



HP ThinPro 5.0

Administratorhandbuch

© Copyright 2014 Hewlett-Packard
Development Company, L.P.

Microsoft, Windows und Windows Vista
sind eingetragene Marken der Microsoft
Unternehmensgruppe in den USA.

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 Herstellers 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: August 2014

Erste Ausgabe: Juni 2014

Teilenummer des Dokuments: 761886-042

Open-Source-Software

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 mit der Übermittlung einer Anforderung online unter <ftp://ftp.hp.com/pub/tcdebian/pool/thinpro50/source/>.

Allgemeines

In diesem Handbuch werden die folgenden Darstellungen zur Unterscheidung der verschiedenen Textelementen verwendet:

Darstellung	Definition
<Variable>	Variablen oder Platzhalter sind in spitze Klammern eingeschlossen. Ersetzen Sie beispielsweise <Pfadname> durch den entsprechenden Pfad, wie z. B. C:\Windows\System. Geben Sie bei der Eingabe des eigentlichen Wertes die Klammern nicht mit ein.
[Optionale Parameter]	Optionale Parameter sind in eckige Klammern eingeschlossen. Geben Sie bei der Angabe der Parameter die Klammern nicht mit ein.
"Wortgetreuer Wert"	Befehlszeilentext zwischen Anführungszeichen muss genau so eingegeben werden, wie er dargestellt ist, einschließlich der Anführungszeichen.

Inhaltsverzeichnis

1 Willkommen	1
So finden Sie weitere Informationsquellen	1
Vergleich von ThinPro und Smart Zero	1
Dokumentorganisation	2
2 Einführung	4
3 Navigieren auf der Benutzeroberfläche	5
Verwenden der Taskleiste	5
Verwenden der Connection Manager-Bedienelemente	6
Anzeigen der Systeminformationen	7
Ausblenden der Systeminformations-Bildschirmanzeigen	7
4 Konfigurationen der Systemsteuerung	8
Übersicht Systemsteuerung	8
Clientaggregation	12
Konfigurieren der Clientaggregation	13
Konfigurieren der Aggregation-Clients	13
Konfigurieren des Aggregation-Servers	14
Anzeigeeinstellungen	14
Konfigurieren von Druckern	15
USB-Geräte umleiten	15
Netzwerkeinstellungen	16
Drahtgebundene Netzwerkeinstellungen	16
Wireless-Netzwerkeinstellungen	17
DNS-Einstellungen	18
IPSec-Regeln	18
Konfigurieren von VPN-Einstellungen	19
Konfigurieren von HP Velocity	19
Anpassungscenter	19
HP ThinState	20
Verwalten von HP ThinPro-Images	20
Aufzeichnung von HP ThinPro-Images auf einem FTP-Server	20
Bereitstellung eines HP ThinPro-Images über FTP oder HTTP	21
Aufzeichnen eines HP ThinPro-Images auf einem USB-Flash-Laufwerk	21
Bereitstellung eines HP ThinPro-Images mit einem USB-Flash-Laufwerk	22

Verwalten von HP ThinPro-Konfigurationen	22
Speichern einer HP ThinPro-Konfiguration auf einem FTP-Server	22
Wiederherstellen einer HP ThinPro-Konfiguration über FTP oder HTTP	23
Speichern einer HP ThinPro-Konfiguration auf einem USB-Flash-Laufwerk	23
Wiederherstellen einer HP ThinPro-Konfiguration von einem USB-Flash- Laufwerk	23
VNC-Shadowing	24
Zertifikate	24
Certificate Manager	25
SCEP Manager	25
DHCP-Optionen	25
5 Gemeinsame Verbindungskonfigurationen	27
Gemeinsame Verbindungseinstellungen	27
Kioskmodus	28
6 Citrix-Verbindungen	29
Funktionen der Citrix-Verbindungsverwaltung	29
Citrix Receiver-Funktionen	29
HDX MediaStream-Supportmatrix	30
Citrix-Verbindung-Supportmatrix	31
Citrix – Allgemeine Einstellungen	31
Citrix – Verbindungsspezifische Einstellungen	35
7 RDP-Verbindungen	36
RPD-Funktionen	36
RDP – Allgemeine Einstellungen	36
RDP – Verbindungsspezifische Einstellungen	37
Verwenden von RemoteFX mit RDP	40
Verwenden von Multi-Monitor-Sitzungen mit RDP	40
Verwenden der Multimedia-Umleitung mit RDP	41
Verwenden der Geräteumleitung mit RDP	41
Verwenden einer USB-Umleitung mit RDP	41
Verwenden der Massenspeicherumleitung mit RDP	42
Verwenden der Druckerumleitung mit RDP	43
Audioumleitung mit RDP verwenden	43
Smart Card-Umleitung mit RDP verwenden	44
8 VMware Horizon View-Verbindungen	45
VMware Horizon View-Einstellungen	45

Verwenden von Multi-Monitor Sitzungen mit VMware Horizon View	48
Verwenden von Tastaturkürzeln mit VMware Horizon View	48
Verwenden der Multimedia-Umleitung mit VMware Horizon View	48
Geräte-Umleitung mit VMware Horizon View verwenden	48
USB-Umleitung mit VMware Horizon View verwenden	48
Massenspeicher-Umleitung mit VMware Horizon View verwenden	49
Drucker-Umleitung mit VMware Horizon View verwenden	49
Audioumleitung mit VMware Horizon View verwenden	49
Smart Card-Umleitung mit VMware Horizon View verwenden	50
Webcam-Umleitung mit VMware Horizon View verwenden	50
Ändern des VMware Horizon View Protokolltyps	51
Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung	51
VMware Horizon View-USB-Gerätefamilien	52
9 Web Browser-Verbindungen	54
Web Browser Allgemeine Einstellungen	54
Web Browser – Verbindungsspezifische Einstellungen	54
10 Zusätzliche Verbindungstypen (gilt nur für ThinPro-Konfiguration)	55
TeemTalk Verbindungseinstellungen	55
XDMCP Verbindungseinstellungen	57
SSH Verbindungseinstellungen	58
Telnet Verbindungseinstellungen	59
Benutzerdefinierte Verbindungseinstellungen	60
11 HP Smart Client Services	61
Unterstützte Betriebssysteme	61
Voraussetzungen für HP Smart Client Services	61
Abrufen von HP Smart Client Services	61
Anzeigen der Automatic Update-Website	62
Ein Automatic Update-Profil erstellen	62
Clients aktualisieren	62
Verwenden der Methode Aktualisierung per Übertragung	63
Verwenden der Aktualisierungsmethode mit der DHCP-Kennung	63
Beispiel für die Durchführung DHCP-Kennung	63
Verwenden der Aktualisierungsmethode mit DNS Alias	64
Verwenden der manuellen Aktualisierungsmethode	64
Eine manuelle Aktualisierung durchführen	64

12 Verwenden des Profile Editors	65
Zugriff auf den Profile Editor	65
Laden eines Client-Profiles	65
Ändern eines Client-Profiles	65
Auswahl der Plattform eines Client-Profiles	66
Auswahl des Verbindungstyps eines Client-Profiles	66
Ändern der Einstellungen der Registrierung eines Client-Profil	66
Aktivieren oder deaktivieren der Benutzerkonfigurationen auf Clients	66
Hinzufügen von Dateien zu einem Client-Profil	67
Hinzufügen einer Konfigurationsdatei zu einem Client-Profil	67
Zertifikate zu einem Client-Profil hinzufügen	67
Hinzufügen eines symbolischen Links zu einem Client-Profil	68
Speichern des Clients-Profiles	68
Konfigurieren eines seriellen oder parallelen Druckers	68
Abrufen der Druckereinstellungen	69
Einrichten von Druckeranschlüssen	69
Drucker auf dem Server installieren	69
13 Fehlerbeseitigung	71
Fehlerbeseitigung der Netzwerkverbindung	71
Fehlerbeseitigung bei Firmware-Beschädigung	72
Re-Imaging der Client-Firmware des Geräts	72
Fehlerbehebung bei abgelaufenen Citrix-Kennwörtern	72
Verwenden Systemdiagnose für die Fehlerbeseitigung	72
Speichern von Systemdiagnosedaten	73
Dekomprimieren der Systemdiagnosedateien	73
Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen	73
Dekomprimieren der Systemdiagnosedateien auf Linux- oder Unix-basierten Systemen	73
Anzeigen der Systemdiagnosedateien	73
Anzeigen von Dateien im Ordner Befehle	73
Anzeigen von Dateien im Ordner /var/log	74
Anzeigen von Dateien im Ordner /etc	74
Anhang A USB Updates	75
Anhang B BIOS-Tools	76
BIOS-Tool für Einstellungen	76
BIOS Flashing-Tool	76

Anhang C Ändern der Größe der Flash-Laufwerk-Partition	77
Anhang D Benutzerdefiniertes Anpassen des Smart Zero-Anmeldebildschirms	78
Anpassen des Bildschirmhintergrunds	78
Gemeinsame Attribute	78
Elemente	81
Image	83
Text	84
Anhang E Registrierungsschlüssel	87
root > Audio	88
root > CertMgr	89
root > ConnectionManager	89
root > ConnectionType	90
root > ConnectionType > custom	90
root > ConnectionType > firefox	94
root > ConnectionType > freerdp	98
root > ConnectionType > ssh	106
root > ConnectionType > teemtalk	112
root > ConnectionType > telnet	115
root > ConnectionType > view	119
root > ConnectionType > xdmcp	127
root > ConnectionType > xen	132
root > DHCP	144
root > Dashboard	144
root > Display	145
root > Network	147
root > SCIM	152
root > Serial	152
root > SystemInfo	153
root > TaskMgr	153
root > USB	154
root > auto-update	158
root > background	160
root > config-wizard	160
root > desktop	161
root > entries	161
root > keyboard	162
root > logging	163
root > mouse	163

root > screensaver	164
root > security	165
root > sshd	165
root > time	165
root > touchscreen	166
root > translation	166
root > usb-update	167
root > users	167
root > vncserver	170

Index	174
--------------------	------------

1 Willkommen

Dieses Handbuch ist für Administratoren von HP Thin Client-Modellen bestimmt, die auf dem HP ThinPro-Betriebssystem basieren. Es wird vorausgesetzt, dass Sie das aktuellste von HP angebotene Image verwenden und sich als Administrator anmelden, wenn Sie Konfigurationen vornehmen oder auf die Administrations-Dienstprogramme zugreifen.

