vermeiden.
root/ConnectionType/xen/general/colorMapping	Bei der Auswahl von <code>Shared - Approximate Colors</code> werden ungefähre Farben aus der Standard-Farbzordnungstabelle verwendet. Bei der Auswahl von <code>Private - Exact Colors</code> werden präzise Farben verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>ApproximateColors</code> direkt zugeordnet.
root/ConnectionType/xen/general/ contentRedirection	Wenn der Wert 1 ist, dann werden Links von Web-Inhalten vom Server an den Client gesendet, so dass der Client versuchen kann, sie lokal zu öffnen.
root/ConnectionType/xen/general/ defaultBrowserProtocol	Steuert das Protokoll, das verwendet wird, um den Host für die Verbindung zu finden. Wenn kein Wert angegeben wird, wird der Standardwert vom Abschnitt <code>[WFClient]</code> der <code>wfclient.ini</code> verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>BrowserProtocol</code> direkt zugeordnet.
root/ConnectionType/xen/general/ drivePathMappedOnA ... drivePathMappedOnZ	Legt das Verzeichnis des lokalen Dateisystems zur Zuordnung zum Remote-Host fest. In der Regel ist dies auf <code>/media</code> eingestellt, damit alle angeschlossenen USB-Laufwerke über einen einzigen Laufwerksbuchstaben dem Remote-Host zugeordnet werden können.
root/ConnectionType/xen/general/ enableAlertSound	Wenn der Wert 1 ist, sind Windows Warntöne aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>DisableSound</code> direkt zugeordnet.
root/ConnectionType/xen/general/ enableClipboard	Wenn der Wert 1 ist, wird die Umleitung der Zwischenablage aktiviert.
root/ConnectionType/xen/general/ enableCursorColors	Bei Einstellung des Werts auf 1 werden farbige Cursor aktiviert. Wenn der Wert 0 ist, können in einigen Fällen grafische Cursorstörungen behoben werden.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/enableDataCompression	Wenn der Wert 1 ist, dann ist Datenkomprimierung aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>Compress</code> direkt zugeordnet.
root/ConnectionType/xen/general/enableDriveMapAndRedirect	Wenn der Wert 1 ist, werden Zuordnung und Umleitung von USB-Speichergeräten aktiviert.
root/ConnectionType/xen/general/enableDriveMapping	Wenn der Wert 1 ist, können Verzeichnisse auf dem lokalen Dateisystem über ein virtuelles Laufwerk zum Remote-Host weitergeleitet werden. Typischerweise würde <code>/media</code> zu <code>Z</code> zugeordnet werden, um ein Weiterleiten von USB-Laufwerken zum Remote-Host zu ermöglichen. Wenn die USB-Umleitung aktiviert ist, sollte diese deaktiviert werden, um Speicherkonflikte zu verhindern. Um auf diese Weise korrekt dem Remote-Host zugeordnet werden zu können, muss das USB-Gerät eines der folgenden Dateisysteme verwenden: FAT32, NTFS, ext2, ext3.
root/ConnectionType/xen/general/enableDynamicDriveMapping	Wenn der Wert 1 ist, werden USB-Speichergeräte auf dem Citrix-Server dynamisch zugeordnet. Bei Einstellung des Werts auf 0 ist die Speichererweiterung für die USB-Speichergeräte deaktiviert.
root/ConnectionType/xen/general/enableForceDirectConnect	Stellen Sie den Wert 1 ein, um die Verbindung zur Citrix-Web-Benutzeroberfläche und PNAgent-Dienste zu umgehen. Die Authentifizierung findet am Server statt, nachdem die erste Verbindung hergestellt wurde.
root/ConnectionType/xen/general/enableH264Compression	Wenn der Wert 1 ist, wird die H.264-Komprimierung aktiviert. Der H.264-Codec bietet mehr Leistung bei umfangreichen und professionellen Grafikanwendungen auf WAN-Netzwerken im Vergleich zum JPEG-Codec.
root/ConnectionType/xen/general/enableHDXFlashRedirection	<b>HINWEIS:</b> Diese Funktion wird nur für die 32-Bit-Version von HP ThinPro unterstützt.  Steuert das Verhalten der HDX Flash-Umleitung. Wenn <code>Always</code> eingestellt ist, dann wird, wenn möglich, die HDX Flash-Umleitung verwendet und der Benutzer wird nicht aufgefordert. Wenn <code>Ask</code> eingestellt ist, dann wird der Benutzer aufgefordert. Durch die Einstellung <code>Never</code> wird diese Funktionalität deaktiviert.
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	<b>HINWEIS:</b> Diese Funktion wird nur für die 32-Bit-Version von HP ThinPro unterstützt.  Steuert das Verhalten des Side Content Fetching (Abrufen der Seiteninhalte) des HDX Flash Servers. Wenn deaktiviert, wird der Client Inhalte abrufen.
root/ConnectionType/xen/general/enableHDXMediaStream	Wenn der Wert 1 ist, dann ist HDX MediaStream aktiviert. In dieser Konfiguration kann für HDX Lync ein Konflikt vorliegen. Wenn der Wert 0 ist, werden Mediendateien weiterhin über Standard-Streaming wiedergegeben, aber die Qualität ist möglicherweise nicht so gut.
root/ConnectionType/xen/general/enableHWH264	Wenn der Wert 1 ist und auch <code>enableH264Compression</code> 1 ist, wird die Hardwarekomprimierung für H.264 aktiviert. Wenn der Wert 0 ist, wird die H.264 Komprimierung von Software bearbeitet.
root/ConnectionType/xen/general/enableMapOnA ... enableMapOnZ	Wenn hier der Wert 1 eingestellt wird, kann diesem Laufwerk auf dem Remote-Host ein lokales Dateisystem zugeordnet werden. Der entsprechende Registrierungsschlüssel <code>DrivePathMappedOn</code> muss auf ein gültiges lokales Verzeichnis eingestellt sein, damit die Laufwerkszuordnung einwandfrei funktioniert.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/enableOffScreenSurface	Wenn der Wert 1 ist, dann kann der Server das Format <code>X PixMap</code> für Offscreen-Zeichnungen verwenden. Reduziert die Bandbreite in 15-Bit- und 24-Bit-Farbe auf Kosten des X-Serverspeichers und der Prozessorzeit. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>EnableOSS</code> direkt zugeordnet.
root/ConnectionType/xen/general/enableSessionReliability	Wenn der Wert 1 ist, wird die Citrix-Sitzungszuverlässigkeit aktiviert. Die Sitzungszuverlässigkeit ändert die Art, wie Sitzungen nach dem Verlust einer Netzwerkverbindung fortgesetzt werden. In der Citrix-Dokumentation finden Sie weitere Informationen zur Sitzungszuverlässigkeit.
root/ConnectionType/xen/general/enableSmallFrames	Wenn der Wert 1 ist, werden kleine Nicht-H.264-Frame-Aktualisierungen für H.264 aktiviert. <code>enableTextTracking</code> muss auch aktiviert sein, damit dies einen Effekt hat.
root/ConnectionType/xen/general/enableSmartCard	Bei Einstellung des Werts auf 1 wird Smart-Card-Anmeldung aktiviert.
root/ConnectionType/xen/general/enableTextTracking	Wenn der Wert 1 ist, werden optimierte verlustfreie Textüberlagerungen für H.264 aktiviert.
root/ConnectionType/xen/general/enableUSBRedirection	Wenn der Wert 1 ist, werden USB-Speichergeräte umgeleitet.
root/ConnectionType/xen/general/enableWindowsAlertSounds	
root/ConnectionType/xen/general/encryptionLevel	Legt die Ebene der Verschlüsselung fest. Die Verschlüsselungsprotokolle für alle Stufen sind im Abschnitt <code>[EncryptionLevelSession]</code> der <code>module.ini</code> definiert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>[EncryptionLevelSession]</code> direkt zugeordnet.
root/ConnectionType/xen/general/fontSmoothingType	Legt die Art der Schriftartglättung fest.
root/ConnectionType/xen/general/hotKey<1thru15>Char	Legt fest, dass die Tastenkombination zur Remote-Sitzung weitergeleitet wird, wenn die Taste bzw. Tastenkombination, die in der entsprechenden <code>HotKeyShift</code> eingerichtet ist, betätigt wird.
root/ConnectionType/xen/general/hotKey<1thru15>Shift	Legt die Taste bzw. Tastenkombination fest, die zur Aktivierung der Tastenkombination dient, die in der entsprechenden <code>HotKeyChar</code> eingerichtet ist.
root/ConnectionType/xen/general/httpAddresses/<UUID>/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Legt die Taste auf der Tastatur zur Deaktivierung des transparenten Tastaturmodus fest. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>KeyPassthroughEscapeChar</code> direkt zugeordnet.
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Legt die Tastatur-Tastenkombination zum Deaktivieren des transparenten Tastaturmodus fest. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>KeyPassthroughEscapeShift</code> direkt zugeordnet.
root/ConnectionType/xen/general/lastComPortNum	Legt die Anzahl der zugeordneten seriellen Ports fest. Wenn der Wert 0 ist, dann ist Zuordnung des seriellen Anschlusses deaktiviert.

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/leftMonitor	Legt fest, dass auf dem Bildschirmbereich des linken Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/localTextEcho	Steuert die Tastatur-Latenzreduktion. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>ZLKeyboardMode</code> direkt zugeordnet.
root/ConnectionType/xen/general/monitorNetwork	Wenn der Wert auf <code>Off</code> eingestellt ist, dann wird die Netzwerkkonnektivität nicht überwacht. Wenn die Einstellung <code>Local network link status only</code> gewählt wurde, wird nur der Local Area Network Linkstatus überwacht. Wenn die Einstellung <code>Server online status</code> gewählt wurde, dann werden sowohl der Local Area Network Linkstatus und die Server-Konnektivität überwacht.
root/ConnectionType/xen/general/mouseClickFeedback	Steuert die Maus-Latenzreduktion. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>ZLMouseMode</code> indirekt zugeordnet.
root/ConnectionType/xen/general/mouseMiddleButtonPaste	Wenn der Wert 1 ist, dann ist die mittlere Maustaste zum Einfügen der Emulation für Windows Sitzungen aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>MouseSendsControlV</code> direkt zugeordnet.
root/ConnectionType/xen/general/noInfoBox	Wenn der Wert 1 ist, dann wird der Client Manager (Wfcmgr) nicht angezeigt, wenn eine Clientsitzung beendet wird. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>PopupOnExit</code> direkt zugeordnet.
root/ConnectionType/xen/general/printerAutoCreation	Durch die Einstellung 0 wird die Druckerzuordnung deaktiviert. Wenn der Wert 1 ist, dann werden lokal definierte Drucker der Verbindung zugeordnet. Wenn der Wert 2 ist, werden USB-Drucker entsprechend der Konfiguration im USB-Manager weitergeleitet.
root/ConnectionType/xen/general/proxyAddress	Die zu verwendende Proxy-Adresse, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist.
root/ConnectionType/xen/general/proxyPassword	Das zu verwendende Proxy-Kennwort, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist. Dieses Kennwort wird mithilfe der rc4-Verschlüsselung verschlüsselt.
root/ConnectionType/xen/general/proxyPort	Der zu verwendende Proxy-Port, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist.
root/ConnectionType/xen/general/proxyType	Wählt den Proxy-typ, der für die XenDesktop-Verbindungen verwendet wird. <code>Use Browser settings</code> wird nur unterstützt, wenn ein lokaler Browser installiert ist.
root/ConnectionType/xen/general/proxyUser	Der zu verwendende Proxy-Benutzername, wenn eine manuelle Proxy-Einstellung über <code>proxyType</code> ausgewählt ist.
root/ConnectionType/xen/general/rightMonitor	Legt fest, dass auf dem Bildschirmbereich des rechten Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/saveLogs	Wenn der Wert 1 ist, werden detaillierte Protokollinformationen gespeichert, nachdem die Sitzung beendet wurde. Diese Protokollinformationen werden im folgenden Verzeichnis gespeichert: <code>/tmp/debug/citrix/&lt;Datum&gt;/</code>
root/ConnectionType/xen/general/serverCheckTimeout	