So finden Sie weitere Informationsquellen

Ressource	Inhalt
HP Support-Website http://www.hp.com/support	Image-Aktualisierungen und Add-ons Dokumentation für HP Software, die in diesem Handbuch nicht detailliert beschrieben wird. TIPP: Wenn Ihre Suchergebnisse die gewünschte Software nicht lokalisieren können, suchen Sie stattdessen nach dem Thin Client-Modell.
Microsoft Support-Website http://support.microsoft.com	Dokumentation für Microsoft Software, die in diesem Handbuch nicht detailliert beschrieben wird.
Citrix Support-Website http://www.citrix.com/support	Dokumentation für Citrix Software, die in diesem Handbuch nicht detailliert beschrieben wird.
VMware Support-Website http://www.vmware.com/support	Dokumentation für VMware Software, die in diesem Handbuch nicht detailliert beschrieben wird.

Vergleich von ThinPro und Smart Zero

Beginnend mit HP ThinPro 5.0 sind ThinPro und Smart Zero zwei unterschiedliche Konfigurationen desselben Betriebssystem-Images. Sie können ganz einfach zwischen den beiden Konfigurationen wechseln, indem Sie eine Option in der Systemsteuerung verwenden. Die folgende Tabelle zeigt einen Vergleich von ThinPro und Smart Zero.

	ThinPro	Smart Zero
Verfügbare Verbindungstypen	<ul style="list-style-type: none">• Citrix• RDP• VMware Horizon View• Web Browser (Firefox)• TeemTalk• XDMCP• SSH• Telnet• Custom	<ul style="list-style-type: none">• Citrix• RDP• VMware Horizon View• Web Browser (Firefox)

Anzahl der Verbindungen, die zu einem Zeitpunkt unterstützt werden	Mehrere	Eine
Kioskmodus-StandardEinstellung	Deaktiviert	Aktiviert

Dokumentorganisation

Dieses Handbuch ist in die folgenden Kapitel und Anhänge unterteilt:

- [„Einführung“ auf Seite 4](#) – Beschreibt die grundlegenden Schritte zur Bereitstellung eines Thin Clients, auf dem HP ThinPro ausgeführt wird.
- [„Navigieren auf der Benutzeroberfläche“ auf Seite 5](#) – Bietet eine Übersicht der verschiedenen Komponenten der Benutzeroberfläche.
- [„Konfigurationen der Systemsteuerung“ auf Seite 8](#) – Beschreibt die verbindungsabhängigen Einstellungen und Konfigurationen in der Systemsteuerung und Details zu einigen der erweiterten Konfigurationen.
- [„Gemeinsame Verbindungskonfigurationen“ auf Seite 27](#) – Beschreibt die Einstellungen die für alle Verbindungstypen gleich sind, und die Konfiguration eines Clients für den Kioskmodus.
- [„Citrix-Verbindungen“ auf Seite 29](#) – Beschreibt die Einstellungen und Konfigurationen für den Verbindungstyp Citrix.
- [„RDP-Verbindungen“ auf Seite 36](#) – Beschreibt die Einstellungen und Konfigurationen für den Verbindungstyp RDP.
- [„VMware Horizon View-Verbindungen“ auf Seite 45](#) – Beschreibt die Einstellungen und Konfigurationen für den Verbindungstyp VMware Horizon View.
- [„Web Browser-Verbindungen“ auf Seite 54](#) – Beschreibt die Einstellungen für den Verbindungstyp Web Browser.
- [„Zusätzliche Verbindungstypen \(gilt nur für ThinPro-Konfiguration\)“ auf Seite 55](#) – Beschreibt die Einstellungen für die Verbindungstypen TeamTalk, XDMCP, SSH, Telnet und Benutzerdefiniert.
- [„HP Smart Client Services“ auf Seite 61](#) – Beschreibt, wie man mit HP Smart Client Services und der Verwendung von Automatic Update über Fernzugriff eine große Anzahl an Thin Clients verwalten kann.
- [„Verwenden des Profile Editors“ auf Seite 65](#) – Beschreibt die Verwendung des Profile Editors zum Einrichten und Bearbeiten von Client-Profilen, die Verbindungsinformationen, Einstellungen und Dateien enthalten, die beim Selbstkonfigurationsvorgang verwendet werden.
- [„Fehlerbeseitigung“ auf Seite 71](#) – Beschreibt häufige Probleme und Lösungen bei der Fehlerbehebung.
- [„USB Updates“ auf Seite 75](#) – Beschreibt die Installation von Add-ons und Profil-Updates von einem USB-Flash-Laufwerk.
- [„BIOS-Tools“ auf Seite 76](#) – Beschreibt die Anzeige und Aktualisierung von BIOS-Einstellungen und das Flashen einer neuen BIOS-Version.
- [„Ändern der Größe der Flash-Laufwerk-Partition“ auf Seite 77](#) – Beschreibt, wie man die Größe der Partition Flash-Laufwerk erhöhen kann.


- [„Benutzerdefiniertes Anpassen des Smart Zero-Anmeldebildschirms“ auf Seite 78](#) – Beschreibt die gängigen Attribute und Elemente, die zur Anpassung des Bildschirmhintergrunds für die Client-Anmeldung verwendet werden.
- [„Registrierungsschlüssel“ auf Seite 87](#) – Liste der Pfade, Funktionen und Optionen für die HP ThinPro-Registrierungsschlüssel.

2 Einführung


Wenn Sie das erste Mal einen neuen Thin Client einschalten, auf dem HP ThinPro installiert ist, wird ein Setup Utility ausgeführt.

Zuerst sucht das Setup Utility nach einer Netzwerkverbindung. Wenn bestimmte Netzwerkeinstellungen erforderlich sind, klicken Sie auf die Schaltfläche **Network Settings** (Netzwerkeinstellungen), um den Network Manager zu öffnen (siehe [Netzwerkeinstellungen auf Seite 16](#) für weitere Informationen).

Das Setup Utility überprüft dann, ob der Thin Client durch HP Smart Client Services oder durch HP Device Manager (HPDM) verwaltet wird. Wenn der Thin Client durch eines dieser Programme verwaltet wird, wird das Setup Utility beendet und das Management-Programm führt vordefinierte Konfigurationen am Thin Client aus.

 **HINWEIS:** Weitere Informationen zu HP Smart Client Services finden Sie unter „[HP Smart Client Services](#)“ auf [Seite 61](#). Weitere Informationen zu HPDM finden Sie unter <http://www.hp.com/go/hpdm>.


Wenn der Thin Client nicht durch HP Smart Client Services oder HPDM verwaltet wird, überprüft das Utility, ob ein Image-Update bei HP erhältlich ist. Falls ja, klicken Sie auf **Install now** (Jetzt installieren), auf der Registerkarte **Software Update**, um das Image zu aktualisieren.

 **TIPP:** Wenn Sie Ihren eigenen internen Ort für die Image-Updates aufrechterhalten möchten, können Sie benutzerdefiniert festlegen, wo das Betriebssystem nach Updates sucht, indem Sie den folgenden Registrierungsschlüssel ändern:


```
root/config-wizard/FirmwareUpdate/firmwareUpdateURL
```

Wenn Sie überprüfen möchten, ob Service Packs oder Package-Updates verfügbar sind, klicken Sie auf **Easy Update**, um die HP Easy Tools zu starten.

Wenn Sie den HPDM Agent oder die Automatic Update-Einstellungen für HP Smart Client Services manuell konfigurieren müssen, klicken Sie auf der Registerkarte **Device Management** (Geräteverwaltung) der Setup Utility und wählen Sie die entsprechende Option.

 **TIPP:** Wenn Sie bei jedem Start des Thin Clients nach Software-Updates suchen möchten, aktivieren Sie die Option **Check for software updates every boot** (Bei jedem Start nach Software-Updates suchen).

Wenn Sie das Setup Utility schließen, ohne dass Verbindungen konfiguriert sind, werden Sie aufgefordert, eine Verbindung zu konfigurieren.

 **HINWEIS:** Dieser Erstverbindungs-Assistent ermöglicht eine schnellere Einrichtung, als der standardmäßige Connection Manager-Assistent.

Wenn Sie beabsichtigen, einen einzigen Thin Client zu konfigurieren und seine Konfigurationen anschließend auf andere Thin Clients mit HP ThinState anwenden möchten (siehe [HP ThinState auf Seite 20](#)), verwenden Sie die Systemsteuerung, um alle gewünschten Konfigurationen vorzunehmen. Weitere Informationen finden Sie unter „[Navigieren auf der Benutzeroberfläche](#)“ auf [Seite 5](#) und „[Konfigurationen der Systemsteuerung](#)“ auf [Seite 8](#).

3 Navigieren auf der Benutzeroberfläche

In diesem Kapitel werden folgende Themen behandelt:

- [Verwenden der Taskleiste](#)
- [Verwenden der Connection Manager-Bedienelemente](#)
- [Anzeigen der Systeminformationen](#)

Verwenden der Taskleiste

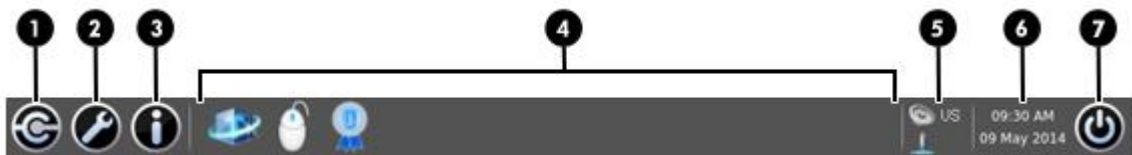
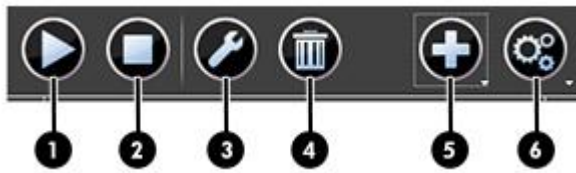


Tabelle 3-1 Komponenten der Taskleiste

1	Connection Manager – Zum Starten, Stoppen, Hinzufügen, Bearbeiten und Löschen von Remote-Verbindungen. Weitere Informationen finden Sie unter Verwenden der Connection Manager-Bedienelemente auf Seite 6 .
2	Systemsteuerung – Zum Konfigurieren des Clients, Wechseln zwischen Administratormodus und Benutzermodus und Suchen nach Softwareupdates. Weitere Informationen finden Sie unter Übersicht Systemsteuerung auf Seite 8 .
3	Systeminformationen – Zum Anzeigen von System-, Netzwerk- und Softwareinformationen zum Client. Weitere Informationen finden Sie unter Anzeigen der Systeminformationen auf Seite 7 .
4	Anwendungsbereich – Zeigt die Symbole für die derzeit geöffneten Anwendungen. TIPP: Um eine Anwendung auszuwählen und in den Vordergrund zu holen, können Sie Strg+Alt gedrückt halten, und dann wiederholt auf die Tabulatortaste drücken.
5	Infobereich – Bietet schnellen Zugriff auf den Audiomixer und die virtuelle Tastatur, und zeigt den aktuellen Netzwerkstatus. Wenn die Sprache auf Chinesisch, Japanisch oder Koreanisch eingestellt ist, wird ebenfalls ein Symbol angezeigt, das schnellen Zugriff auf die Bedienelemente der Smart Common Input Method (SCIM) angezeigt.
6	Datum und Uhrzeit – Zeigt das aktuelle Datum und die Uhrzeit an. Klicken Sie hier, um auf die Datum- und Uhrzeiteinstellungen zuzugreifen.
7	Ein/Aus-Taste – Zum Abmelden vom Client, Neustart oder Ausschalten des Clients.

Verwenden der Connection Manager-Bedienelemente



1	Start – Startet die ausgewählte Verbindung.
2	Stopp – Beendet die ausgewählte Verbindung.
3	Bearbeiten – Öffnet einen Connection Manager speziell für den ausgewählten Verbindungstyp (z. B. Citrix Connection Manager) und ermöglicht das Bearbeiten der für die ausgewählte Verbindung spezifischen Einstellungen.
4	Löschen – Löscht die ausgewählte Verbindung.
5	Hinzufügen – Zum Hinzufügen einer neuen Verbindung. HINWEIS: Siehe Vergleich von ThinPro und Smart Zero auf Seite 1 für eine Liste der verfügbaren Verbindungstypen.
6	Einstellungen – Ermöglicht das 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:

- [„Gemeinsame Verbindungskonfigurationen“ auf Seite 27](#)
- [„Citrix-Verbindungen“ auf Seite 29](#)
- [„RDP-Verbindungen“ auf Seite 36](#)
- [„VMware Horizon View-Verbindungen“ auf Seite 45](#)
- [„Web Browser-Verbindungen“ auf Seite 54](#)
- [„Zusätzliche Verbindungstypen \(gilt nur für ThinPro-Konfiguration\)“ auf Seite 55](#)

Anzeigen der Systeminformationen

Klicken Sie in der Taskleiste auf die Schaltfläche **Systeminformationen**, um System-, Netzwerk- und Softwareinformationen zum Client anzuzeigen. In der folgende Tabelle werden die Informationen beschrieben, die auf den einzelnen Registerkarten angezeigt werden.

Tabelle 3-2 Registerkarte System Information (Systeminformationen)

Registerkarte	Beschreibung
General (Allgemein)	Zeigt Informationen über BIOS, Betriebssystem, CPU und Speicher an.
Network (Netzwerk)	Zeigt Informationen über Netzwerkschnittstelle, Gateway und DNS-Einstellungen an.
Net Tools (Netzwerk-Tools)	Bietet die folgenden Tools zur Überwachung und Problembhebung: <ul style="list-style-type: none">• Ping – Spezifizieren einer IP-Adresse von einem anderen Gerät im Netzwerk, um eine Verbindung aufzubauen.• DNS Lookup – Zum Auflösen eines Domänennamens in eine IP-Adresse.• Trace Route – Zum Nachverfolgen des Pfades, auf dem ein Netzwerkpaket von einem Gerät zum anderen gesendet wird.
Software Information (Softwareinformationen)	Zeigt Name und Versionsnummer der auf dem Client installierten Software an.
System Logs (Systemprotokolle)	Zeigt folgende Protokolle an: <ul style="list-style-type: none">• Network Manager• Smart Zero Client Service• DHCP Wired Leases• DHCP Wireless Leases• Kernel• X Server• Connection Manager <p>Markieren Sie Enable Debug Mode (Debugmodus aktivieren), um weitere Informationen anzuzeigen, die möglicherweise von HP Support bei der Problembhebung angefragt werden.</p> <p>Klicken Sie auf Diagnostic (Diagnose), um eine Diagnosedatei zu speichern. Weitere Informationen finden Sie unter Verwenden Systemdiagnose für die Fehlerbeseitigung auf Seite 72.</p>

Ausblenden der Systeminformations-Bildschirmanzeigen

Siehe [root > SystemInfo auf Seite 153](#) für Informationen über die Registrierungsschlüssel, die zum Ausblenden von Systeminformationen verwendet werden können.

4 Konfigurationen der Systemsteuerung

Dieses Kapitel enthält die folgenden Themen:

- [Übersicht Systemsteuerung](#)
- [Clientaggregation](#)
- [Anzeigeeinstellungen](#)
- [Konfigurieren von Druckern](#)
- [USB-Geräte umleiten](#)
- [Netzwerkeinstellungen](#)
- [Anpassungscenter](#)
- [HP ThinState](#)
- [VNC-Shadowing](#)
- [Zertifikate](#)
- [DHCP-Optionen](#)

Übersicht Systemsteuerung

Die Systemsteuerung bietet Zugriff auf Dienstprogramme für die Konfiguration des Clients. Die Dienstprogramme sind alle im Administratormodus zugänglich. Im Benutzermodus kann nur auf die Dienstprogramme zugegriffen werden, die vom Administrator für die Verwendung durch den Benutzer aktiviert wurden.

So wechseln Sie zwischen Administratormodus und Benutzermodus:

- ▲ Wählen Sie in der Systemsteuerung **Administrator/User Mode Switch** (Zwischen Administrator-/Benutzermodus wechseln).

Wenn Sie zum ersten Mal in den Administratormodus wechseln, werden Sie aufgefordert, ein Administratorkennwort einzurichten. Das Administratorkennwort muss im Anschluss jedes Mal eingegeben werden, wenn Sie zum Administratormodus wechseln möchten.

💡 **TIPP:** Wenn Sie sich im Administratormodus befinden, ist der Bildschirm rot umrandet.

Die folgenden Tabellen beschreiben die Dienstprogramme der Systemsteuerung, die in den einzelnen Menü-Kategorien verfügbar sind.

💡 **TIPP:** Um anzugeben, auf welche Dienstprogramme die Standardbenutzer Zugriff haben, wählen Sie in der Systemsteuerung **Setup > Customization Center** (Setup > Anpassungscenter) und wählen die Dienstprogramme in der Liste der **Applications** (Anwendungen) aus oder ab.

Tabelle 4-1 Control Panel > Peripherals (Systemsteuerung > Peripheriegeräte)

Menüoption	Beschreibung
Client Aggregation (Clientaggregation)	Zum Konfigurieren der Einstellungen für die Clientaggregation. Ermöglicht die Kombination der Thin

Tabelle 4-1 Control Panel > Peripherals (Systemsteuerung > Peripheriegeräte) (Fortsetzung)

Menüoption	Beschreibung
	Clients, sodass zusätzliche Anzeigebereiche geschaffen werden. Weitere Informationen finden Sie unter Clientaggregation auf Seite 12 .
Display Preferences (Anzeigeeinstellungen)	Ermöglicht das Konfigurieren und Testen von Optionen für eine primäre und sekundäre Anzeige. Weitere Informationen finden Sie unter Anzeigeeinstellungen auf Seite 14 .
Keyboard Layout (Tastaturlayout)	Damit können Sie das Tastaturlayout ändern, um es der Sprache der Tastatur anzupassen.
Sound	Zur Stufenregelung von Audio-Wiedergabe und -Eingang.
Mouse (Maus)	Zum Konfigurieren der Mausgeschwindigkeit und der Mauseingabe für Rechtshänder oder Linkshänder.
Printers (Drucker)	Zum Einrichten von lokalen und Netzwerkdruckern. Lokale Drucker können im Netzwerk gemeinsam genutzt werden. Weitere Informationen finden Sie unter Konfigurieren von Druckern auf Seite 15 .
Touchscreen	Zum Konfigurieren der Touchscreen-Optionen.
USB Manager	Zum Konfigurieren der Umleitungsoptionen für USB-Geräte. Weitere Informationen finden Sie unter USB-Geräte umleiten auf Seite 15 .
SCIM Input Method Setup (Einstellung der Eingabemethode)	Ermöglicht die Konfiguration der Smart Common Input Method (SCIM) für die Eingabe von Chinesisch, Japanisch und Koreanisch. Weitere Informationen zu diesem Open-Source-Programm finden Sie unter http://sourceforge.net/apps/mediawiki/scim/index.php?title=Main_Page .

Tabelle 4-2 Control Panel > Setup (Systemsteuerung > Setup)

Menüoption	Beschreibung
Background Manager (Hintergrundeinstellungen)	Zum Konfigurieren des Hintergrund-Designs.
Date and Time (Datum und Uhrzeit)	Zum Konfigurieren der Zeitzone sowie der Datums- und Uhrzeitoptionen.
Language (Sprache)	Damit können Sie die Client-Bedienoberfläche in einer anderen Sprache anzeigen.
Network (Netzwerk)	Zum Konfigurieren der Netzwerkeinstellungen. Weitere Informationen finden Sie unter Netzwerkeinstellungen auf Seite 16 .
Screensaver (Bildschirmschoner)	Zum Konfigurieren eines Bildschirmschoners.

Tabelle 4-2 Control Panel > Setup (Systemsteuerung > Setup) (Fortsetzung)

Menüoption	Beschreibung
Sicherheit	Damit können Sie die Systemkennwörter für Administrator und Benutzer des Clients einrichten oder ändern.
Customization Center (Anpassungszentrum)	<p>Es stehen folgende Aktionen zur Verfügung:</p> <ul style="list-style-type: none">• Wechseln zwischen den ThinPro- und Smart Zero-Konfigurationen• Konfigurieren der Desktop- und Taskleisten-Optionen• Auswahl der Verbindungstypen und Dienstprogramme der Systemsteuerung, auf die Standardbenutzer zugreifen können <p>Weitere Informationen finden Sie unter Anpassungszentrum auf Seite 19.</p>

Tabelle 4-3 Control Panel > Management (Systemsteuerung > Verwaltung)

Menüoption	Beschreibung
AD/DDNS Manager	<p>Zum Hinzufügen des Clients zu einer Organisationseinheit des Active Directory-Servers und zur Aktivierung automatischer Dynamic DNS-Updates der Zuordnung von Namen und IP-Adresse des Clients.</p> <p>HINWEIS: Dieses Dienstprogramm aktiviert nicht die Authentifizierung gegenüber der Active Directory-Datenbank.</p>
HPDM Agent	<p>Zum Konfigurieren des HP Device Manager (HPDM) Agent.</p> <p>Weitere Informationen zu HP Device Manager finden Sie im <i>HP Device Manager Administratorhandbuch</i>.</p>
Automatic Update (Automatische Updates)	<p>Damit können Sie den Automatic Update-Server manuell zurücksetzen.</p> <p>Weitere Informationen finden Sie unter „HP Smart Client Services“ auf Seite 61.</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 Client installieren können.</p> <p>Weitere Informationen über HP Easy Tools finden Sie im <i>HP Easy Tools Administratorhandbuch</i>.</p>
Snapshots (Momentaufnahmen)	<p>Zum Wiederherstellen eines früheren Zustands oder der Standard-Werkzeugeinstellungen des Clients.</p>
SSHD Manager	<p>Ermöglicht den Zugriff über ein 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 HP ThinState auf Seite 20.</p>
VNC-Shadow	<p>Zum Konfigurieren von VNC-Shadowing-Optionen.</p>

Tabelle 4-3 Control Panel > Management (Systemsteuerung > Verwaltung) (Fortsetzung)

Menüoption	Beschreibung
	Weitere Informationen finden Sie unter VNC-Shadowing auf Seite 24 .