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/sessionSharingClient	Wenn auf 1 gesetzt, werden Anforderungen zur Sitzungs freigabe an andere Citrix-Sitzungen auf dem gleichen X-Display gesendet. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>EnableSessionSharingClient</code> direkt zugeordnet.
root/ConnectionType/xen/general/showOnAllMonitors	Wenn der Wert 1 ist, wird der virtuelle Desktop auf allen Monitoren angezeigt.
root/ConnectionType/xen/general/smartCardModuleMap/CoolKeyPK11	Gibt den Pfad zum Smart Card-Sicherheitsmodul <code>CoolKey PKCS #11</code> an.
root/ConnectionType/xen/general/smartCardModuleMap/GemaltoDotNet	Gibt den Pfad zum Smart Card-Sicherheitsmodul <code>Gemalto .NET</code> an.
root/ConnectionType/xen/general/smartCardModuleMap/OpenSC	Gibt den Pfad zum Smart Card-Sicherheitsmodul <code>Open SC</code> an.
root/ConnectionType/xen/general/sound	Legt die Audioqualität fest. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>AudioBandwidthLimit</code> indirekt zugeordnet.
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/<UUID>/address	
root/ConnectionType/xen/general/topMonitor	Legt fest, dass auf dem Bildschirmbereich des oberen Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/transparentKeyPassthrough	Steuert, wie bestimmte Windows Tastenkombinationen behandelt werden. Wenn der Wert <code>Translated</code> eingestellt ist, dann gilt die Tastenkombinationen für den lokalen Desktop. Wenn der Wert <code>Direct in full screen desktops only</code> eingestellt ist, dann gilt die Tastenkombinationen nur für die Remote-Sitzung, wenn sich diese im Vollbildmodus befindet. Wenn der Wert <code>Direct</code> eingestellt ist, dann gilt die Tastenkombinationen immer für die Remote-Sitzung gelten, solange das Fenster aktiv ist. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>TransparentKeyPassthrough</code> indirekt zugeordnet.
root/ConnectionType/xen/general/twRedundantImageItems	Regelt die Anzahl der Display-Bereiche, die in Thinwire nachverfolgt werden, um ein überflüssiges Zeichnen von Bitmap-Bildern zu verhindern. Ein ausreichender Wert für 1024 x 768 Sitzungen ist 300.
root/ConnectionType/xen/general/useAlternateAddress	Wenn der Wert 1 ist, dann wird eine alternative Adresse für Firewall Verbindungen verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>UseAlternateAddress</code> direkt zugeordnet.
root/ConnectionType/xen/general/useBitmapCache	Bei Einstellung des Werts auf 1 wird der permanente Disk-Cache aktiviert. Der permanente Disk-Cache speichert häufig verwendete grafische Objekte wie Bitmaps auf der Festplatte des Thin Client. Die Verwendung des permanenten Disk-Cache verbessert die Leistung für Verbindungen mit niedriger Bandbreite, reduziert aber die Größe des verfügbaren Speicherplatzes auf dem Thin Client. Für Thin Clients in Hochgeschwindigkeits-LANs ist die Verwendung des permanenten Disk-Cache nicht notwendig. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>PersistentCacheEnabled</code> direkt zugeordnet.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/general/useEUKS</code>	Regelt die Verwendung von Extended Unicode Keyboard Support (EUKS - Erweiterte Unicode-Tastaturunterstützung) auf Windows Servern. Wenn der Wert 0 ist, dann wird EUKS nicht verwendet. Wenn der Wert 1 ist, dann wird EUKS als Ausweichmöglichkeit verwendet. Wenn der Wert 2 ist, dann wird EUKS verwendet, wenn möglich.
<code>root/ConnectionType/xen/general/useLocalIM</code>	Wenn diese Einstellung aktiviert ist, wird die lokale X Eingabemethode verwendet, um die Tastatureingabe zu interpretieren. Dies wird nur für europäische Sprachen unterstützt. Diese Einstellung ist der Citrix INI-Dateieinstellung <code>useLocalIME</code> direkt zugeordnet.
<code>root/ConnectionType/xen/general/userAgent</code>	Die Zeichenfolge dieses Schlüssels wird vom Citrix-Client präsentiert und ist nützlich für Administratoren, um zu wissen, woher die Verbindungsanforderung stammt.
<code>root/ConnectionType/xen/general/waitForNetwork</code>	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
<code>root/ConnectionType/xen/general/webcamFramesPerSec</code>	Steuert die <code>HDXWebCamFramesPerSec</code> Variable in der <code>All_Regions.ini</code> -Datei.
<code>root/ConnectionType/xen/general/webcamSupport</code>	Wenn der Wert 0 ist, dann sind die Webcam und die Webcam-Soundwiedergabe deaktiviert. Wenn er auf 1 gesetzt ist, dann sind die Webcam und das Webcam Audio mit der Komprimierung aktiviert. Wenn der Wert 2 ist, dann ist die USB-Umleitung der Webcam und das Webcam Audio aktiviert.
<code>root/ConnectionType/xen/general/windowHeight</code>	Legt die Höhe des Fensters in Pixel fest, wenn <code>windowSize</code> auf <code>Fixed Size</code> eingestellt ist.
<code>root/ConnectionType/xen/general/windowPercent</code>	Legt die Größe des Fensters als Prozentsatz fest, wenn <code>windowSize</code> auf <code>Percentage of Screen Size</code> eingestellt ist.
<code>root/ConnectionType/xen/general/windowSize</code>	Wenn als <code>Default</code> festgelegt, dann werden die serverseitige Einstellungen verwendet. Wenn <code>Full Screen</code> eingestellt ist, wird die Verbindung auf allen verfügbaren Bildschirmen ohne Ränder maximiert. Bei der Einstellung auf <code>Fixed Size</code> können die Schlüssel <code>windowWidth</code> und <code>windowSizeHeight</code> verwendet werden, um die Größe des Fensters in Pixel anzugeben. Wenn <code>Percentage of Screen Size</code> eingestellt ist, kann der Schlüssel <code>WindowPercent</code> verwendet werden, um die Größe des Fensters als Prozentsatz des gesamten Bildschirmbereichs anzugeben. Damit die Einstellung <code>Percentage of Screen Size</code> wirksam ist, muss <code>EnableForceDirectConnect</code> auf 1 eingestellt werden und <code>TWIMode</code> muss auf 0 eingestellt werden. Diese Einstellung funktioniert nur mit XenApp und nur, wenn der Server direkte Verbindungen erlaubt. Diese Einstellung funktioniert nicht mit XenDesktop.
<code>root/ConnectionType/xen/general/windowWidth</code>	Legt die Breite des Fensters in Pixel fest, wenn <code>windowSize</code> auf <code>Fixed Size</code> eingestellt ist.
<code>root/ConnectionType/xen/gui/XenDesktopPanel/ disabled</code>	Wenn der Wert 1 ist, dann sind das Xen-Desktop-Fenster und seine Taskleiste deaktiviert. Wird in der Regel verwendet, wenn <code>autoStartResource</code> oder <code>autoStartDesktop</code> aktiviert ist.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/gui/XenManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/gui/XenManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/gui/XenManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/gui/XenManager/widgets/address</code>	Zum Einstellen des Status für das Widget <b>Dienst-URL</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/appInMenu</code>	Zum Einstellen des Status für das Widget <b>Anwendung auf der Taskleiste anzeigen</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop</code>	Zum Einstellen des Status für das Widget <b>Anwendung auf dem Desktop anzeigen</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect</code>	Zum Einstellen des Status für das Widget <b>Automatische Verbindungswiederherstellung</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop</code>	Zum Einstellen des Status für das Widget <b>Desktop automatisch starten</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource</code>	Zum Einstellen des Status für das Widget <b>Ressource automatisch starten</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/autostart</code>	Zum Einstellen des Status für das Widget <b>Autostart Priorität</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer

Registrierungsschlüssel	Beschreibung
	kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/domain</code>	Zum Einstellen des Status für das Widget <b>Domäne</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection</code>	Zum Einstellen des Status für das Widget <b>Alternative Verbindung</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/folder</code>	
<code>root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon</code>	Zum Einstellen des Status für das Widget <b>Symbol auf Desktop anzeigen</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/isInMenu</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/ConnectionType/xen/gui/XenManager/widgets/label</code>	Zum Einstellen des Status für das Widget <b>Name</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/password</code>	Zum Einstellen des Status für das Widget <b>Kennwort</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/username</code>	Zum Einstellen des Status für das Widget <b>Benutzername</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork</code>	Zum Einstellen des Status für das Widget <b>Vor der Anmeldung auf Netzwerkverbindung warten</b> in Citrix Connection Manager. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

Registrierungsschlüssel	Beschreibung
<code>root/ConnectionType/xen/gui/fbpanel/autohide</code>	Wenn der Wert <code>true</code> ist, dann wird automatisch die Taskleiste ausgeblendet.
<code>root/ConnectionType/xen/gui/fbpanel/edge</code>	Legt die Standard-Position der Taskleiste fest, wenn mehr als ein veröffentlichter Desktop oder mehr als eine veröffentlichte Anwendung verfügbar ist.
<code>root/ConnectionType/xen/gui/fbpanel/hidden</code>	Bei Auswahl 1, ist die Taskleiste vollständig ausgeblendet, aber nur, wenn <code>autoStartResource</code> oder <code>autoStartDesktop</code> aktiviert ist.

## CpuMgr

Registrierungsschlüssel	Beschreibung
<code>root/CpuMgr/General/CpuNumber</code>	Zeigt die Anzahl der CPUs im System an. Dieser Wert ist schreibgeschützt.
<code>root/CpuMgr/General/EnableCpuMgr</code>	Wenn der Wert 1 ist, steuert der CPU-Manager die Systemleistung. Wenn der Wert 0 ist, wird das System mit seiner Standard-Leistungstufe ausgeführt.
<code>root/CpuMgr/General/ScalingAvailableGovernors</code>	Zeigt die verfügbaren CPU-Skalierungsregler im System an. Dieser Wert ist schreibgeschützt.
<code>root/CpuMgr/General/ScalingGovernor</code>	Legt den zu verwendenden CPU-Skalierungsregler fest, wenn der CPU-Manager aktiviert ist. Die verfügbaren Regler sind von der Hardware abhängig. Einige häufig verwendete Regler sind <code>performance</code> und <code>ondemand</code> . Der <code>performance</code> -Regler benötigt am meisten Energie und konfiguriert das System so, dass es mit maximaler Leistung ausgeführt wird, selbst wenn es nicht genutzt wird. Der <code>ondemand</code> -Regler konfiguriert Systemressourcen basierend auf dem aktuellen Bedarf und kann die beste Leistung pro Watt ergeben, aber die Benutzerleistung leidet möglicherweise, wenn das System ständig die Leistung erhöht oder verringert. Der Standard-Regler ist <code>performance</code> . Die Änderung eines Reglers wird sofort wirksam.

## DHCP

Dieser Ordner ist vorhanden, um temporäre Registrierungsschlüssel zu unterstützen, die hinzugefügt werden, wenn das System eine DHCP-Lease erwirbt. Es ist keine Änderung erforderlich.

## Dashboard



**HINWEIS:** Das Dashboard entspricht der Taskleiste.

Registrierungsschlüssel	Beschreibung
<code>root/Dashboard/GUI/Clock</code>	Wenn der Wert 1 ist, wird die Uhr in der Taskleiste angezeigt.
<code>root/Dashboard/GUI/ConnectionManager</code>	Wenn der Wert 1 ist, wird der HP Connection Manager in der Taskleiste angezeigt.