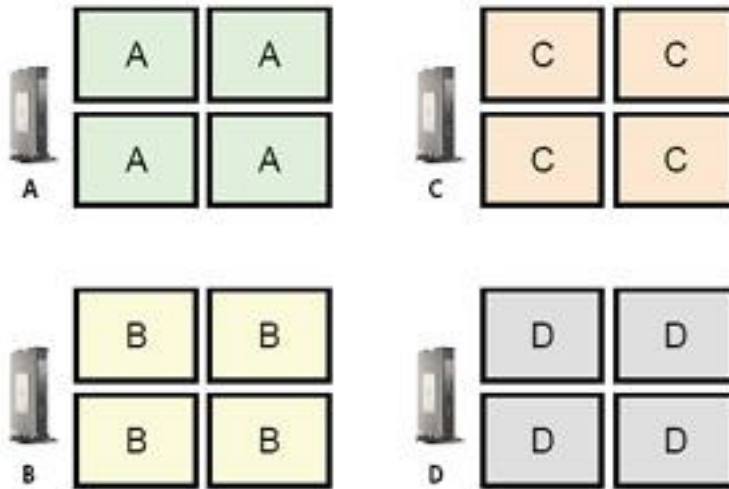
Tabelle 4-4 Control Panel > Advanced (Systemsteuerung > Erweitert)

Menüoption	Beschreibung
Certificates (Zertifikate)	Öffnet den Zertifikat-Manager, mit dem man ganz einfach Zertifikate importieren, anzeigen oder entfernen kann. Weitere Informationen finden Sie unter Certificate Manager auf Seite 25 .
CPU Manager	Zur Auswahl der CPU-Leistung zwischen Balanced (Ausgeglichen) und High Performance .
DHCP Options (DHCP-Optionen)	Zum Konfigurieren der DHCP-Optionen. Weitere Informationen finden Sie unter DHCP-Optionen auf Seite 25 .
SCEP Manager	Ermöglicht die netzwerkbasierte Zertifikatsverwaltung.
Serial Manager	Zur Konfiguration serieller Geräte.
Keyboard Shortcuts (Tastenkombinationen)	Zum Erstellen, Ändern und Löschen von Tastenkombinationen.
Task Manager	Damit können Sie die CPU-Auslastung und den CPU-Nutzungsverlauf für den Client überwachen.
Text Editor	Öffnet einen einfachen Texteditor zum Anzeigen und Bearbeiten von Textdateien.
X Terminal	Zum Ausführen von Linux-Befehlen.

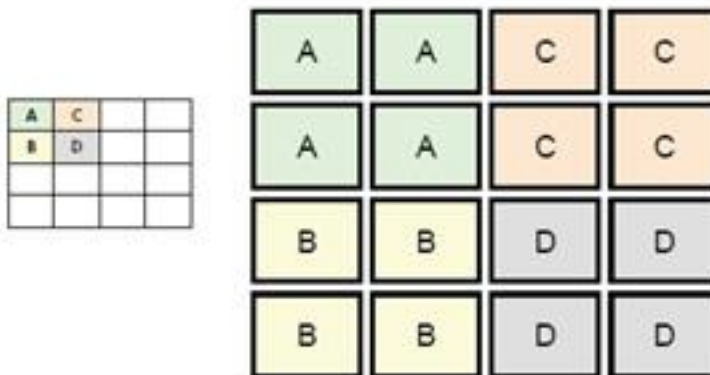
Clientaggregation

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

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

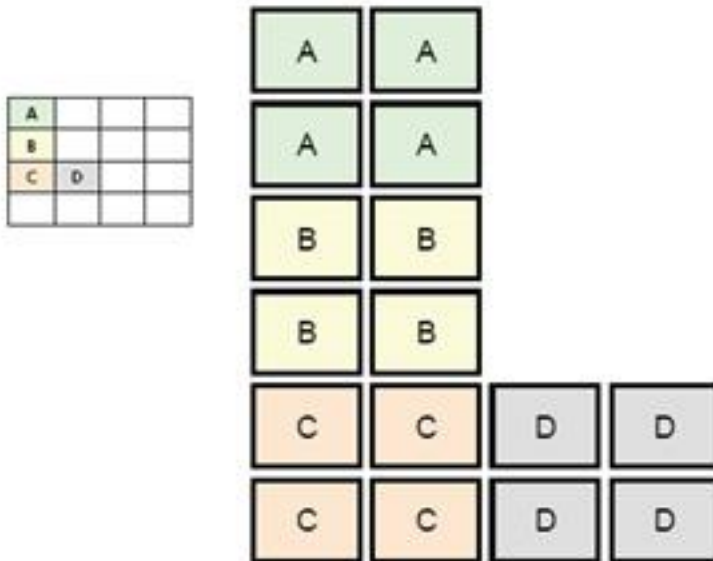


Mithilfe der Clientaggregation können Sie die vier Clients in einem 4 x 4-Raster anordnen. Die folgende Abbildung zeigt eine der möglichen Anordnungen.




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 Clients hinweg ausgedehnt oder zwischen ihnen verschoben werden. In der Regel wird jeder Client Fenster erstellen, die auf der jeweiligen Verbindung zum zugehörigen Remote-Computer basieren, und es wird kein Bedarf bestehen, die Fenster zwischen den Clients zu verschieben.

Der Client, der physisch mit der Tastatur und der Maus verbunden ist, wird als Aggregation-Server bezeichnet. Die anderen 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 13](#)
2. [Konfigurieren des Aggregation-Servers auf Seite 14](#)

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. Klicken Sie auf **Client**.

3. Geben Sie den Server-Hostnamen oder die IP-Adresse des Aggregation-Servers in das Feld ein.
4. Klicken Sie auf **Apply** (Übernehmen).

Konfigurieren des Aggregation-Servers

So konfigurieren Sie den Aggregation-Server:

1. Wählen Sie in der Systemsteuerung **Peripherals > Client Aggregation** (Peripheriegeräte > Clientaggregation).
2. Klicken Sie auf **Server**.
3. Der Aggregation-Server wird in einem blauen Feld angezeigt, das seinen Hostnamen enthält. Klicken Sie auf den Aggregation-Server und ziehen Sie ihn an die gewünschte Stelle im 4 x 4-Raster.
4. Klicken Sie auf 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 4x4-Raster lässt sich jederzeit ändern, indem Sie auf einen Client-Computer klicken und diesen an eine neue Position ziehen.

Nach dem Konfigurieren der Aggregation-Clients und des Aggregation-Servers versuchen diese automatisch, über verschlüsselte Verbindungen miteinander zu kommunizieren. Klicken Sie auf **Status**, um den Verbindungsstatus zwischen den Computern anzuzeigen.

Anzeigeeinstellungen

HP ThinPro ermöglicht das Erstellen von Profilen für Anzeigeeinstellungen und die Anwendung verschiedener Profile auf verschiedene Monitore. 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 klicken Sie anschließend auf **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.
- 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. Klicken Sie im Dialogfeld **Printing** (Drucken) auf **Add** (Hinzufügen).
3. Wählen Sie im Dialogfeld **New Printer** (Neuer Drucker) den Drucker, den Sie konfigurieren möchten, und klicken Sie dann auf **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 klicken Sie dann auf **Forward** (Weiter).
5. Wählen Sie das Modell und den Treiber für den Drucker, und klicken Sie dann auf **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, klicken Sie auf **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. Klicken Sie auf **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 ändern. Klicken Sie dazu auf das Kontrollkästchen links neben dem Gerätenamen zum Wechseln zwischen den folgenden Umleitungsoptionen:
 - **Use Defaults** (Standardeinstellungen verwenden)
 - **Redirect** (Umleiten)
 - **Do Not Redirect** (Nicht umleiten)
4. Wenn Sie fertig sind, klicken Sie auf **OK**.

Netzwerkeinstellungen

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

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

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

- [Drahtgebundene Netzwerkeinstellungen](#)
- [Wireless-Netzwerkeinstellungen](#)
- [DNS-Einstellungen](#)
- [IPSec-Regeln](#)
- [Konfigurieren von VPN-Einstellungen](#)
- [Konfigurieren von HP Velocity](#)

Drahtgebundene Netzwerkeinstellungen

Die folgende Tabelle beschreibt die im Network Manager unter der Registerkarte **Wired** (Drahtgebunden) verfügbaren Optionen.

Option	Beschreibung
Enable IPv6 (IPv6 aktivieren)	Aktiviert das IPv6. Standardmäßig wird IPv4 verwendet und es können nicht beide gleichzeitig verwendet werden.
Ethernet Speed (Ethernet-Geschwindigkeit)	Zum Festlegen der Ethernet-Geschwindigkeit. Wenn Ihre Switch oder Hub nicht über eine spezielle Anforderung verfügt, lassen Sie dies auf der Standardeinstellung Automatic (Automatisch).
Connection Method (Verbindungsmethode)	Zur Auswahl zwischen Automatic (Automatisch) und Static (Statisch). Wenn Ihre Netzwerkkumgebung DHCP verwendet, sollte die Option Automatic (Automatisch) ohne weitere Konfigurationen funktionieren. Wenn Static (Statisch) ausgewählt ist, werden die Einstellungen für Static Address Configuration (Statische Adressenkonfiguration) zur Verfügung stehen. Vergewissern Sie sich, dass Sie diese Werte dem entsprechend eingeben, ob Sie IPv4 oder IPv6 verwenden.
MTU	Ermöglicht die Eingabe der maximalen Übertragungseinheit (in Byte).
Security Settings (Sicherheitseinstellungen)	Zum Festlegen der Authentifizierungseinstellung auf eine der folgenden Optionen: <ul style="list-style-type: none"> • None (Keine) • 802.1X-TTLS

Option	Beschreibung
	<ul style="list-style-type: none"> 802.1X-PEAP 802.1X-TLS <p>Beachten Sie Folgendes über TTLS und PEAP:</p> <ul style="list-style-type: none"> Die Einstellung der Option Inner Authentication (Innere Authentifizierung) sollte auf das eingestellt werden, was Ihr Server unterstützt. Die Einstellung des CA Certificate (CA-Zertifikat) sollte auf das Server-Zertifikat auf dem lokalen Client verweisen. Username (Benutzername) und Password (Kennwort) sind die Anmeldeinformationen des Benutzers. <p>Beachten Sie Folgendes über TLS:</p> <ul style="list-style-type: none"> Die Einstellung des CA Certificate (CA-Zertifikat) sollte auf das Server-Zertifikat auf dem lokalen Client verweisen. Wenn Ihre Datei für den Private Key (Privater Schlüssel) .p12 oder .pfx ist, kann die Einstellung User Certificate (Benutzerzertifikat) leer bleiben. Die Einstellung der Identity (Identität) sollte der Benutzername sein, der dem Benutzerzertifikat entspricht. Die Einstellung des Private Key Password (Privates Schlüsselkennwort) ist das Kennwort der privaten Schlüsseldatei des Benutzers.

Wireless-Netzwerkeinstellungen

Die folgende Tabelle beschreibt die im Network Manager unter der Registerkarte **Wireless** verfügbaren Optionen.



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

Option	Beschreibung
Scan AP (AP scannen)	Sucht nach verfügbaren Wireless-Netzwerken.
SSID	Verwenden Sie dieses Kontrollkästchen, um die SSID des Wireless-Netzwerks manuell einzugeben, wenn sie beim Scan nicht erkannt wurde.
SSID Hidden (SSID Ausgeblendet)	Aktivieren Sie diese Option, wenn die SSID des Wireless-Netzwerks auf Ausgeblendet eingestellt ist (nicht übermitteln).
Enable IPv6 (IPv6 aktivieren)	Aktiviert das IPv6. Standardmäßig wird IPv4 verwendet und es können nicht beide gleichzeitig verwendet werden.
Enable Power Management (Energieverwaltung aktivieren)	Aktiviert die Energieverwaltungsfunktion für den Wireless-Adapter.
Connection Method (Verbindungsmethode)	Zur Auswahl zwischen Automatic (Automatisch) und Static (Statisch). Wenn Ihre Netzwerkumgebung DHCP verwendet wird, sollte die Option Automatic (Automatisch) ohne weitere Konfigurationen funktionieren. Wenn Static (Statisch) ausgewählt ist, werden die Einstellungen für Static Address Configuration (Statische Adressenkonfiguration) zur Verfügung stehen. Vergewissern Sie sich, dass Sie diese Werte dem entsprechend eingeben, ob Sie IPv4 oder IPv6 verwenden.
Security Settings (Sicherheitseinstellungen)	Zum Festlegen der Authentifizierungseinstellung auf eine der folgenden Optionen: <ul style="list-style-type: none"> None (Keine)

Option	Beschreibung
	<ul style="list-style-type: none"> • WEP • WPA/WPA2-PSK • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS • EAP FAST <p>Für WEP und WPA/WPA2-PSK müssen Sie nur den Netzwerkschlüssel eingeben und auf OK klicken.</p> <p>Stellen Sie für EAP-FAST Anonymous Identity (Anonyme Identität), Username (Benutzername), Password (Kennwort) und Provisioning Method (Bereitstellungsmethode) ein. Die Einstellungen der PAC-Datei müssen Sie nicht ändern.</p> <p>Weitere Informationen über TTLS, PEAP und TLS finden Sie unter Drahtgebundene Netzwerkeinstellungen auf Seite 16.</p>

DNS-Einstellungen


Die folgende Tabelle beschreibt die im Network Manager 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 Servers (DNS-Server)	Verwenden Sie dieses Feld, um benutzerdefinierte Informationen des DNS-Servers festzulegen.
Search Domains (Domänen durchsuchen)	Verwenden Sie dieses Feld, um die Domänen zu beschränken, die durchsucht werden.
HTTP Proxy FTP Proxy HTTPs Proxy	<p>Verwenden Sie diese Felder, um Proxy-Server-Informationen im folgenden Format einzugeben:</p> <p><code>http://<ProxyServer>:<Port></code></p> <p>HP empfiehlt das Präfix <code>http://</code> für alle drei Proxy-Einstellungen zu verwenden, da es besser unterstützt wird.</p> <p>HINWEIS: Die Proxy-Einstellungen sind auf die Umgebungsvariablen <code>http_proxy</code>, <code>ftp_proxy</code> und <code>https_proxy</code> für das System eingestellt.</p>

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** (Quell-Adresse) ist die IP-Adresse des Thin Client und die Ziel-Adresse ist die IP-Adresse des Systems, mit dem der 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.

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 [Vergleich von ThinPro und Smart Zero auf Seite 1](#) 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
Launch the Connection Manager at start up (Beim Systemstart den Connection Manager starten)	Wenn aktiviert, wird HP Connection Manager beim Systemstart automatisch gestartet.
Enable/disable right click (Aktivieren/Deaktivieren der rechten Maustaste)	Deaktivieren Sie diese Option, um das Kontextmenü zu deaktivieren, das angezeigt wird, wenn Sie mit der rechten Maustaste auf den Desktop klicken.
Allow user to switch to admin mode (Benutzer erlauben in den Administratormodus zu wechseln)	Deaktivieren Sie diese Option, um die Option Administrator/User Mode Switch (Wechsel zwischen Administrator-/Benutzermodus) in der Systemsteuerung im Benutzermodus zu entfernen.
Enable X host access control security (X-Host-Zugriffskontroll-sicherheit aktivieren)	Wenn aktiviert, dürfen nur die Systeme, die im Bereich XHost Access Control List (X-Host-Zugriffskontrollliste) aufgeführt werden den Thin Client über Fernzugriff steuern.
Enable USB Update (USB-Update aktivieren)	Ermöglicht die Installation von Updates über ein USB-Flash-Laufwerk. Weitere Informationen finden Sie unter „ USB Updates “ auf Seite 75.
Authenticate USB Update (USB-Update authentifizieren)	Deaktivieren Sie diese Option, um Standardbenutzern die Installation von Updates über USB zu erlauben.

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

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


HP ThinState

HP ThinState ermöglicht Ihnen das Aufzeichnen und Bereitstellen eines HP ThinPro-Image oder die Konfiguration auf einem anderen 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, indem 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 the **HP ThinPro Image** aus, und klicken Sie auf **Next** (Weiter).

3. Wählen Sie **make a copy of the HP ThinPro image** (Eine Kopie von HP ThinPro Image erstellen) aus, und klicken Sie auf **Next** (Weiter).
4. Wählen Sie **a FTP server** (Einen FTP-Server) und klicken Sie dann auf **Next** (Weiter).
5. Geben Sie die FTP-Server-Informationen in die Felder ein.

 **HINWEIS:** Die Image-Datei wird standardmäßig nach dem Hostnamen des Clients 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. Klicken Sie auf **Finish** (Beenden).


Wenn die Image-Aufzeichnung beginnt, werden alle Anwendungen beendet und es erscheint ein neues Fenster, das den Fortschritt anzeigt. Wenn ein Problem auftritt, klicken Sie auf **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 Clients-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 the **HP ThinPro Image** aus, und klicken Sie auf **Next** (Weiter).
3. Wählen Sie **restore an HP ThinPro image** (Ein HP ThinPro Image wiederherstellen) aus, und klicken Sie auf **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. Klicken Sie auf **Finish** (Beenden).

Wenn die Image-Bereitstellung beginnt, werden alle Anwendungen beendet und es erscheint ein neues Fenster, das den Fortschritt anzeigt. Wenn ein Problem auftritt, klicken Sie auf **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. Schließen Sie ein USB-Flash-Laufwerk an einen USB-Anschluss am Client an.
2. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
3. Wählen Sie the **HP ThinPro Image** aus, und klicken Sie auf **Next** (Weiter).
4. Wählen Sie **make a copy of the HP ThinPro image** (Eine Kopie von HP ThinPro Image erstellen) aus, und klicken Sie auf **Next** (Weiter).
5. Wählen Sie **create a bootable USB flash drive** (Bootfähiges USB-Flash-Laufwerk erstellen) und klicken Sie dann auf **Next** (Weiter).
6. Wählen Sie das USB-Flash-Laufwerk und klicken Sie dann auf **Finish** (Beenden).


Wenn die Image-Aufzeichnung beginnt, werden alle Anwendungen beendet und es erscheint ein neues Fenster, das den Fortschritt anzeigt. Wenn ein Problem auftritt, klicken Sie auf **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 Clients-Flash-Laufwerks wird beschädigt.

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


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

Verwalten von HP ThinPro-Konfigurationen

Eine HP ThinPro-Konfigurationsdatei enthält die Verbindungen und Einstellungen, die mithilfe der Dienstprogramme der Systemsteuerung konfiguriert wurden. Eine Konfigurationsdatei ist nur für die Version des HP ThinPro geeignet, in der sie erstellt wurde.

Speichern einer HP ThinPro-Konfiguration auf einem FTP-Server

So speichern Sie eine HP ThinPro-Konfiguration auf einem FTP-Server:

 **WICHTIG:** Das Verzeichnis auf dem FTP-Server, indem 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 **HP ThinPro configuration** (HP ThinPro Konfiguration) aus, und klicken Sie auf **Next** (Weiter).
3. Wählen Sie **save the configuration** (Konfiguration speichern) aus, und klicken Sie auf **Next** (Weiter).
4. Wählen Sie **on a FTP server** (Auf einem FTP-Server) und klicken Sie dann auf **Next** (Weiter).

5. Geben Sie die FTP-Server-Informationen in die Felder ein.
6. Klicken Sie auf **Finish** (Beenden).

Wiederherstellen einer HP ThinPro-Konfiguration über FTP oder HTTP

So stellen Sie eine HP ThinPro-Konfiguration über FTP oder HTTP wieder her:

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie **HP ThinPro configuration** (HP ThinPro Konfiguration) aus, und klicken Sie auf **Next** (Weiter).
3. Wählen Sie **restore a configuration** (Eine Konfiguration wiederherstellen) aus, und klicken Sie auf **Next** (Weiter).
4. Wählen Sie **on a remote server** (Auf einem Remote-Server) und klicken Sie dann auf **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. Klicken Sie auf **Finish** (Beenden).