Registrierungsschlüssel	Beschreibung
root/Dashboard/GUI/ControlPanel	Wenn der Wert 1 ist, wird die Systemsteuerung in der Taskleiste angezeigt.
root/Dashboard/GUI/PowerButton	Wenn der Wert 1 ist, wird die Schaltfläche „Ein/Aus“ in der Taskleiste angezeigt.
root/Dashboard/GUI/Search	Wenn der Wert 1 ist, wird die Schaltfläche „Suchen“ auf der Taskleiste angezeigt.
root/Dashboard/GUI/SystemInformation	Wenn der Wert 1 ist, wird die Schaltfläche „Systeminformation“ in der Taskleiste angezeigt.
root/Dashboard/GUI/SystemTray	Wenn der Wert 1 ist, wird der Infobereich in der Taskleiste angezeigt.
root/Dashboard/GUI/TaskBar	Wenn der Wert 1 ist, dann wird der Anwendungsbereich auf der Taskleiste angezeigt.
root/Dashboard/General/AlwaysOnTop	Wenn der Wert 1 ist, wird die Taskleiste immer im Vordergrund benutzt.
root/Dashboard/General/AutoHide	Wenn der Wert 1 ist, wird die Taskleiste automatisch ausgeblendet.
root/Dashboard/General/EnterLeaveTimeout	Legt die Dauer in Millisekunden fest, bevor die Taskleiste ausgeblendet bzw. einblendet wird, wenn <code>AutoHide</code> aktiviert ist.
root/Dashboard/General/IconSize	Regelt die Größe der Symbole in der Taskleiste.
root/Dashboard/General/Length	Legt die Länge der Taskleiste fest.
root/Dashboard/General/LengthToScreenSide	Wenn der Wert 1 ist, ist die Länge der Taskleiste fest und entspricht der Länge der Bildschirmseite, an der sie angeheftet ist.
root/Dashboard/General/PanelDockSide	Legt die Seite des Bildschirms fest, an der die Taskleiste angedockt ist.
root/Dashboard/General/RemainPixel	Legt die Anzahl an Pixeln fest, die sichtbar sind, wenn die Taskleiste ausgeblendet ist.
root/Dashboard/General/SlidingTimeout	Legt die Dauer in Millisekunden fest, die benötigt werden, um die Taskleiste ein- oder auszublenden, wenn <code>AutoHide</code> aktiviert ist.
root/Dashboard/General/Width	Legt die Breite der Taskleiste fest.

## Display

Registrierungsschlüssel	Beschreibung
root/Display/Configuration/displaymode	Legt den Anzeigemodus fest. Wenn der Wert 0 ist, dann wird der Standard-Modus (einer 1 – 4-Monitor-Konfiguration) verwendet. Wenn der Wert 1 ist, dann kann eine 6-Monitor-Konfiguration verwendet werden, aber nur auf unterstützten Plattformen mit der entsprechenden Add-on-Karte.
root/Display/Configuration/hexlayout	Gibt das Layout in Sechs-Monitor-Modus an.
root/Display/Configuration/hexprofile	Gibt das im Sechs-Monitor-Modus verwendete Profil an.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
<code>root/Display/Configuration/primaryprofile</code>	Legt das Profil fest, das für den primären Monitor über den Profilenames verwendet wird. Für Smart Zero muss dies immer auf Standard eingestellt werden.
<code>root/Display/Configuration/quaternarymode</code>	Legt die Position des vierten Monitors im Verhältnis des in <code>Quaternaryrelative</code> angegebenen Monitors fest. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.
<code>root/Display/Configuration/quaternaryprofile</code>	Legt das Profil fest, das für den vierten Monitor über den Profilenames verwendet wird.
<code>root/Display/Configuration/quaternaryrelative</code>	Zeigt an, welcher Monitor referenziert wird, um die Position des vierten Monitors einzustellen.
<code>root/Display/Configuration/secondaryConnector</code>	Gibt den sekundären Anschluss an.
<code>root/Display/Configuration/secondarymode</code>	Gibt die Position des sekundären Monitors in Bezug auf den primären Monitor an. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.
<code>root/Display/Configuration/secondaryorientation</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/Display/Configuration/secondaryprofile</code>	Legt das Profil fest, das für den sekundären Monitor über den Profilenames verwendet wird.
<code>root/Display/Configuration/swapstate</code>	Gibt an, welcher Anschluss den Hauptmonitor verbindet. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. In der Regel bedeutet 0, dass der primäre Monitor am VGA-Anschluss ist, und 1 bedeutet, dass er am „anderen“ Anschluss ist. Für den t510 bedeutet 0, dass der primäre Monitor am DVI-I-Anschluss ist, und 1 bedeutet, dass der primäre Monitor am DVI-D-Anschluss ist. Für Plattformen mit einer Video-Add-on-Karte bedeutet 0, dass der primäre Monitor sich auf der integrierten Grafikkarte befindet und 1 bedeutet, dass der primäre Monitor auf der Add-on-Videokarte ist.
<code>root/Display/Configuration/tertiarymode</code>	Legt die Position des dritten Monitors im Verhältnis des in <code>tertiaryrelative</code> angegebenen Monitors fest. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.
<code>root/Display/Configuration/tertiaryprofile</code>	Legt das Profil fest, das für den dritten Monitor über den Profilenames verwendet wird.
<code>root/Display/Configuration/tertiaryrelative</code>	Zeigt an, welcher Monitor referenziert wird, um die Position des dritten Monitors einzustellen.
<code>root/Display/Profiles/&lt;UUID&gt;/colorScaling</code>	Legt die Farbtemperatur oder direkte RGB-Skalierung für ThinClients mit integrierten Monitoren fest. Der Eintrag ist ein sechsstelliger Hex-Wert RRGGBB, wobei <code>ffffff</code> eine vollständige (100 %) Skalierung auf allen drei Farbkanälen bedeuten würde.
<code>root/Display/Profiles/&lt;UUID&gt;/depth</code>	Legt die Display-Farbtiefe in Bits pro Pixel fest. Eine höhere Farbtiefe bedeutet bessere Qualität, aber geringere Leistung.

Registrierungsschlüssel	Beschreibung
root/Display/Profiles/<UUID>/height	Legt die gewünschte Monitor-Auflösungshöhe fest. Wenn der Wert 0 ist, dann wird die Auflösung automatisch erkannt.
root/Display/Profiles/<UUID>/label	Legt den Profilnamen in der Anzeige fest. Für Smart Zero muss dies immer auf <code>Standard</code> eingestellt werden.
root/Display/Profiles/<UUID>/orientation	Legt die Monitorausrichtung wie folgt fest: 0 = Normal; 1 = Nach links drehen; 2 = Nach rechts drehen; 3 = Invertieren.
root/Display/Profiles/<UUID>/refresh	Gibt die gewünschte Bildwiederholungsrate für den Monitor an. Nicht alle Bildwiederholungsrate werden für alle Auflösungen unterstützt. Wenn der Wert 0 ist, dann wird die Aktualisierungsrate automatisch erkannt. Die unterstützten Werte sind abhängig vom Monitor. Das Einrichten einer Aktualisierungsrate, die von dem angeschlossenen Monitor nicht unterstützt wird, wird zu einem schwarzen Bildschirm führen. HP empfiehlt, diese Einstellung auf 0 zu lassen.
root/Display/Profiles/<UUID>/width	Legt die gewünschte Monitor-Auflösungsbreite fest. Wenn der Wert 0 ist, dann wird die Auflösung automatisch erkannt.
root/Display/userLock	Wenn der Wert 1 ist und die Anzeigeeinstellungen vom Benutzer geändert wurden, werden die Anzeigeeinstellungen beim Import eines Clientprofils beibehalten.
root/Display/userLockEngaged	Dieser Registrierungsschlüssel wird automatisch auf 1 gesetzt, nachdem die Anzeigeeinstellungen vom Benutzer geändert wurden. Sie müssen diese Einstellung in der Regel nicht ändern.

## Network

Registrierungsschlüssel	Beschreibung
root/Network/ActiveDirectory/Domain	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/DynamicDNS	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Enabled	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Method	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Password	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Username	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/DNSServers	Hier kann ein zusätzlicher DNS-Server für die Auflösung des Domännennamens angegeben werden. Die angegebenen Server werden zusätzlich zu jeglichen über DHCP abgerufenen Servern

Registrierungsschlüssel	Beschreibung
	verwendet. Es können bis zu drei IPv4- oder IPv6-Adressen, durch Kommas getrennt, angegeben werden.
root/Network/DefaultHostnamePattern	Legt das Standard-Hostnamensmuster fest, das zu verwenden ist, wenn neue Hostnamen generiert werden. Dies wird verwendet, wenn sowohl der Registrierungsschlüssel <code>Hostname</code> als auch <code>/etc/hostname</code> leer ist. Verwenden Sie im Muster des Hostnamen <code>%</code> als Trennzeichen. Im Beispiel <code>HPTC%MAC:1-6%</code> wäre <code>HPTC</code> das Präfix und die ersten sechs Zeichen der MAC-Adresse des Thin Client würden folgen. Wenn die MAC-Adresse des Thin Client also <code>11:22:33:44:55:66</code> ist, dann wäre der generierte Hostname <code>HPTC112233</code> . Ist das Muster <code>TC%MAC%</code> , wäre der generierte Hostname <code>TC112233445566</code> . Wenn das Muster <code>HP%MAC:7%</code> ist, dann wäre der generierte Hostname <code>HP1122334</code> .
root/Network/EncryptWpaConfig	Wenn der Wert 1 ist, wird das Kennwort verschlüsselt.
root/Network/FtpProxy	Legt die FTP-Proxy-Adresse fest. HP empfiehlt, dass das folgende Format für diesen Wert verwendet wird, da das <code>http</code> -Präfix besser unterstützt ist: <code>http://ProxyServer:Port</code>
root/Network/Hostname	Legt den Hostnamen des Thin Client fest.
root/Network/HttpProxy	Legt die HTTP-Proxy-Adresse fest. HP empfiehlt die Verwendung des folgenden Format: <code>http://ProxyServer:Port</code>
root/Network/HttpsProxy	Legt die HTTPS-Proxy-Adresse fest. HP empfiehlt, dass das folgende Format für diesen Wert verwendet wird, da das <code>http</code> -Präfix besser unterstützt ist: <code>http://ProxyServer:Port</code>
root/Network/IPSec/IPSecRules/<UUID>/DstAddr	Legt die Zieladresse für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethod	Legt die Authentifizierungsmethode für die IPSec Regel fest. <code>PSK</code> wird für einen Pre-shared-Schlüssel verwendet und <code>Certificate</code> für die Verwendung der Zertifikat-Dateien.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodCACert	Wenn die Authentifizierungsmethode <code>Certificate</code> ist, wird der Dateipfad des CA-Zertifikats in diesem Registrierungsschlüssel gespeichert.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodClientCert	Wenn die Authentifizierungsmethode <code>Certificate</code> ist, wird der Dateipfad des Client-Zertifikats in diesem Registrierungsschlüssel gespeichert.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPresharedKey	Wenn die Authentifizierungsmethode <code>PSK</code> ist, wird der Pre-shared-Key-Wert in diesem Registrierungsschlüssel gespeichert.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPrivateKey	Wenn die Authentifizierungsmethode <code>Certificate</code> ist, wird der private Schlüsseldatei-Pfad, der dem Client-Zertifikat entspricht, in diesem Registrierungsschlüssel gespeichert.
root/Network/IPSec/IPSecRules/<UUID>/MMDHGroup	Legt die Phase 1 der Diffie-Hellman-Gruppe fest.
root/Network/IPSec/IPSecRules/<UUID>/MMEncryptionAlg	Legt die Phase 1 des Verschlüsselungsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/MMIntegrityAlg	Legt die Phase 1 des Integritätsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/MMLifetimeMinutes	Legt die Phase 1 der Lebensdauer fest.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
root/Network/IPSec/IPSecRules/<UUID>/QMAHEnable	Ermöglicht Phase 2 AH.
root/Network/IPSec/IPSecRules/<UUID>/QMAHIntegrityAlg	Legt die Phase 2 AH des Integritätsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEnable	Ermöglicht Phase 2 ESP.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEncryptionAlg	Legt die Phase 2 ESP des Verschlüsselungsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/QMESPIntegrityAlg	Legt die Phase 2 ESP des Integritätsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/QMLifetimeSeconds	Legt die Phase 2 der Lebensdauer fest.
root/Network/IPSec/IPSecRules/<UUID>/RuleDescription	Legt die Beschreibung für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/RuleEnable	Bei Einstellung des Werts auf 1 ist die Regel aktiviert.
root/Network/IPSec/IPSecRules/<UUID>/RuleName	Legt den Namen für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/SrcAddr	Legt die Quell-Adresse für die IPSec-Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/TunnelDstAddr	Legt die Tunnel-Zieladresse für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/TunnelEnable	Ermöglicht Tunnelmodus für die IPSec Regel.
root/Network/IPSec/IPSecRules/<UUID>/TunnelSrcAddr	Legt die Tunnel-Quell-Adresse für die IPSec-Regel fest.
root/Network/KeepPreviousDNS	Wenn der Wert 1 ist, werden bereits konfigurierte DNS-Server und Suchdomänen, die nicht vom Netzwerkmanager generiert wurden, in resolv.conf aufbewahrt. Wenn der Wert 0 ist, dann wird resolv.conf komplett überschrieben.
root/Network/SearchDomains	Zusätzliche Suchdomänen für die FQDN-Auflösung können hier angegeben werden. Die angegebenen Domänen werden an alle unvollständigen Definitionen angehängt werden, als Versuch, einen FQDN zu erzeugen, der über DNS aufgelöst werden kann. Zum Beispiel wird eine Suchdomäne <code>mydomain.com</code> die Serverdefinition <code>Myserver</code> ordnungsgemäß zu <code>myserver.mydomain.com</code> lösen, auch wenn der DNS-Server <code>Myserver</code> nicht in seinem Namenslösungsverzeichnis hat. Bis zu fünf zusätzliche Suchdomänen können angegeben werden.
root/Network/VPN/AutoStart	Wenn der Wert 1 ist, startet VPN automatisch beim Systemstart.
root/Network/VPN/PPTP/Domain	Legt die PPTP-Domäne fest.
root/Network/VPN/PPTP/Gateway	Legt das PPTP-Gateway fest.
root/Network/VPN/PPTP/Password	Legt das PPTP-Benutzerkennwort fest.
root/Network/VPN/PPTP/Username	Legt den PPTP-Benutzernamen fest.
root/Network/VPN/Type	Legt den VPN-Typ fest.
root/Network/VPN/VPNC/Domain	Legt die VPNC-Domäne fest.