Speichern einer HP ThinPro-Konfiguration auf einem USB-Flash-Laufwerk

So speichern Sie eine HP ThinPro-Konfiguration auf einem USB-Flash-Laufwerk:

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

Wiederherstellen einer HP ThinPro-Konfiguration von einem USB-Flash-Laufwerk

So stellen Sie eine HP ThinPro-Konfiguration von einem USB-Flash-Laufwerk wieder her:

1. Schließen Sie das USB-Flash-Laufwerk, das die Konfigurationsdatei enthält, an einen USB-Anschluss am Ziel-Client an.
2. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).


3. Wählen Sie **HP ThinPro configuration** (HP ThinPro Konfiguration) aus, und klicken Sie auf **Next** (Weiter).
4. Wählen Sie **restore a configuration** (Eine Konfiguration wiederherstellen) aus, und klicken Sie auf **Next** (Weiter).
5. Wählen Sie **on a USB key** (Auf einem USB-Stick) und klicken Sie dann auf **Next** (Weiter).
6. Wählen Sie den USB-Stick aus.
7. Klicken Sie auf **Browse** (Durchsuchen).
8. Doppelklicken Sie auf die gewünschte Konfigurationsdatei auf dem USB-Stick.
9. Klicken Sie auf **Finish** (Beenden).

VNC-Shadowing

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

So greifen Sie auf das Dienstprogramm VNC Shadow zu:

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

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

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

Option	Beschreibung
Enable VNC Shadow (Systemstart von VNC aktivieren)	Ermöglicht das VNC-Shadowing.
VNC Read Only (VNC Schreibgeschützt)	Öffnet die VNC-Sitzung als schreibgeschützt.
VNC Use Password (Kennwort für VNC verwenden)	Macht bei Zugriff auf den Client über VNC ein Kennwort erforderlich. Klicken Sie auf Set Password (Kennwort festlegen), um das Kennwort festzulegen.
VNC Notify User to Allow Refuse (VNC-Benachrichtigung an Benutzer Zugriff zulassen/verweigern)	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 Show Timeout for Notification (VNC Zeitlimit für Benachrichtigung anzeigen)	Legt die Dauer in Sekunden, die das Benachrichtigungs-Dialogfeld angezeigt wird fest.
Benutzer-Benachrichtigung	Ermöglicht Ihnen, eine Nachricht im Dialogfeld für die Benachrichtigung an den Remote-Benutzer anzuzeigen.
Refuse connections in default (Verbindungen standardmäßig verweigern)	Wenn aktiviert, wird die VNC-Verbindung standardmäßig verweigert, sobald die Zeit abgelaufen ist.
Re-set VNC server right now (VNC-Server jetzt gleich zurücksetzen)	Setzt den VNC-Server zurück, nachdem die neuen Einstellungen angewendet wurden.

Zertifikate

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


Certificate Manager

So öffnen Sie den Certificate Manager:

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

Verwenden Sie den Certificate 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 den Profile Editor verwenden, um das Zertifikat einem Profil zuzuweisen, wie beschrieben unter [Zertifikate zu einem Client-Profil hinzufügen auf Seite 67](#).

 **HINWEIS:** Im Allgemeinen funktioniert ein selbst signiertes 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 des Clients und die Zertifikatsanforderung 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 Clients 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 Clients. 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 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 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 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 Client und auf dem DHCP-Server:

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

5 Gemeinsame Verbindungskonfigurationen

Dieses Kapitel behandelt Konfigurationen, die für alle Verbindungstypen gleich sind.

- [Gemeinsame Verbindungseinstellungen](#)
- [Kioskmodus](#)

Gemeinsame Verbindungseinstellungen

In der folgenden Tabelle werden die Einstellungen beschrieben, die auf der letzten Seite des Connection Manager-Assistenten für die einzelnen Verbindungstypen verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die Verbindung, die Sie derzeit konfigurieren.

Tabelle 5-1 Gemeinsame Verbindungseinstellungen

Option	Beschreibung
Fallback Connection (Ausweichverbindung)	Spezifiziert die Ausweichverbindung. Wenn die Verbindung nicht gestartet werden kann, versucht stattdessen die Ausweichverbindung zu starten. HINWEIS: Diese Option ist nicht verfügbar für den Verbindungstyp VMware Horizon View.
Auto Start priority (Autostart-Priorität)	Bestimmt die Reihenfolge, in der die Verbindungen automatisch gestartet werden. 0 bedeutet, dass die Autostartfunktion deaktiviert ist. Die anderen Werte bestimmen die Startreihenfolge, wobei 1 die höchste Priorität hat.
Share credentials with screensaver (Anmeldeinformationen für Bildschirmschoner freigeben)	Ermöglicht den Benutzern den lokalen Bildschirmschoner zu entsperren, indem sie ihre Anmeldeinformationen für diese Verbindung eingeben. HINWEIS: Diese Option ist nur für die Verbindungstypen Citrix, RDP und VMware Horizon View verfügbar.
Auto reconnect (Automatische Neuverbindung)	Wenn aktiviert, wird diese Verbindung automatisch versuchen die Verbindung wiederherzustellen, wenn sie unterbrochen wurde. HINWEIS: Das Beenden einer Verbindung über den HP Connection Manager wird eine automatische Neuverbindung verhindern.
Wait for network before connecting (Auf Netzwerk warten vor Verbindungsaufbau)	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.
Show icon on desktop (Symbol auf Desktop anzeigen)	Wenn aktiviert, wird für diese Verbindung ein Desktopsymbol erstellt.
Allow the user to launch this connection (Benutzer erlauben diese Verbindung zu starten)	Wenn aktiviert, kann diese Verbindung von einem Standardbenutzer gestartet werden.
Allow the user to edit this connection (Benutzer erlauben diese Verbindung zu bearbeiten)	Wenn aktiviert, kann diese Verbindung von einem Standardbenutzer geändert werden.

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 Anwendungen automatisch bei der Anmeldung startet, sodass der Kioskmodus praktisch nahtlos arbeitet.

Der einfachste Weg, einen Thin Client für den Kioskmodus zu konfigurieren, ist es ihn auf die Smart Zero-Konfiguration umzuschalten (siehe [Anpassungscenter auf Seite 19](#)) 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 eingestellt.

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

- Stellen Sie im Anpassungscenter die Taskleiste auf **Auto hide** (Automatisch ausblenden) ein.
- Gehen Sie im Connection Manager für die Verbindung wie folgt vor:
 - Setzen Sie die **Auto start priority** (Autostart-Priorität) auf **1**.
 - Aktivieren Sie **Auto reconnect** (Automatische Neuverbindung).
 - Falls verfügbar, aktivieren Sie **Share credentials with screensaver** (Anmeldeinformationen für Bildschirmschoner freigeben).
 - Wenn Sie nur eine Web Browser-Verbindung herstellen möchten, wählen Sie **Enable kiosk mode** (Kioskmodus aktivieren).
- Legen Sie bei Bedarf im USB Manager das richtige USB-Umleitungsprotokoll fest.

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

6 Citrix-Verbindungen

- [Funktionen der Citrix-Verbindungsverwaltung](#)
- [Citrix Receiver-Funktionen](#)
- [Citrix-Verbindung-Supportmatrix](#)
- [Citrix – Allgemeine Einstellungen](#)
- [Citrix – Verbindungsspezifische Einstellungen](#)

Funktionen der Citrix-Verbindungsverwaltung

Wenn Sie eine Citrix-Verbindung verwenden, können Sie den Client so konfigurieren, dass automatisch die folgenden Funktionen ausgeführt werden:

- Ressource starten, wenn nur eine einzige Ressource veröffentlicht wird
- Eine bestimmte Ressource starten
- Einen veröffentlichten Desktop starten
- Sitzungen beim Verbindungsstart erneut verbinden
- Die Verbindung nach einem angegebenen Zeitrahmen abmelden
- Veröffentlichte Ressourcen mithilfe der folgenden konfigurierbaren Abkürzungen starten:
 - Desktopsymbole
 - Startmenüsymbole
 - Taskleisten-Symbole

Citrix Receiver-Funktionen


Die Citrix Receiver-Funktionen umfassen Folgendes:

- Einstellungen für die Fenstergröße und -tiefe
- Nahtloser Fenstersupport
- Einstellungen für die Soundqualität
- Zuordnung von statischen Laufwerken
- Zuordnung von dynamischen Laufwerken
- USB-Umleitung für XenDesktop und VDI-in-a-Box




HINWEIS: Basierend auf internen Tests und Validierungen, hat HP festgestellt, dass eine Webcam, die über eine Citrix-Verbindung unter Verwendung einer einfachen USB-Umleitung verbunden ist, keine gute Leistung erbringt. HP empfiehlt, diese Konfiguration nicht zu verwenden und schlägt vor, dass Kunden, die diese Funktion benötigen, die Citrix HDX-Technologie ausprobieren, um ein zufriedenstellendes Leistungsniveau zu gewährleisten.


- Smart Card Virtual Channel-Aktivierung

 **HINWEIS:** Diese Funktion ist gleichbedeutend mit einer Smart Card Anmeldung/ Authentifizierung bei der Verwendung von direkten, nicht-PNAgent-Verbindungen. Bei einer PNAgent-Verbindung, aktiviert oder deaktiviert die Smart Card Virtual Channel-Aktivierung den Smart Card Virtual Channel, bietet jedoch keine anfängliche Verbindungsauthentifizierung. Für eine Smart Card-Authentifizierung für XenApp und XenDesktop verwenden Sie die bereitgestellte Internetbrowser-Verbindung anstelle der Citrix-Verbindung. Stellen Sie sicher, dass der Internetzugriff aktiviert ist.


- Druckerzuordnung
- Zuordnung des seriellen Anschlusses
- HDX MediaStream (hardwarebeschleunigt bei den meisten Modellen)

 **HINWEIS:** Weitere Informationen finden Sie unter [HDX MediaStream-Supportmatrix auf Seite 30](#).


- HDX Flash-Umleitung (nur x86)
- HDX Webcam-Komprimierung

 **HINWEIS:** HDX Webcam-Komprimierung funktioniert am besten mit x86-Einheiten. HP hat festgestellt, dass die Leistung der Webcams mit ARM-Einheiten schlecht ist und rät davon ab, ARM-Einheiten für die Webcam-Umleitung zu verwenden.

- HDX RealTime (MS Lync-Optimierung) (nur x86)

 **HINWEIS:** Dies ist nur auf Lync 2010 verfügbar.

- Authentifizierung bei Citrix Access Gateway 5.0 und NetScaler Gateway 9.x/10.x mit ICA Proxy-Modus

 **HINWEIS:** Nur Zertifikate vom Typ CA-issued, SHA-1 werden unterstützt. Selbstsignierte und SHA-2-Zertifikate werden nicht unterstützt.