Registrierungsschlüssel	Beschreibung
root/Network/VPN/VPNC/Gateway	Legt das VPNC-Gateway fest.
root/Network/VPN/VPNC/Group	Legt die VPNC-Gruppe fest.
root/Network/VPN/VPNC/GroupPassword	Legt das VPNC-Gruppenkennwort fest.
root/Network/VPN/VPNC/IKEDHGroup	Legt die VPNC IKE Diffie-Hellman-Gruppe fest.
root/Network/VPN/VPNC/LocalUDPPort	Legt den lokalen UDP-Port für VPNC fest. Wenn der Wert 0 ist, wird ein zufälliger Port verwendet. Diese Einstellung gilt nur, wenn der NAT-Traversal-Modus (NATMode) auf <code>cisco-udp</code> festgelegt ist.
root/Network/VPN/VPNC/NATMode	Legt den NAT-Traversal-Modus für VPNC fest.
root/Network/VPN/VPNC>Password	Legt das VPNC-Benutzerkennwort fest.
root/Network/VPN/VPNC/PerfectForwardSecrecy	Legt für die VPNC Diffie-Hellman-Gruppe fest, dass Perfect Forward Secrecy (PFS) verwendet werden soll.
root/Network/VPN/VPNC/Security	Legt die VPNC-Sicherheitsstufe fest.
root/Network/VPN/VPNC/Username	Legt den VPNC-Benutzernamen fest.
root/Network/Wired/DefaultGateway	Legt das Standard-Gateway fest, das vom Gerät für die Kommunikation mit dem Internet verwendet wird. In der Regel ist dies die IP-Adresse des Routers. Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
root/Network/Wired/EnableDefGatewayAsDNS	Wenn der Wert 1 ist, dann wird der Standard-Gateway auch als Namensservers benutzt.
root/Network/Wired/EthernetSpeed	Legt die Verbindungsgeschwindigkeit der primären Ethernet-Netzwerkschnittstelle fest. <code>Automatic</code> ermöglicht, dass die schnellste verfügbare Verbindungsgeschwindigkeit verwendet wird, die in der Regel 1 Gbit/s oder 100 Mbit/s/Full je nach Switch ist. Die Verbindungsgeschwindigkeit kann auch erzwungen werden, um eine einzige Geschwindigkeit (100 Mbit/s oder 10 Mbit/s) und einen Duplexmodus (Voll oder Halb) zu verwenden, sodass Switches oder Hubs unterstützt werden, die keine angemessene Autonegotiation durchführen.
root/Network/Wired/IPAddress	Legt die IPv4-Adresse des Thin Client fest. Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
root/Network/Wired/IPv6Enable	Wenn der Wert 1 ist, dann ist IPv6 aktiviert.
root/Network/Wired/Interface	Legt die Standard-Ethernet-Schnittstelle oder NIC fest.
root/Network/Wired/MTU	Legt die MTU fest. Es spielt dabei keine Rolle, wenn die IP-Adresse statisch oder DHCP-erworben wird.
root/Network/Wired/Method	Wenn <code>Automatic</code> eingestellt ist, verwendet der Thin Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn <code>Static</code> eingestellt ist, werden die Werte der Registrierungsschlüssel <code>IP-Adresse</code> , <code>SubnetMask</code> und <code>DefaultGateway</code> verwendet. HP rät, in einem generischen Clientprofil <code>Static</code> nicht zu verwenden, da es dazu führt, dass alle Thin Clients die gleiche IP-Adresse erhalten.
root/Network/Wired/Security/CACert	Legt den Pfad zu der CA-Zertifikatsdatei fest.
root/Network/Wired/Security/EnableMachineAuth	Wenn der Wert 1 ist, wird die Computerauthentifizierung für PEAP aktiviert.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
root/Network/Wired/Security/Identity	Legt die Identität oder anonyme Identität fest.
root/Network/Wired/Security/InnerAuth	Legt das PEAP innere Authentifizierung-Protokoll fest.
root/Network/Wired/Security/InnerAuthTTLS	Legt das TTLS innere Authentifizierung-Protokoll fest.
root/Network/Wired/Security/MachineAuthName	Speichert den Namen des Computerkontos, wenn die Computerauthentifizierung aktiviert ist.
root/Network/Wired/Security/MachineAuthPassword	Speichert das Kennwort des Computerkontos, wenn die Computerauthentifizierung aktiviert ist.
root/Network/Wired/Security/PEAPVersion	Legt die PEAP-Version fest.
root/Network/Wired/Security/Password	Legt das Kennwort fest.
root/Network/Wired/Security/PrivateKey	Legt den Pfad zu einer privaten Schlüsseldatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wired/Security/Type	Legt den 802.1x-Authentifizierungstyp fest.
root/Network/Wired/Security/UserCert	Legt den Pfad zu einer Benutzer-Zertifikatsdatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wired/Security/Username	Legt den Benutzernamen fest.
root/Network/Wired/SubnetMask	Legt die Subnetzmaske des Geräts fest, z. B. 255.255.255.0 (für ein Standard-Klasse C Subnetz). Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
root/Network/Wireless/DefaultGateway	Legt das Standard-Gateway fest, das vom Gerät für die Kommunikation mit dem Internet verwendet wird. In der Regel ist dies die IP-Adresse des Routers. Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
root/Network/Wireless/EnableDefGatewayAsDNS	Wenn der Wert 1 ist, dann wird der Standard-Gateway auch als Namensservers benutzt.
root/Network/Wireless/IPAddress	Legt die IPv4-Adresse des Thin Client fest. Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
root/Network/Wireless/IPv6Enable	Wenn der Wert 1 ist, dann ist IPv6 aktiviert.
root/Network/Wireless/Interface	Legt die drahtlose Standardschnittstelle oder den kabellosen Netzwerkadapter fest.
root/Network/Wireless/Method	Wenn <code>Automatic</code> eingestellt ist, verwendet der Thin Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn <code>Static</code> eingestellt ist, werden die Werte der Registrierungsschlüssel <code>IP-Adresse</code> , <code>SubnetMask</code> und <code>DefaultGateway</code> verwendet. HP rät, in einem generischen Clientprofil <code>Static</code> nicht zu verwenden, da es dazu führt, dass alle Thin Clients die gleiche IP-Adresse erhalten.
root/Network/Wireless/PowerEnable	Wenn der Wert 1 ist, dann ist das Energiemanagement der drahtlosen Netzwerk-Karte aktiviert.
root/Network/Wireless/SSID	Legt den drahtlosen Zugangspunkt fest, der über SSID verwendet wird.
root/Network/Wireless/SSIDHidden	Gibt an, ob die SSID des drahtlosen Zugangspunkts ausgeblendet ist.
root/Network/Wireless/SSIDWhiteList	Gibt eine Positivliste für WLAN-Access Points an. Wenn der Wert dieses Registrierungsschlüssels nicht leer ist, werden nur die im

Registrierungsschlüssel	Beschreibung
	Wert angegebenen SSIDs in den Prüfergebnissen für WLAN-Access Points angezeigt. Verwenden Sie ein Semikolon, um die SSIDs zu trennen.
<code>root/Network/Wireless/Security/CACert</code>	Legt den Pfad zu der CA-Zertifikatsdatei fest.
<code>root/Network/Wireless/Security/EAPFASTPAC</code>	Legt den Pfad der PAC-Datei für die EAP-FAST-Authentifizierung fest.
<code>root/Network/Wireless/Security/EAPFASTProvision</code>	Legt die bereitgestellte Option für die EAP-FAST-Authentifizierung fest.
<code>root/Network/Wireless/Security/Identity</code>	Legt die Identität oder anonyme Identität fest.
<code>root/Network/Wireless/Security/InnerAuth</code>	Legt das PEAP innere Authentifizierung-Protokoll fest.
<code>root/Network/Wireless/Security/InnerAuthTTLs</code>	Legt das TTLS innere Authentifizierung-Protokoll fest.
<code>root/Network/Wireless/Security/PEAPVersion</code>	Legt die PEAP-Version fest.
<code>root/Network/Wireless/Security/Password</code>	Legt das Kennwort fest.
<code>root/Network/Wireless/Security/PrivateKey</code>	Legt den Pfad zu einer privaten Schlüsseldatei fest. Dies dient nur der TLS-Authentifizierung.
<code>root/Network/Wireless/Security/Type</code>	Legt den drahtlosen Authentifizierungstyp fest.
<code>root/Network/Wireless/Security/UserCert</code>	Legt den Pfad zu einer Benutzer-Zertifikatsdatei fest. Dies dient nur der TLS-Authentifizierung.
<code>root/Network/Wireless/Security/Username</code>	Legt den Benutzernamen fest.
<code>root/Network/Wireless/Security/WEPAuth</code>	Legt den WEP-Authentifizierungstyp fest.
<code>root/Network/Wireless/Security/WEPIndex</code>	Legt den WEP-Kennwortindex fest.
<code>root/Network/Wireless/SubnetMask</code>	Legt die Subnetzmaske des Geräts fest, z. B. 255.255.255.0 (für ein Standard-Klasse C Subnetz). Diese Einstellung wird nur wirksam, wenn <code>Method</code> auf <code>Static</code> eingestellt ist.
<code>root/Network/Wireless/WpaDriver</code>	Gibt den Treiber an, der von <code>wpa_supplicant</code> verwendet wird (standardmäßig <code>wext</code> ). <code>n180211</code> ist der einzige Treiber, der aktuell unterstützt wird.
<code>root/Network/Wireless/bcmwlCountryOverride</code>	Überschreibt den Wert für das Land aus dem BIOS, wenn der erforderliche Wert im BIOS nicht vorhanden ist. Der <code>bcmwl</code> -Treiber akzeptiert die <code>wl_country</code> -Option, die bei Bedarf aus BIOS-Werten abgerufen wird (gegenwärtig wird nur Indonesien unterstützt). Ein Systemneustart ist erforderlich, damit die Änderungen wirksam werden.
<code>root/Network/disableLeftClickMenu</code>	Wenn der Wert 1 ist, dann ist das Linksklick-Menü für das Netzwerk-Taskleistensymbol deaktiviert.
<code>root/Network/disableRightClickMenu</code>	Wenn der Wert 1 ist, dann ist das Rechtsklick-Menü für das Netzwerk-Taskleistensymbol deaktiviert.
<code>root/Network/iPeak/ShowStatus</code>	Wenn der Wert 1 ist, dann wird der HP Velocity-Status als Teil des Symbols in der Taskleiste angezeigt. HP Velocity wird auf HP t420 nicht unterstützt.
<code>root/Network/iPeak/Status</code>	Wenn der Wert 1 ist, wird HP Velocity aktiviert. Wenn der Wert 2 ist, dann ist HP Velocity im Monitor-Modus aktiviert. Durch die Einstellung 0 wird HP Velocity deaktiviert. HP Velocity wird auf HP t420 nicht unterstützt.

Registrierungsschlüssel	Beschreibung
root/Network/userLock	Wenn der Wert 1 ist und die Netzwerkeinstellungen vom Benutzer geändert wurden, werden die Netzwerkeinstellungen beim Import eines Clientprofils beibehalten.
root/Network/userLockEngaged	Dieser Registrierungsschlüssel wird automatisch auf 1 gesetzt, nachdem die Netzwerkeinstellungen vom Benutzer geändert wurden. Sie müssen diese Einstellung in der Regel nicht ändern.

## SCIM

Registrierungsschlüssel	Beschreibung
root/SCIM/ScimEnabled	Wenn der Wert 1 ist, dann ist SCIM für Eingaben in Chinesisch, Japanisch und Koreanisch aktiviert.

## ScepMgr

Registrierungsschlüssel	Beschreibung
root/ScepMgr/General/AutoRenew/Enabled	Wenn der Wert 1 ist, werden Zertifikate automatisch erneuert, bevor sie ablaufen.
root/ScepMgr/General/AutoRenew/TimeFrame	Legt die Anzahl der Tage vor dem Ablaufdatum eines Zertifikats fest, die der SCEP-Manager versucht, das Zertifikat automatisch zu erneuern.
root/ScepMgr/IdentifyingInfo/CommonName	Legt den allgemeinen Namen fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. Ihr Name oder der vollständig qualifizierte Domänenname (Fully-Qualified Domain Name, FQDN) des Geräts. Der FQDN wird standardmäßig verwendet, wenn dieser Wert nicht angegeben wird.
root/ScepMgr/IdentifyingInfo/CountryName	Legt das Land bzw. die Region fest, das bzw. die für SCEP-Identifizierungsdaten verwendet werden soll.
root/ScepMgr/IdentifyingInfo/EmailAddress	Legt die E-Mail-Adresse fest, die für SCEP-Identifizierungsdaten verwendet werden soll.
root/ScepMgr/IdentifyingInfo/LocalityName	Legt den Ortsnamen fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. den Namen einer Stadt.
root/ScepMgr/IdentifyingInfo/OrganizationName	Legt den Organisationsnamen fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. einen Firmennamen oder einen Behördenamen.
root/ScepMgr/IdentifyingInfo/OrganizationUnitName	Legt den Namen einer Organisationseinheit fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. einen Abteilungsamen oder einen Gruppennamen.
root/ScepMgr/IdentifyingInfo/StateName	Legt den Staat bzw. das Bundesland fest, der bzw. das für SCEP-Identifizierungsdaten verwendet werden soll.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/CertFileChanged	Der Registrierungsschlüssel dient nur dazu, die anderen Anwendungen zu informieren, dass eine Zertifikatsdatei geändert wurde. Dieser Schlüssel sollte keine Änderung erfordern.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/KeySize	Legt die Schlüsselgröße fest, die für das generierte Schlüsselpaar verwendet werden soll.

Registrierungsschlüssel	Beschreibung
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerName	Legt den Namen des SCEP-Servers fest.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerUrl	Legt die URL des SCEP-Servers fest, die erforderlich ist, damit der SCEP-Client ein Zertifikat registrieren kann.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Code	Enthält den Statuscode der SCEP-Registrierung. Dieser Wert ist schreibgeschützt.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Detail	Enthält detaillierte Informationen über die SCEP-Registrierung. Dieser Wert ist schreibgeschützt.

## Search

Registrierungsschlüssel	Beschreibung
root/Search/Category/Applications/ConnectionManager/checked	
root/Search/Category/Applications/ConnectionManager/enabled	
root/Search/Category/Applications/Connections/checked	
root/Search/Category/Applications/Connections/enabled	
root/Search/Category/Applications/ControlPanel/checked	
root/Search/Category/Applications/ControlPanel/enabled	
root/Search/Category/Applications/Desktop/checked	
root/Search/Category/Applications/Desktop/enabled	
root/Search/Category/Applications/icon	
root/Search/Category/Applications/name	
root/Search/Category/FileSystem/caseSensitive	
root/Search/Category/FileSystem/enabled	
root/Search/Category/FileSystem/folderFilter	Gibt die Ordner im Dateisystem an, die der Benutzer durchsuchen darf. Verwenden Sie ein Semikolon, um Ordner zu trennen. Beispiel: /home/user;/usr/bin
root/Search/Category/FileSystem/location	
root/Search/Category/FileSystem/subFolder	
root/Search/Category/Miscellaneous/CheckForUpdate	
root/Search/Category/Miscellaneous/Logout	
root/Search/Category/Miscellaneous/Reboot	

Registrierungsschlüssel	Beschreibung
root/Search/Category/Miscellaneous/ShutDown	
root/Search/Category/Miscellaneous/Sleep	
root/Search/Category/Miscellaneous/SwitchToAdmin	
root/Search/Category/Regeditor/byDir	
root/Search/Category/Regeditor/byKey	
root/Search/Category/Regeditor/byValue	
root/Search/Category/Regeditor/byWhole	
root/Search/GUI/showCategory	

## Serial

Registrierungsschlüssel	Beschreibung
root/Serial/<UUID>/baud	Legt die Geschwindigkeit des seriellen Geräts fest.
root/Serial/<UUID>/dataBits	Legt fest, wie viele Bits in jedem Zeichen sind.
root/Serial/<UUID>/device	Legt das serielle Gerät fest, das am System angeschlossen ist.
root/Serial/<UUID>/flow	Legt die Flusssteuerung des seriellen Geräts fest, die das Starten und Anhalten der seriellen Kommunikation kommuniziert.
root/Serial/<UUID>/name	Legt den Windows Geräteanschluss fest, der für die Kommunikation mit dem seriellen Gerät verwendet wird.
root/Serial/<UUID>/parity	Legt die Paritätsbit des seriellen Geräts fest. Der Paritätsbit wird für die Fehlererkennung verwendet. Die Einstellung <code>none</code> bedeutet, es gibt keine Paritätserkennung.

## SystemInfo

Registrierungsschlüssel	Beschreibung
root/SystemInfo/Pages/General	Wenn der Wert 0 ist, wird die Registerkarte <b>Allgemein</b> im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/NetTools	Wenn der Wert 0 ist, wird die Registerkarte <b>Net-Tools</b> im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/Network	Wenn der Wert 0 ist, wird die Registerkarte <b>Netzwerk</b> im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/ServicePacks	Wenn der Wert 0 ist, wird die Registerkarte <b>Service Packs</b> im Abschnitt <b>Softwareinformationen</b> im Fenster „Softwareinformationen“ für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInformation	Wenn der Wert 0 ist, wird die Registerkarte <b>Softwareinformationen</b> im Fenster mit den Systeminformationen für Endbenutzer ausgeblendet.

Registrierungsschlüssel	Beschreibung
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInstalled	Wenn der Wert 0 ist, wird die Registerkarte <b>Installierte Software</b> im Abschnitt <b>Softwareinformationen</b> im Fenster „Softwareinformationen“ für Endbenutzer ausgeblendet.
root/SystemInfo/Pages/SystemLogs	Wenn der Wert 0 ist, wird die Registerkarte <b>Systemprotokolle</b> im Fenster „Systeminformationen“ für Endbenutzer ausgeblendet.
root/SystemInfo/authorized	Wenn der Wert 0 ist, ist die Schaltfläche „Systeminformationen“ auf der Taskleiste für Endbenutzer deaktiviert.

## TaskMgr

Registrierungsschlüssel	Beschreibung
root/TaskMgr/General/AlwaysOnTop	Wenn der Wert 1 ist, wird das Task-Manager-Fenster immer im Vordergrund angezeigt.

## USB

Registrierungsschlüssel	Beschreibung
root/USB/Classes/<ClassType>/ClassID	Legt die ID-Nummer der USB-Klasse fest.
root/USB/Classes/<ClassType>/DisplayName	Legt den Namen der USB-Klasse fest.
root/USB/Classes/<ClassType>/State	Legt fest, ob die Klasse zum Remote-Host zugeordnet ist.
root/USB/Classes/<ClassType>/Visible	Legt fest, ob die Klasse in der Benutzeroberfläche angezeigt wird, nicht in der Benutzeroberfläche angezeigt wird oder deaktiviert ist.
root/USB/Classes/ShowTab	Wenn der Wert 1 ist, wird der Abschnitt <b>Classes</b> (Klassen) im USB-Manager angezeigt.
root/USB/Devices/<UUID>/DisplayName	Legt den Namen fest, der im USB-Manager angezeigt wird. Wenn der Name nicht angegeben wird, versucht der USB-Manager, einen passenden Namen anhand der Geräteinformationen zu generieren.
root/USB/Devices/<UUID>/ProductID	Legt die Produkt-ID des Geräts fest.
root/USB/Devices/<UUID>/State	Legt fest, ob das Gerät dem Remote-Host wie folgt zugeordnet ist: 0 = Nicht umleiten; 1 = Standardeinstellungen verwenden; 2 = Umleitung.
root/USB/Devices/<UUID>/VendorID	Legt die Vendor-ID des Geräts fest.
root/USB/root/autoSwitchProtocol	Wenn der Wert 1 ist, wird das Remote-USB-Protokoll basierend auf dem ausgewählten Protokoll automatisch umgeschaltet.
root/USB/root/mass-storage/allowed	Wenn der Wert 1 ist, werden Massenspeichergeräte automatisch bereitgestellt, wenn das Protokoll <code>local</code> ist.
root/USB/root/mass-storage/read-only	Wenn der Wert 1 ist und wenn Massenspeichergeräte automatisch bereitgestellt werden, werden diese schreibgeschützt bereitgestellt.

Registrierungsschlüssel	Beschreibung
root/USB/root/opendebug	Wenn der Wert 1 ist, wird eine Debug-Nachricht auf <code>/tmp/USB-mgr-log</code> geschrieben.
root/USB/root/protocol	Legt das Protokoll fest, dem Remote-USB zugewiesen ist. Gültige Werte sind abhängig von den auf dem System installierten Protokollen, können jedoch <code>local</code> , <code>xen</code> , <code>freerdp</code> und <code>View</code> einschließen.

## auto-update

Registrierungsschlüssel	Beschreibung
root/auto-update/DNSAliasDir	Legt das Standard-Root-Verzeichnis für den DNS-Alias-Modus auf dem Server fest, der HP Smart Client-Dienste hostet.
root/auto-update/ManualUpdate	Wenn der Wert 1 ist, sind die DHCP-Kennung, die DNS-Alias und die Aktualisierungsmethoden der Übertragung für Automatic Update deaktiviert. Wenn eine manuelle Aktualisierung durchgeführt wird, müssen die Registrierungsschlüssel <code>password</code> , <code>path</code> , <code>protocol</code> , <code>user</code> und <code>ServerURL</code> eingestellt werden, um sicherzustellen, dass der Updateserver bekannt ist.
root/auto-update/ScheduledScan/Enabled	Wenn der Wert 1 ist, prüft der Thin Client in regelmäßigen Abständen den Automatic Update-Server, um nach Aktualisierungen zu suchen. Wenn der Wert 0 ist, wird vom Thin Client nur beim Systemstart auf Aktualisierungen geprüft.
root/auto-update/ScheduledScan/Interval	Legt die Zeit fest, die zwischen geplanten Updates gewartet wird. Dies sollte im Format <code>HH:MM</code> angegeben werden. Mehr als 24-Stunden-Intervalle können angegeben werden. Beispiel: um alle 48 Stunden auftretende Scans zu haben, stellen Sie hier <code>48:00</code> ein.
root/auto-update/ScheduledScan/Period	Thin Clients aktivieren die geplante Prüfung während des definierten Zeitraums nach dem Zufallsprinzip. Die Verwendung längerer Zeitabstände verhindert Fälle, in denen alle Thin Clients zur gleichen Zeit aktualisiert werden, was eine Netzwerküberlastung verursachen könnte. Die Dauer sollte im Format <code>HH:MM</code> angegeben werden. Beispiel: Um die Thin Client-Aktualisierungen über einen Zeitraum von 2,5 Stunden zu verteilen, stellen Sie hier <code>02:30</code> ein.
root/auto-update/ScheduledScan/StartTime	Legt die Startzeit von der ersten Periode des geplanten Update-Scans im Format <code>HH:MM</code> fest, unter Verwendung des 24-Stunden-Zeitformats. Beispiel: <code>4:35</code> nachmittags wäre <code>16:35</code> .
root/auto-update/ServerURL	Legt die IP-Adresse oder den Domännamen des Update-Servers fest, der verwendet wird, wenn <code>ManualUpdate</code> aktiviert ist.
root/auto-update/VisibleInSystray	Wenn der Wert 1 ist, dann ist die Automatic Update-Taskleistensymbol aktiviert.
root/auto-update/enableOnBootup	Wenn der Wert 1 ist, dann ist die automatische Aktualisierung beim Systemstart aktiviert.
root/auto-update/enableSystrayLeftClickMenu	Wenn der Wert 1 ist, dann ist das Linksklick-Menü für das Automatic Update-Taskleistensymbol aktiviert.