HDX MediaStream-Supportmatrix


 **HINWEIS:** Bestimmte Videotypen funktionieren mit Low-End-Einheiten möglicherweise nicht einwandfrei. High-End-Einheiten werden für die HDX-Media-Umleitung empfohlen.

Tabelle 6-1 HDX MediaStream-Supportmatrix

Funktion	Support
Bildfrequenz	<ul style="list-style-type: none">• 24 FPS
Auflösung	<ul style="list-style-type: none">• 1080p• 720p
Video-Container	<ul style="list-style-type: none">• WMV• AVI• MPG• MPEG• MOV• MP4
Video-Codecs	<ul style="list-style-type: none">• WMV2

Tabelle 6-1 HDX MediaStream-Supportmatrix (Fortsetzung)

Funktion	Support
	<ul style="list-style-type: none"> • WMV3/VC-1 • H.264/AVC/MPEG-4 Teil 10 • MPEG-4 Teil 2 • H.263 • DivX • Xvid • MPEG1
Audio-Codecs	<ul style="list-style-type: none"> • MP3 • WMA • AAC • PCM • MPEG-Audio • MLAW/ULAW

Citrix-Verbindung-Supportmatrix

Die folgende Tabelle beschreibt die unterstützten Citrix-Backends.

Tabelle 6-2 Citrix-Verbindung-Supportmatrix

		Backend		
		XenApp	XenDesktop	VDI-in-a-Box
Zugriffstyp	Direkt (Betriebssystemunabhängig)	4.5/5/6/6.4		
	PNAgent (Vorgängerversion)	4.5 / 5 / 6 / 6.5 / 7.X	4.5 / 5.5 / 5.6.5 / 7.X	5.x
	Internetbrowser	4.5 / 5 / 6 / 6.5 / 7.X	4.5 / 5.5 / 5.6.5 / 7.X	5.x
	StoreFront	4.5 / 5 / 6 / 6.5 / 7.X	4.5 / 5.5 / 5.6.5 / 7.X	5.x

Citrix – Allgemeine Einstellungen

Die folgenden Tabellen beschreiben die Einstellungen, die im XEN Connection General Settings Manager verfügbar sind. Diese Einstellungen sind universal und gelten für alle Citrix-Verbindungen.



HINWEIS: Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 6-3 XEN Connection General Settings Manager > Options (Optionen)

Option	Beschreibung
Enable HDX MediaStream (HDX MediaStream aktivieren)	Wann immer möglich, aktiviert HDX MediaStream die Verarbeitungsleistung des Thin Clients, um den multimedialen Inhalt wiederzugeben. Vom Datenzentrum aus wird die komprimierte multimediale Information in ihrem ursprünglichen Format direkt zum Thin Client gesendet. Der Vorgang wird je nach Verarbeitungsleistung und der multimedialen Kapazität des Thin Clients variieren.
Enable Windows Alert Sound (Windows Signalton aktivieren)	Aktiviert akustische Windows-Signale.
ICA Acceleration (LAN Only) (ICA-Beschleunigung (nur LAN))	Aktiviert die ICA-Beschleunigung.
Disable Info Box Before Connecting (Vor Verbinden Infofeld deaktivieren)	Die Informationsbox wird erst nach dem Verbindungsaufbau angezeigt.
Use Asynchronous COM-port Polling (Asynchrone COM-Port-Abfrage verwenden)	Aktiviert die asynchrone Abfrage des COM-Anschlusses.
Allow Smart Card Logon (Smart Card Anmeldung zulassen)	Ermöglicht die Authentifizierung über eine an den Client angeschlossene SmartCard bei der Anmeldung.
Enable Off Screen Surface (Off-Screen-Oberfläche aktivieren)	Weist den ICA-Client an, Bildschirmaktualisierungen in eine speicherinterne Bitmap anstatt auf dem Bildschirm zu schreiben, um die Bandbreiteneffizienz zu verbessern.
Enable Session Reuse (Session-Wiederverwendung aktivieren)	Ermöglicht die Wiederverwendung von Sitzungen.
Enable Auto Reconnect (Automatische Neuverbindung aktivieren)	Ermöglicht eine automatische Verbindungswiederholung für Verbindungen, die getrennt wurden.
Enable UseLocalIM (UseLocalIM aktivieren)	Verwendet die lokale Eingabemethode, um die Tastatureingabe zu interpretieren. Das wird nur für europäische Sprachen unterstützt.
Use EUKS Number (EUKS-Nummer verwenden)	Kontrolliert die Verwendung des Extended Unicode Keyboard Supports auf Windows-Servern: 0=kein EUKS 1=EUKS verwendet als Ausweidlösung 2=EUKS wann immer möglich verwenden
Minimum Bitmap Cache Size (Minimale Bitmapcache-Größe)	Minimiert die Größe des Bitmap-Cache.
Use Data Compression (Datenkomprimierung verwenden)	Aktiviert die Datenkomprimierung für diese Verbindung.
Enable Middle Button Paste (Einfügen mit mittlerer Taste aktivieren)	Bietet die Möglichkeit, durch Klicken der mittleren Maustaste Daten aus der Zwischenablage einzufügen.
Use Disk Cache for Bitmap (Disk-Cache für Bitmap verwenden)	Aktiviert die Zwischenspeicherung von Verbindungsbitmaps auf dem Datenträger.
HDX Flash Redirection (HDX Flash-Umleitung)	Aktiviert die HDX Flash-Umleitung, um Flash-Inhalte lokal abzuspielen.
HDX Flash Server Side Content Fetch (Serverseitiges Abrufen der HDX Flash-Inhalte)	Ermöglicht dem Server, die Flash-Inhalte zur Umleitung einzuholen.
Webcam/Headset Optimizations (Webcam-/Headset-Optimierungen)	Verwendet High-Level Webcam-/Headset-Umleitung.

Tabelle 6-3 XEN Connection General Settings Manager > Options (Optionen) (Fortsetzung)

Option	Beschreibung
Sound	Gibt die zu verwendende Audioqualität an. Gültige Optionen sind: High Quality (Hohe Qualität), Med Quality (Mittlere Qualität) und Low Quality (Niedrige Qualität).
Speed Screen	Gültige Optionen sind: Auto , On (Ein) und Off (Aus).
Mouse Click Feedback (Mausklick-Feedback)	Gültige Optionen sind: Auto , On (Ein) und Off (Aus).
Local Text Echo (Lokales Textecho)	Steuert die Tastatur-Latenzreduktion. Die empfohlene Einstellung ist Auto (Automatisch).
Encryption Level (Verschlüsselungsstufe)	Gibt die Verschlüsselungsstufe einer ICA-Sitzung an.
Monitor Network Connectivity (Netzwerkonnktivität überwachen)	Geht zurück zur lokalen GUI, wenn die Netzwerkverbindung abbricht.

Tabelle 6-4 XEN Connection General Settings Manager > Local Resources (Lokale Ressourcen)

Option	Beschreibung
Allow Audio Input (Audio-Eingabe zulassen)	Ermöglicht die Audioeingabe über den Thin Client.
Auto Printer Creation (Automatische Druckererstellung)	Ermöglicht die automatische Druckerkonfiguration.
Enable Dynamic Drive Mapping (Dynamische Laufwerkszuordnung aktivieren)	Ordnet USB-Geräte, die während der Sitzung angeschlossen werden automatisch zu.
Enable Static Drive Mapping (Legacy) (Statische Laufwerkszuordnung (Vorgängerversion) aktivieren)	Bietet die Möglichkeit, lokalen Pfaden Laufwerke zuzuordnen.

Tabelle 6-5 XEN Connection General Settings Manager > Window (Fenster)

Option	Beschreibung
Enable Seamless Window (Nahtloses Fenster aktivieren)	Ermöglicht die Anzeige eines einzelnen Fensters auf dem lokalen ThinPro-Desktop wie bei einer nativen Anwendung.
Default Window Size (Standard-Fenstergröße)	Ermöglicht die Festlegung der Standardfenstergröße. Verfügbare Optionen: Full Screen (Vollbild), Fixed Size (Feste Größe), Percentage of Screen Size (Prozentuale Angabe der Fenstergröße).
Default Window Colors (Standard-Fensterfarben)	Ermöglicht die Festlegung der Standardfarbtiefe. Verfügbare Optionen: 16 , 256 , 16-Bit , 24-Bit , Auto .
Default 256 Color Mapping (Standardzuordnung 256 Farben)	Diese Option ist nur aktiviert, wenn Default Window Colors (Standardfarbtiefe) auf 256 eingestellt ist. Verfügbare Optionen: Shared - Approximate Colors (Gemeinsam - Angenäherte Farben) und Private - Exact Colors (Privat - Exakte Farben).

Tabelle 6-6 XEN Connection General Settings Manager > Firewall

Option	Beschreibung
Proxy Type (Proxytyp)	Verfügbare Optionen: None - direct (Kein - direkt), SOCKS , Secure - HTTPS (Sicher - HTTPS), Use browser settings (Browsereinstellungen)

Tabelle 6-6 XEN Connection General Settings Manager > Firewall (Fortsetzung)

Option	Beschreibung
	verwenden), Automatically detect proxy (Proxy automatisch erkennen).
Proxy Address (Proxyadresse)	Die IP-Adresse des Proxy-Servers.
Proxy Port (Proxy-Port)	Der Port für die Verbindung zum Proxy-Server.
Username (Benutzername)	Der Benutzername für die Verbindung zum Proxy-Server.
Password (Kennwort)	Das Kennwort für die Verbindung zum Proxy-Server.
Use Alternate Address for Firewall Connection (Alternative Adresse für Firewallverbindung 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.

Tabelle 6-7 XEN Connection General Settings Manager > Keyboard Shortcuts (Tastenkombinationen)

Option	Beschreibung
Handling of keyboard shortcuts (Verwendung von Tastenkombinationen)	Gibt an, wie Funktionstasten bedient werden sollen. Verfügbare Optionen: Translated (Übersetzt), Direct in full screen desktops only (Direkt nur in Vollbild-Desktops) und Direct (Direkt).
Stop Direct key handling (Verwendung von Direkttasten stoppen)	Diese Option ist nicht aktiviert, wenn die Option Handling of keyboard shortcuts (Verwendung von Tastaturkurzbefehlen) auf Translated (Übersetzt) eingestellt ist.
<List of keyboard shortcuts> (Liste der Tastenkombinationen)	Diese Option ist nur aktiviert, wenn Handling of keyboard shortcuts (Verwendung von Tastaturkurzbefehlen) auf Translated (Übersetzt) oder Direct in full screen desktops only (Direkt - Nur in Vollbild-Desktops) eingestellt ist.