Registrierungsschlüssel	Beschreibung
<code>root/auto-update/enableSystrayRightClickMenu</code>	Wenn der Wert 1 ist, dann ist das Rechtsklick-Menü für das Automatic Update-Taskleistensymbol aktiviert.
<code>root/auto-update/gui/auto-update/ManualUpdate</code>	Zum Einstellen des Status für das Widget <b>Enable manual configuration</b> (Manuelle Konfiguration aktivieren) im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/ServerURL</code>	Zum Einstellen des Status für das Widget <b>Server</b> im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/enableOnBootup</code>	Zum Einstellen des Status für das Widget <b>Enable Automatic Update on system startup</b> (Automatic Update beim Systemstart aktivieren) im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/password</code>	Zum Einstellen des Status für das Widget <b>Password</b> (Kennwort) im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/protocol</code>	Zum Einstellen des Status für das Widget <b>Protocol</b> (Protokoll) im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/gui/auto-update/tag</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/auto-update/gui/auto-update/user</code>	Zum Einstellen des Status für das Widget <b>User name</b> (Benutzername) im Automatic Update-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/auto-update/password</code>	Legt das Kennwort fest, das verwendet wird, wenn <code>ManualUpdate</code> aktiviert ist. Dies wird nur verwendet, wenn das <code>protocol</code> auf <code>ftp</code> eingestellt ist. Dieser Wert ist normalerweise verschlüsselt.
<code>root/auto-update/path</code>	Legt den relativen Pfad von der Standard-Server-URL fest, wenn <code>ManualUpdate</code> aktiviert ist. Dies ist normalerweise leer oder auf <code>auto-update</code> eingestellt.

Registrierungsschlüssel	Beschreibung
<code>root/auto-update/preserveConfig</code>	Wenn der Wert 1 ist, dann werden die aktuellen Einstellungen der Thin Client-Konfiguration bei einem Image-Update über Automatic Update beibehalten.
<code>root/auto-update/protocol</code>	Legt das Protokoll fest, das verwendet wird, wenn <code>ManualUpdate</code> aktiviert ist.
<code>root/auto-update/tag</code>	Der Registrierungsschlüssel ist veraltet. Er hat zuvor die für DHCP (137) verwendete Tag-Nummer festgelegt. Dies wird jetzt über den Tag-Namen <code>Auto-Update</code> erkannt.
<code>root/auto-update/user</code>	Legt den Benutzernamen fest, der verwendet wird, wenn <code>ManualUpdate</code> aktiviert ist. Dies wird nur verwendet, wenn 'Protocol' auf 'ftp' eingestellt ist.

## background

Registrierungsschlüssel	Beschreibung
<code>root/background/bginfo/alignment</code>	Legt die Textausrichtung für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/enabled</code>	Wenn der Wert 1 ist, werden Systeminformationen auf dem Desktophintergrund angezeigt (Hintergrundsysteminformationen).
<code>root/background/bginfo/horizontalLocation</code>	Legt die Position der Hintergrundsysteminformationen auf der X-Achse als Prozentsatz fest.
<code>root/background/bginfo/interval</code>	Legt das Intervall für die Textaktualisierung der Hintergrundsysteminformationen in Sekunden fest.
<code>root/background/bginfo/preset</code>	Legt für die Voreinstellungsdatei der Hintergrundsysteminformationen <code>use</code> fest. Wenn dieser Wert auf <code>none</code> festgelegt ist, können Sie die Einstellungen im Hintergrund-Manager anpassen.
<code>root/background/bginfo/shadowColor</code>	Legt die Schattenfarbe für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/shadowOffset</code>	Legt den Schattenoffset für die Hintergrundsysteminformationen fest. Wenn der Wert 0 ist, wird der Schatten deaktiviert.
<code>root/background/bginfo/text</code>	Legt den Text für die Hintergrundsysteminformationen fest. Weitere Informationen finden Sie im HP ThinPro-Whitepaper <i>Login Screen Customization</i> (nur auf Englisch verfügbar).
<code>root/background/bginfo/textColor</code>	Legt die Textfarbe für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/textSize</code>	Legt die Textgröße für die Hintergrundsysteminformationen fest.
<code>root/background/bginfo/verticalLocation</code>	Legt die Position der Hintergrundsysteminformationen auf der Y-Achse als Prozentsatz fest.
<code>root/background/desktop/color</code>	Durch die Einstellung von <code>theme</code> auf <code>none</code> für das Design, speichert dieser Schlüssel die Standardfarbe, die das benutzerdefinierte Design verwendet.
<code>root/background/desktop/imagePath</code>	Durch die Einstellung von <code>theme</code> auf <code>none</code> für das Design, speichert dieser Schlüssel den Image-Pfad des Desktop-Hintergrunds, die das benutzerdefinierte Design verwendet.

Registrierungsschlüssel	Beschreibung
root/background/desktop/lastBrowseDir	Durch die Einstellung von <code>theme</code> auf <code>none</code> für das Design, speichert dieser Schlüssel das zuletzt verwendete Verzeichnis.
root/background/desktop/style	Durch die Einstellung von <code>theme</code> auf <code>none</code> , speichert dieser Schlüssel, wie das Hintergrundbild auf dem Desktop erscheint (wie z.B. <code>center</code> , <code>tile</code> , <code>stretch</code> , <code>fit</code> und <code>fill</code> ).
root/background/desktop/theme	Legt die System-Design-Einstellung fest. Dieser Wert wird über den Hintergrund-Manager in der Systemsteuerung festgelegt. Die gültigen Werte hängen von den Designs ab, die auf dem System vorhanden sind. Dieser Schlüssel kann auf <code>none</code> eingestellt werden, damit die Benutzer das Design definieren können, auf <code>auto</code> , damit das System automatisch das Design des entsprechenden Protokolls für Smart Zero festlegt, oder auf <code>default</code> , damit das Standard-Design für ThinPro verwendet wird.

## config-wizard

Registrierungsschlüssel	Beschreibung
root/config-wizard/FirmwareUpdate/firmwareUpdateTimeout	Legt die Timeout-Dauer in Sekunden fest, wenn nach Updates gesucht wird. Bei Auswahl -1 gibt es keine Zeitüberschreitung.
root/config-wizard/FirmwareUpdate/firmwareUpdateURL	Legt die FTP-URL für Image-Aktualisierungen fest.
root/config-wizard/FirmwareUpdate/preserveConfig	Wenn der Wert 1 ist, werden die aktuellen Einstellungen der Thin Client-Konfiguration beibehalten, wenn ein Image-Update über den Erstkonfigurationsassistenten erfolgt.
root/config-wizard/enableConnectionCheck	Wenn der Wert 1 ist, dann ist die Prüfung der Verbindung beim Systemstart aktiviert.
root/config-wizard/enableNetworkCheck	Wenn der Wert 1 ist, dann ist der Netzwerktest beim Systemstart aktiviert.
root/config-wizard/updateCheck	Bei Einstellung des Werts auf 1 ist die Update-Prüfung beim Systemstart aktiviert.

## desktop

Registrierungsschlüssel	Beschreibung
root/desktop/shortcuts/<action>/command	Legt den Befehl fest, der durch die Verknüpfung ausgeführt wird.
root/desktop/shortcuts/<action>/enabled	Bei Einstellung des Werts auf 1 wird die Verknüpfung aktiviert.
root/desktop/shortcuts/<action>/shortcut	Gibt den Verknüpfungsnamen an.

## entries

Registrierungsschlüssel	Beschreibung
root/entries/<UUID>/command	
root/entries/<UUID>/folder	
root/entries/<UUID>/icon	
root/entries/<UUID>/label	
root/entries/<UUID>/metaInfo	
root/entries/<UUID>/onDesktop	
root/entries/<UUID>/onMenu	

## keyboard

Registrierungsschlüssel	Beschreibung
root/keyboard/DrawLocaleLetter	Wenn der Wert 1 ist, dann wird das Tastatur-Taskeleistensymbol die lokale Sprachzeichenfolge statt statischer Bilder verwenden.
root/keyboard/SystrayMenu/keyboardLayout	Wenn der Wert 1 ist, bietet das Kontextmenü für das Tastatur-Symbol der Systeminfo eine Option zum Öffnen des Tools für das Tastaturlayout in der Systemsteuerung.
root/keyboard/SystrayMenu/languages	Wenn der Wert 1 ist, bietet das Kontextmenü für das Tastatur-Symbol der Systeminfo eine Option zum Öffnen des Sprachentools in der Systemsteuerung.
root/keyboard/SystrayMenu/virtualKeyboard	Wenn der Wert 1 ist, bietet das Rechtsklick-Kontextmenü im Tastatur-Systeminfo-Symbol eine Option zum Öffnen der virtuellen Tastatur.
root/keyboard/VisibleInSystray	Wenn der Wert 1 ist, dann wird das Tastatur-Taskeleistensymbol angezeigt, und gibt das aktuelle Tastaturlayout an.
root/keyboard/XkbLayout	Dies ist ein interner Schlüssel, der verwendet wird, um ein XKB-Tastaturlayout zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbModel	Dies ist ein interner Schlüssel, der verwendet wird, um ein XKB-Tastaturmodell zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbOptions	Dies ist ein interner Schlüssel, der verwendet wird, um XKB-Tastaturoptionen zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbVariant	Dies ist ein interner Schlüssel, der verwendet wird, um eine XKB-Tastaturvariante zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/enable2	Wenn der Wert 1 ist, dann kann über die durch <code>switch</code> definierte Tastenkombination auf das sekundäre Tastaturlayout umgeschaltet werden.
root/keyboard/layout	Legt das primäre Tastaturlayout fest.
root/keyboard/layout2	Legt das sekundäre Tastaturlayout fest.

Registrierungsschlüssel	Beschreibung
root/keyboard/model	Legt das primäre Tastaturmodell fest.
root/keyboard/model2	Legt das sekundäre Tastaturmodell fest.
root/keyboard/numlock	Wenn der Wert 1 ist, dann wird die Funktion <b>NUM Lock</b> beim Systemstart aktiviert.
root/keyboard/rdp_kb	Dies ist ein interner Schlüssel, der verwendet wird, um eine RDP-Tastaturkarte zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/switch	Legt die Tastenkombination zum Umschalten zwischen dem ersten und dem zweiten Tastaturlayout fest ( <code>enable2</code> muss auch auf 1 eingestellt sein). Gültige Werte sind: <code>grp:ctrl_shift_toggle,grp:ctrl_alt_toggle,grp:alt_shift_toggle</code> .
root/keyboard/variant	Legt die primäre Tastaturvariante fest.
root/keyboard/variant2	Legt die sekundäre Tastaturvariante fest.

## logging

Registrierungsschlüssel	Beschreibung
root/logging/general/debug	Wenn der Wert 1 ist, dann ist Debugging für alle unterstützten Debug-Subsysteme aktiviert. Dies wird gewöhnlich in Verbindung mit <code>generateDiagnostic.sh</code> oder dem <b>Diagnostic</b> Diagnose-Tool der Systeminformation verwendet, um ein Diagnosepaket mit Systemdebugging-Protokollen zu erzeugen.
root/logging/general/debugLevel	Legt die Debugstufe fest. Dieser Wert wird von anderen Modulen genutzt, um die entsprechenden Protokolle zu generieren.
root/logging/general/showDebugLevelBox	Wenn der Wert 1 ist, ist die Option <b>Debugebene</b> auf der Registerkarte <b>Systemprotokolle</b> im Fenster <b>Systeminformationen</b> für Endbenutzer verfügbar. Wenn der Wert 0 ist, ist die Option nur für Administratoren verfügbar.

## mouse

Registrierungsschlüssel	Beschreibung
root/mouse/MouseHandedness	Wenn der Wert 0 ist, dann ist die Maus für Rechtshänder. Wenn der Wert 1 ist, dann ist die Maus für Linkshänder.
root/mouse/MouseSpeed	Legt die Beschleunigung des Mauszeigers fest. In der Regel ist ein Wert von 0 bis 25 der nutzbare Bereich. Ein Wert von 0 deaktiviert die Beschleunigung vollständig, wodurch die Maus sich in einem konstant langsamen, aber messbaren Tempo bewegt.
root/mouse/MouseThreshold	Legt die Anzahl an Pixeln fest, bevor Mausbeschleunigung aktiviert wird. Ein Wert von 0 legt die Beschleunigung als eine natürliche Kurve fest, welche die Beschleunigung graduell skaliert, sodass sowohl präzise als auch schnelle Bewegungen möglich sind.

## restore-points

Registrierungsschlüssel	Beschreibung
<code>root/restore-points/factory</code>	Gibt an, welcher Schnappschuss für eine Rücksetzung auf die Werkseinstellungen verwendet werden soll.

## screensaver

Registrierungsschlüssel	Beschreibung
<code>root/screensaver/SlideShowAllMonitors</code>	Wenn der Wert 1 ist, wird die Bildschirmschoner-Diashow auf allen Monitoren angezeigt. Wenn der Wert 0 ist, wird die Diashow nur auf dem primären Monitor angezeigt.
<code>root/screensaver/SlideShowInterval</code>	Legt das Intervall in Sekunden für Bilderwechsel in der Bildschirmschoner-Diashow fest.
<code>root/screensaver/SlideShowPath</code>	Gibt das Verzeichnis an, das die Bilder für die Bildschirmschoner-Diashow enthält.
<code>root/screensaver/enableCustomLogo</code>	Wenn der Wert 1 ist, dann werden die in <code>LogoPath</code> definierten, benutzerdefinierten Image für den Bildschirmschoner verwendet.
<code>root/screensaver/enableDPMS</code>	Wenn der Wert 0 ist, dann ist die Monitor-Energieverwaltung deaktiviert. Dies bewirkt, dass der Monitor eingeschaltet bleibt, bis er manuell ausgeschaltet wird.
<code>root/screensaver/enableScreensaver</code>	Wenn der Wert 1 ist, wird der Bildschirmschoner aktiviert.
<code>root/screensaver/enableSleep</code>	Wenn der Wert 1 ist, dann ist der Standbymodus aktiviert.
<code>root/screensaver/lockScreen</code>	Wenn der Wert 1 ist, ist ein Kennwort erforderlich, um vom Bildschirmschoner zum Desktop zurückkehren.
<code>root/screensaver/logoPath</code>	Legt den Pfad zu einem benutzerdefinierten Image für den Bildschirmschoner fest.
<code>root/screensaver/mode</code>	Legt den wiedergebenden Modus für die Anzeige des Bildschirmschoners fest (z. B. <code>Center</code> , <code>Tile</code> und <code>Stretch</code> ). Bei Auswahl von <code>Default</code> (Standard), wird das Bild ohne jegliche Verarbeitung angezeigt. Wenn der Wert <code>SlideShow</code> ist, durchläuft der Bildschirmschoner die Bilder im Verzeichnis, das von <code>SlideShowPath</code> angegebene wird.
<code>root/screensaver/off</code>	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Monitor ausgeschaltet wird.
<code>root/screensaver/origImageCopyPath</code>	Dies ist der Pfad, auf dem das benutzerdefinierte Image gespeichert ist, wenn <code>mode</code> auf <code>Default</code> eingestellt ist.
<code>root/screensaver/standby</code>	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Monitor in den Standby-Modus wechselt.
<code>root/screensaver/suspend</code>	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Monitor in den Suspend-Modus wechselt.
<code>root/screensaver/timeoutScreensaver</code>	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Bildschirmschoner startet.
<code>root/screensaver/timeoutSleep</code>	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Thin Client in den Sleep-Modus wechselt.

## security

Registrierungsschlüssel	Beschreibung
<code>root/security/mustLogin</code>	Wenn der Wert 1 ist, wird eine Anmeldung aller Benutzer vor dem Zugriff auf den Desktop erzwungen.

## sshd

Registrierungsschlüssel	Beschreibung
<code>root/sshd/enabled</code>	Wenn der Wert 1 ist, wird der SSH-Dämon aktiviert und es kann über SSH auf den Thin Client zugegriffen werden.
<code>root/sshd/userAccess</code>	Wenn der Wert 1 ist, können Endbenutzer über SSH eine Verbindung mit dem Thin Client herstellen.

## time

Registrierungsschlüssel	Beschreibung
<code>root/time/NTPServers</code>	Gibt zu verwendende NTP-Server über eine Liste mit Kommas als Trennzeichen an. Private NTP-Server oder große virtuelle NTP-Cluster wie <code>pool.ntp.org</code> sind die beste Auswahl, um die Serverlast zu minimieren. Deaktivieren Sie dieses Feld, um zur Verwendung von DHCP-Servern (Tag 42) anstelle einer festen Liste zurückzukehren.
<code>root/time/TimeServerIPAddress</code>	Dies ist der Zeitserver, der vom Linux-Befehl <code>net</code> verwendet wird. Diese Server sind in der Regel die DC-Server im Unternehmensnetzwerk. Dies sollte verwendet werden, wenn NTP-Server nicht konfiguriert sind oder nicht auf Tastatureingaben reagieren. Der Linux-Befehl <code>net</code> identifiziert diese Server selbstständig. Es kann hier jedoch eine spezifische Server-IP-Adresse bereitgestellt werden, falls gewünscht.
<code>root/time/WebServerURL</code>	Legt die Web-Server-URL (wie <code>hp.com</code> ) fest, die verwendet wird, wenn unter Verwendung des <code>http</code> -Protokoll die Zeit abgerufen wird. Diese URL kann sich innerhalb des Intranets oder im Internet befinden.
<code>root/time/timezone</code>	Legt die Zeitzone fest. Zeitzonen sollten angegeben werden, wie von <b>Linux Timezone</b> (Linux Zeitzone) im Tool für <b>Datum und Uhrzeit</b> in der Systemsteuerung definiert und sollten folgendes Format aufweisen: <i>Region/Subregion</i> .
<code>root/time/use24HourFormat</code>	Wenn der Wert <code>-1</code> ist, wählt das System das Format automatisch entsprechend dem Gebietschema. Bei Einstellung des Werts auf <code>0</code> wird das englische Format <code>a.m./p.m.</code> verwendet. Bei Einstellung des Werts auf <code>1</code> wird das 24-Stunden-Format verwendet.
<code>root/time/useDHCPTimezone</code>	Wenn der Wert <code>1</code> ist, versucht der Thin Client, die Zeitzone über DHCP einzustellen. Um die Zeitzone über diesen Registrierungsschlüssel korrekt einzustellen, stellen Sie sicher, dass der DHCP-Server für den Thin Client die DHCP-Kennung <code>tcode</code> weiterleitet (was normalerweise die Kennung <code>101</code> ist, jedoch auch <code>100</code> und <code>2</code> sein kann).
<code>root/time/useNTPServers</code>	Wenn der Wert <code>1</code> ist, ist die Verwendung von NTP-Zeitservern zum Synchronisieren der Thin Client-Uhr aktiviert. Wenn dies aktiviert ist, stellen Sie sicher, dass ein NTP-Server über DHCP oder über <code>NTPServers</code> angegeben ist.

## touchscreen

Registrierungsschlüssel	Beschreibung
<code>root/touchscreen/calibrated</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/enabled</code>	Wenn der Wert <code>1</code> ist, dann ist die Eingabe über den Touch-Bildschirm aktiviert.
<code>root/touchscreen/maxxx</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
<code>root/touchscreen/maxy</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/minx</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/miny</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/port</code>	Gibt den Anschluss an, an dem der Touchscreen angeschlossen ist.
<code>root/touchscreen/swapx</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/swapy</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/touchscreen/type</code>	Gibt den Typ der Controller des Touchscreens an.

## translation

Registrierungsschlüssel	Beschreibung
<code>root/translation/coreSettings/localeMapping/&lt;LanguageCode&gt;</code>	Dies sind interne Tasten, die verwendet werden, um die Textzeichenfolge neben der entsprechenden Sprache in der Sprachauswahl bereitzustellen. Dieser Schlüssel sollte keine Änderung erfordern.
<code>root/translation/coreSettings/localeSettings</code>	Legt das Gebietsschema für den Thin Client fest. Dieses Gebietsschema wird außerdem an die Remote-Verbindung weitergeleitet. Gültige Gebietsschemas sind <code>en_US</code> (Englisch), <code>de_DE</code> (Deutsch), <code>es_ES</code> (Spanisch), <code>fr_FR</code> (Französisch), <code>ru_RU</code> (Russisch), <code>ja_JP</code> (Japanisch), <code>ko_KR</code> (Koreanisch), <code>zh_CN</code> (vereinfachtes Chinesisch) und <code>zh_TW</code> (traditionelles Chinesisch).
<code>root/translation/gui/LocaleManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/translation/gui/LocaleManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/translation/gui/LocaleManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/translation/gui/LocaleManager/widgets/localeSettings</code>	Zum Einstellen des Status für das Widget „Locale Setting“ (Gebietsschema) im Sprachentool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

## usb-update

Registrierungsschlüssel	Beschreibung
<code>root/usb-update/authentication</code>	Wenn der Wert 1 ist, dann ist ein Administratorkennwort für USB-Updates erforderlich.
<code>root/usb-update/enable</code>	Wenn der Wert 1 ist, dann ist die automatische Erkennung für USB-Update aktiviert.
<code>root/usb-update/height</code>	Legt die Höhe des USB-Update-Fensters in Pixel fest.
<code>root/usb-update/searchMaxDepth</code>	Legt die Tiefe der Unterverzeichnisse zum Durchsuchen nach Updates fest. Das Einrichten einer hohen Suchtiefe führt möglicherweise zu Verzögerungen auf USB-Sticks, die Tausende von Verzeichnissen haben.
<code>root/usb-update/width</code>	Die Breite des USB-Update-Fensters in Pixel.

## users

Registrierungsschlüssel	Beschreibung
root/users/gui/hptc-user-rights/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/gui/hptc-user-rights/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/gui/hptc-user-rights/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/root/password	Legt das Administratorkennwort fest. Wenn kein Wert angegeben ist, ist der Administratormodus gesperrt.
root/users/user/SSO	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/user/WOL	Wenn der Wert 1 ist, wird Wake-on-LAN (WOL) aktiviert.
root/users/user/XHostCheck	Wenn der Wert 1 ist, dann sind nur die in <code>Root/Users/User/Xhosts</code> aufgelisteten Systeme in der Lage, den Thin Client Remote zu steuern.
root/users/user/apps/hptc-ad-dns-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>AD/DDNS Manager</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-agent-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>HPDM Agent</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-auto-update/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Automatic Update</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-background-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Hintergrund-Manager</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-cert-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Zertifikat-Manager</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-clientaggregation-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Clientaggregation</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-date-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Datum und Uhrzeit</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-dhcp-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>DHCP-Optionen</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-display-prefs/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Anzeigeeinstellungen</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-easy-update/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Easy Update</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-energy-star/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Energy Star</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-il8n-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Sprache</b> in der Systemsteuerung zugreifen.

<b>Registrierungsschlüssel</b>	<b>Beschreibung</b>
root/users/user/apps/hptc-keyboard-layout/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Tastaturlayout</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-mixer/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Sound</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-mouse/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Maus</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-network-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Netzwerkmanager</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-printer-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Drucker</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-restore/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Schnappschüsse</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-screenlock-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Energieverwaltung</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-security/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Sicherheit</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-shortcut-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Manager für Tastenkombinationen</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-sshd-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>SSH-Manager</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-task-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Task-Manager</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-text-editor/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Text-Editor</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-thinstate/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>ThinState</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-touchscreen/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Touchscreen</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-usb-mgr/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>USB-Manager</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-user-rights/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Anpassungscenter</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-vncshadow/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>VNC-Shadow</b> in der Systemsteuerung zugreifen.
root/users/user/apps/hptc-xterm/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>X-Terminal</b> in der Systemsteuerung zugreifen.  <b>ACHTUNG:</b> Das Aktivieren des Zugriffs auf ein X-Terminal stellt ein Sicherheitsrisiko dar und wird in einer Produktionsumgebung nicht empfohlen. Das X-Terminal sollte nur zur Verwendung der Fehlersuche (Debugging) in geschützten, nicht produktiven Umgebung aktiviert werden.
root/users/user/apps/scim-setup/authorized	Wenn der Wert 1 ist, können Endbenutzer auf das Element <b>Einrichten der SCIM-Eingabemethode</b> in der Systemsteuerung zugreifen.

Registrierungsschlüssel	Beschreibung
<code>root/users/user/hideDesktopPanel</code>	Bei Einstellung des Werts auf 1 werden Desktop-Bedienfelder, wie z. B. die Taskleiste, nicht gestartet oder auf dem Desktop angezeigt.
<code>root/users/user/kioskMode</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/users/user/launchConnectionManager</code>	Wenn der Wert 1 ist, wird Connection Manager beim Systemstart gestartet.
<code>root/users/user/rightclick</code>	Wenn der Wert 1 ist, dann ist das Rechtsklick-Menü für den Desktop aktiviert.
<code>root/users/user/showPasswordButton</code>	Wenn der Wert 1 ist, ist die Option <b>Show password</b> (Kennwort anzeigen) im Anmeldedialogfeld für Administratoren verfügbar.
<code>root/users/user/ssoconnectiontype</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/users/user/switchAdmin</code>	Wenn der Wert 1 ist, ist der Wechsel in den Administratormodus aktiviert.
<code>root/users/user/xhosts/&lt;UUID&gt;/xhost</code>	Gibt die IP-Adresse oder den Hostnamen eines Systems an, die bzw. der Zugriff zur Remotesteuerung des Thin Clients erhalten soll, wenn XHostCheck aktiviert ist.

## vncserver

Registrierungsschlüssel	Beschreibung
<code>root/vncserver/coreSettings/enableVncShadow</code>	Wenn der Wert 1 ist, dann ist der VNC-Shadowing-Server für den Thin Client aktiviert.
<code>root/vncserver/coreSettings/userNotificationMessage</code>	Legt die Benachrichtigungsmeldung fest, die dem Benutzer angezeigt wird, wenn jemand versucht, sich via VNC mit dem Thin Client zu verbinden.
<code>root/vncserver/coreSettings/vncNotifyShowTimeout</code>	Wenn der Wert 1 ist, dann wird eine Zeitüberschreitung für das Dialogfeld für die Benachrichtigung angewendet, die dem Benutzer angezeigt wird, wenn jemand versucht, sich via VNC mit dem Thin Client zu verbinden.
<code>root/vncserver/coreSettings/vncNotifyTimeout</code>	Legt die Zeitüberschreitung in Sekunden für das Dialogfeld für die Benachrichtigung fest, die dem Benutzer angezeigt wird, wenn jemand versucht, sich via VNC mit dem Thin Client zu verbinden.
<code>root/vncserver/coreSettings/vncNotifyUser</code>	Wenn der Wert 1 ist, wird dem Benutzer eine Benachrichtigung angezeigt, wenn jemand versucht, sich via VNC mit den Thin Client zu verbinden.
<code>root/vncserver/coreSettings/vncPassword</code>	Legt das Kennwort für VNC-shadowing fest. Der Schlüssel <code>VncUsePassword</code> muss ebenfalls aktiviert werden.
<code>root/vncserver/coreSettings/vncReadOnly</code>	Wenn der Wert 1 ist, dann wird VNC-Shadowing im nur-Ansicht-Modus arbeiten.
<code>root/vncserver/coreSettings/vncRefuseInDefault</code>	Wenn der Wert 1 ist, werden VNC-Anforderungen automatisch abgelehnt, wenn der Benutzer nicht vor Ablauf des Zeitlimits mit dem Benachrichtigungsdialog interagiert.

Registrierungsschlüssel	Beschreibung
<code>root/vncserver/coreSettings/vncTakeEffectRightNow</code>	Wenn der Wert 1 ist, dann werden VNC-Einstellungen sofort wirksam, nachdem sie geändert wurden.
<code>root/vncserver/coreSettings/vncUsePassword</code>	Wenn der Wert 1 ist, dann ist das in <code>VncPassword</code> angegebene Kennwort für VNC-shadowing erforderlich.
<code>root/vncserver/coreSettings/vncUseSSL</code>	Wenn der Wert 1 ist, dann wird SSL für VNC-Verbindungen verwendet.
<code>root/vncserver/gui/VNCShadowManager/name</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/vncserver/gui/VNCShadowManager/status</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/vncserver/gui/VNCShadowManager/title</code>	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
<code>root/vncserver/gui/VNCShadowManager/widgets/enableVncShadow</code>	Zum Einstellen des Status für das Widget <b>VNC-Shadow aktivieren</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/userNotificationMessage</code>	Zum Einstellen des Status für das Widget <b>Benutzerbenachrichtigung</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout</code>	Zum Einstellen des Status für das Widget <b>VNC-Zeitlimit für Benachrichtigung anzeigen</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout</code>	Zum Einstellen des Status für das numerische Widget im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser</code>	Zum Einstellen des Status für das Widget <b>VNC Notify User to Allow Refuse</b> (VNC: Benutzer benachrichtigen, um Ablehnung zuzulassen) im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
<code>root/vncserver/gui/VNCShadowManager/widgets/vncPassword</code>	Zum Einstellen des Status für das Widget <b>Kennwort einrichten</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit

Registrierungsschlüssel	Beschreibung
root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly	ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault	Zum Einstellen des Status für das Widget <b>VNC: Schreibgeschützt</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow	Zum Einstellen des Status für das Widget <b>Verbindungen standardmäßig verweigern</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword	Zum Einstellen des Status für das Widget <b>VNC-Server jetzt zurücksetzen</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL	Zum Einstellen des Status für das Widget <b>VNC: Kennwort verwenden</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL	Zum Einstellen des Status für das Widget <b>VNC: SSL verwenden</b> im VNC-Shadow-Tool. Durch die Einstellung <code>active</code> wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung <code>inactive</code> wird das Widget ausgeblendet. Durch die Einstellung <code>read-only</code> wird das Widget im schreibgeschützten Modus angezeigt.

# Index

## A

- AD/DDNS Manager 52
- Add-Ons 1
- Administratormodus 4
- Aktualisieren von Thin Clients
  - Aktualisieren per DHCP-Kennung 64
  - Aktualisieren per DNS-Alias 65
  - Aktualisierung per Übertragung 64
  - Manuelle Aktualisierung 65
- Anzeigeeinstellungen 45
- Anzeigeprofile 45
- Audioeinstellungen 42
- Audiumleitung
  - RDP 25
  - VMware Horizon View 32
- Auslieferungszustand 52

## B

- Background Manager 47
- Benutzermodus 4
- Benutzeroberfläche
  - Connection Manager (nur ThinPro) 7
  - Desktop 5
  - Taskleiste 6
  - Übersicht 5
- Betriebssystemkonfiguration, Auswählen 2
- Bildschirmschoner-Einstellungen 47

## C

- Certificate Manager 59
- Citrix
  - Einstellungen, allgemeine 10
  - Einstellungen, pro Verbindung 13
  - HP True Graphics 15
- Clientaggregation 43
- Clientkonfiguration 44
- Serverkonfiguration 45
- Clientprofil
  - Anpassung 67

- Hinzufügen eines symbolischen Links 70
- Hinzufügen von Dateien 68
- Laden 67
- Registrierungseinstellungen 68
- Speichern 70
- Zertifikate 68
- Custom-Verbindungen 41

## D

- Datums- und Uhrzeiteinstellungen 47
- DHCP-Optionen 59
- Drucker 46
- Druckerkonfiguration 70
- Druckerumleitung
  - RDP 24
  - VMware Horizon View 32

## E

- Easy Update 52
- Einführung 1
- Energieverwaltung 47
- Energieverwaltungseinstellungen 47

## F

- Fehlerbeseitigung 73
  - Netzwerkverbindung 73
  - verwenden der Systemdiagnose 74

## G

- Geräteumleitung
  - RDP 23
  - VMware Horizon View 31

## H

- HP Device Manager. *Siehe* HPDM Agent
  - Siehe auch* Remoteverwaltungsdienst
- HPDM Agent 52
- HP Smart Client Services
  - Installation 62

- Profile Editor. *Siehe* Profile Editor
- Übersicht 62
- unterstützte Betriebssysteme 62
- Siehe auch* Remoteverwaltungsdienst
- HP TeemTalk. *Siehe* TeemTalk
- HP True Graphics 15
- HP Velocity 51

## I

- Image-Aktualisierungen 1
- Imageerstellung und -verwendung. *Siehe* HP ThinState

## K

- Kennwörter, ändern 47
- Kioskmodus 9
- Komponenten-Manager 53
- Konfiguration eines parallelen Druckers 70
- Konfiguration eines seriellen Druckers 70

## M

- Massenspeicherumleitung
  - RDP 24
  - VMware Horizon View 31
- Mauseinstellungen 42
- MMR. *Siehe* Multimedia-Umleitung
- Multimedia-Umleitung
  - RDP 23
  - VMware Horizon View 31

## N

- Netzwerkeinstellungen
  - DNS 49
  - drahtgebunden 48
  - HP Velocity 51
  - IPSec 50
  - VPN 50
  - Wireless 49
  - Zugreifen 47

## P

Profile Editor 67

## R

### RDP

- Audioumleitung 25
- Druckerumleitung 24
- Einstellungen, allgemeine 17
- Einstellungen, pro Verbindung 17
- Geräteumleitung 23
- Massenspeicherumleitung 24
- Multimedia-Umleitung 23
- RemoteFX 22
- Sitzungen mit mehreren Monitoren 22
- Smart Card-Umleitung 26
- USB-Umleitung 23

Registrierungsschlüssel 79

RemoteFX 22

Remoteverwaltungsdienst,  
Auswählen 3

## S

SCEP Manager 58, 59

Schnappschüsse 52

SCIM 42

Serial Manager 58

Sicherheitseinstellungen 47

Smart Card-Umleitung

RDP 26

VMware Horizon View 33

Smart Zero. *Siehe*

Betriebssystemkonfiguration

Snipping Tool 58

So finden Sie weitere

Informationsquellen 1

Spracheinstellungen 47

SSH 39

SSHD-Manager 52

Standbymodus 47

Systemdiagnose 74

Systemsteuerung

AD/DDNS Manager 52

Anpassungscenter 47

Anzeige-Einstellungen 45

Auslieferungszustand 52

Clientaggregation 43

Datum und Uhrzeit 47

DHCP Options Manager 59

Dienstprogramme, ausblenden  
47

Easy Update 52

Einrichten der SCIM-

Eingabemethode 42

Energieverwaltung 47

Hintergrundeinstellungen 47

Komponenten-Manager 53

Maus 42

Netzwerk 47

SCEP Manager 58

Schnappschüsse 52

Serial Manager 58

Sicherheit 47

Snipping Tool 58

Sound 42

Sprache 47

SSHD-Manager 52

Task-Manager 58

Tastenkombinationen 58

Text-Editor 58

ThinState. *Siehe* HP ThinState

Touchscreen 42

Übersicht 42

VNC-Shadow 57

Wireless-Statistiken 52

X-Terminal 58

## T

Task-Manager 58

Tastenkombinationen 58

TeemTalk 36

Telnet 39

Text-Editor 58

Thin Clients

Aktualisieren. *Siehe* Aktualisieren  
von Thin Clients

ThinPro. *Siehe*

Betriebssystemkonfiguration

ThinState. *Siehe* HP ThinState

Touchscreen-Einstellungen 42

## U

USB-Umleitung

RDP 23

USB-Manager 46

VMware Horizon View 31

## V

Verbindungen

Ausblenden 47

Erweiterte Einstellungen 8  
Konfiguration 8

VMware Horizon View

Ändern von Protokollen 34

Audioumleitung 32

Druckerumleitung 32

Einstellungen, pro Verbindung  
26

Geräteumleitung 31

Massenspeicherumleitung 31

Multimedia-Umleitung 31

Sitzungen mit mehreren  
Monitoren 30

Smart Card-Umleitung 33

Tastenkombinationen 31

USB-Umleitung 31

Webcam-Umleitung 33

Zertifikate 34

VNC-Shadowing 57

## W

Web Browser

Einstellungen, allgemeine 35

Einstellungen, pro Verbindung  
36

Webcam-Umleitung

VMware Horizon View 33

Webseiten

Citrix-Support 1

HP Support 1

Microsoft Support 1

VMware-Support 1

Wireless-Statistiken 52

## X

XDMCP 38

X-Terminal 58

## Z

Zertifikate

Installation 59

VMware Horizon View 34