Tabelle 6-8 XEN Connection General Settings Manager > Session (Sitzung)

Option	Beschreibung
Auto Logout Delay Before App Launch (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.
Auto Logout Delay After App Close (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.
Auto Logout Delay with Single App (Automatische Abmeldungsverzögerung bei einzigen Anwendung)	Wenn Sie einen Citrix-Server mit einer einzigen veröffentlichten Ressource verwenden, wird mit dieser Option die Anzahl der Sekunden festgelegt, die zur Verfügung steht zwischen dem Schließen der von Xen veröffentlichten Ressource und der automatischen Abmeldung des Benutzers und Zurückkehren zum Anmeldebildschirm.

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

Tabelle 6-8 XEN Connection General Settings Manager > Session (Sitzung) (Fortsetzung)

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

Citrix – Verbindungsspezifische Einstellungen

Die folgende Tabelle beschreibt die Einstellungen, die im Citrix Connection Manager verfügbar sind. Diese Einstellungen sind verbindungs-spezifisch und gelten nur für die Citrix-Verbindung, die Sie derzeit konfigurieren.



 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 6-9 Citrix Connection Manager > Seite 1

Option	Beschreibung
Name	Der Verbindungsname.
Server URL	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.
Storefront Connection (StoreFront-Verbindung)	Zeigt an, dass dies eine Verbindung zum neuen StoreFront-Verbindungsservice von Citrix ist.
Username (Benutzername)	Der für die Verbindung zu verwendende Benutzername.
Password (Kennwort)	Das Kennwort, das für die Verbindung verwendet werden soll.
Domain (Domäne)	Die Domäne, die für die Verbindung verwendet werden soll.
Auto Start Resource (Autostart-Ressource)	Der Name einer Autostart-Ressource.
Auto Start Desktop (Autostart-Desktop)	Startet automatisch eine Ressource vom Typ Desktop, wenn diese vorhanden ist.
Show applications on desktop (Anwendungen auf Desktop anzeigen)	Zeigt Remote-Ressourcen auf dem lokalen Desktop an.

 **HINWEIS:** Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des Citrix Connection Manager.

7 RDP-Verbindungen

- [RPD-Funktionen](#)
- [RDP – Allgemeine Einstellungen](#)
- [RDP – Verbindungsspezifische Einstellungen](#)
- [Verwenden von RemoteFX mit RDP](#)
- [Verwenden von Multi-Monitor-Sitzungen mit RDP](#)
- [Verwenden der Multimedia-Umleitung mit RDP](#)
- [Verwenden der Geräteumleitung mit RDP](#)

RPD-Funktionen

Der RDP-Client basiert auf FreeRDP 1.1 und erfüllt die folgenden Anforderungen für RDP 7.1:

- Hardware-beschleunigtes RemoteFX
- MMR wird unterstützt, wenn eine Verbindung zu Windows-Hosts hergestellt wird und die Desktop Experience-Funktion aktiviert ist (Windows 7 oder Windows Server 2008 R2)
- USBR wird unterstützt, wenn eine Verbindung zu virtuellen Windows 7-Remotedesktophosts hergestellt wird
- Bidirektionales Audio
- Echter Multi-Monitor-Support

RDP – Allgemeine Einstellungen

Die folgende Tabelle beschreibt die Einstellungen, die im RDP7 Connection General Settings Manager verfügbar sind. Diese Einstellungen sind universal und gelten für alle RDP-Verbindungen.


 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 7-1 RDP7 Connection General Settings Manager

Option	Beschreibung
Send hostname as (Hostnamen senden als)	Gibt an, ob der Hostname des Clients oder die MAC-Adresse als der angegebene Hostname an das Remote-System gesendet werden soll.
Enable Multimedia Redirection (Multimedia-Umleitung aktivieren)	Aktiviert die Multimedia-Umleitung.

RDP – Verbindungsspezifische Einstellungen

Die folgenden Tabellen beschreiben die Einstellungen, die im RDP7 Connection Manager verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die RDP-Verbindung, die Sie derzeit konfigurieren.



HINWEIS: Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 7-2 RDP7 Connection Manager > Seite 1

Option	Beschreibung
Name	Ein benutzerdefinierter Name für diese Verbindung
Address (Adresse)	Die IP-Adresse oder der Servername für diese Verbindung
Port	Der Verbindungsport (standardmäßig 3389)
Username (Benutzername)	Der Benutzername für diese Verbindung
Password (Kennwort)	Das Kennwort für diese Verbindung
Domain (Domäne)	Der Domänenname für diese Verbindung (optional)
Allow Smartcard Login (Smart Card-Anmeldung zulassen)	Ermöglicht die Smart Card-Authentifizierung
Enable RD Gateway (RD-Gateway aktivieren)	Ermöglicht zusätzliche RD-Gateway-Optionen, wie Gateway-Adresse, -Port und -Anmeldeinformationen)

Tabelle 7-3 RDP7 Connection Manager > Seite 2

Option	Modi	Beschreibung
Hide Window Decoration (Fensterdekoration ausblenden)	Standard Desktop	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.
Window Size (Fenstergröße)	Standard Desktop Alternate Shell (Andere Shell)	Legt die Fenstergröße auf full (voll), fixed (fest) oder percent (prozentual) fest.
Percentage Size (Prozentuale Größe)	Standard Desktop Alternate Shell (Andere Shell)	Wenn Window Size (Fenstergröße) auf percent (prozentual) eingestellt ist, legt diese Option den Prozentsatz fest, den ein Desktopfenster auf dem Bildschirm einnimmt. HINWEIS: Die daraus resultierende Größen können gerundet werden. HINWEIS: RemoteFX unterstützt nur eine feste Liste von Auflösungen.
Fixed Size (Feste Größe)	Standard Desktop Alternate Shell (Andere Shell)	Wenn Window Size (Fenstergröße) auf fixed (fest) eingestellt ist, legt diese Option die Breite und Höhe, die das Desktopfenster einnimmt, in Pixeln fest.
Application (Anwendung)	Remote Application (Remote-Anwendung)	Gibt den Pfad an, auf dem die Anwendung ausgeführt wird. Wenn Sie den Modus RDP Seamless Windows (RPD Nahtlose Fenster) verwenden, geben Sie den Pfad der

Tabelle 7-3 RDP7 Connection Manager > Seite 2 (Fortsetzung)

Option	Modi	Beschreibung
		<p>seamlessrdpshell.exe 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>
Command (Befehl)	Alternate Shell (Andere Shell)	Gibt die Anwendung an, die im Modus Alternate Shell (Andere Shell) ausgeführt wird. Geben Sie den Befehl ein, der die Anwendung ausführt. Um Microsoft Word auszuführen, geben Sie z. B. <code>Word.exe</code> ein.
Directory (Verzeichnis)	Alternate Shell (Andere Shell)	Geben Sie den Arbeitsverzeichnispfad des Servers für die Programmdateien der Anwendung ein. Beispiel: Das Arbeitsverzeichnis für Microsoft Word ist <code>C:\Program Files\Microsoft</code> .

Tabelle 7-4 RDP7 Connection Manager > Seite 3

Option	Beschreibung
Enable motion events (Bewegungsereignisse aktivieren)	Wenn aktiviert, werden die Mausebewegungen beständig an den RDP-Server übermittelt.
Enable data compression (Datenkomprimierung aktivieren)	Ermöglicht die Massenkompromierung von Daten zwischen dem RDP-Server und dem Client.
Enable deprecated RDP encryption (Veraltete RDP-Verschlüsselung aktivieren)	Aktiviert die RDP-Verschlüsselung der letzten Generation, wenn NLA nicht verfügbar ist.
Enable certificate check (Zertifikatsüberprüfung aktivieren)	Wenn aktiviert, wird die Gültigkeit der Identität und des Zertifikats des RDP-Servers überprüft.
Enable offscreen cache (Offscreen-Cache aktivieren)	Wenn aktiviert, wird der Offscreen-Speicher verwendet, um Bitmaps zu cachen.
Attach to admin console (An Administratorkonsole anheften)	Fügt die Verbindung zum Administrator-Konsolenanschluss hinzu.
Cross-session copy/paste (Sitzungsübergreifendes Kopieren/Einfügen)	Wenn aktiviert, ist das Kopieren und Einfügen zwischen verschiedenen RDP-Sitzungen möglich.
Hostname to send (Hostname für Sendevorgang)	Normalerweise wird der Client-Hostname für Client-Zugriffslizenzen verwendet. Dieses Feld erlaubt das Senden eines anderen Werts.

Tabelle 7-5 RDP7 Connection Manager > Seite 4

Option	Beschreibung
Audio Devices (Audiogeräte)	Gibt an, ob die Audiogeräte über High-Level RDP-Audioumleitung oder Low-Level USB-Umleitung umgeleitet werden oder für diese Verbindung deaktiviert sind.
Printers (Drucker)	Gibt an, ob die Drucker über eine High-Level Druckerumleitung (für die eine Einrichtung über das Dienstprogramm Drucker in der Systemsteuerung erforderlich ist) oder über eine Low-Level USB-Umleitung umgeleitet werden oder für diese Verbindung deaktiviert sind.

Tabelle 7-5 RDP7 Connection Manager > Seite 4 (Fortsetzung)

Option	Beschreibung
Serial/Parallel Ports (Serielle/Parallele Ports)	Gibt an, ob die seriellen und parallelen Ports umgeleitet werden oder für diese Verbindung deaktiviert sind.
USB Storage (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.
Local Partitions (Lokale Partitionen)	Gibt an, ob lokale Partitionen des Thin Client Flash-Laufwerks umgeleitet werden oder für diese Verbindung deaktiviert sind.
Other USB Devices (Sonstige 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.

Tabelle 7-6 RDP7 Connection Manager > Seite 5

Option	Beschreibung
Choose your connection speed to optimize performance (Auswahl der Verbindungsgeschwindigkeit zur Optimierung der Leistung)	<p>Das Auswählen einer Verbindungsgeschwindigkeit (LAN, Broadband (Breitband) oder Modem) wird die folgenden Optionen aktivieren oder deaktivieren, um die Leistung zu optimieren:</p> <ul style="list-style-type: none"> • Desktop background (Desktop-Hintergrund) • Font smoothing (Schriftglättung) • Desktop composition (Desktopgestaltung) • Show contents of window while dragging (Inhalte des Fensters beim Verschieben anzeigen) • Menu and window animation (Menü- und Fensteranimation) • Themes (Designs) <p>Die Auswahl von Client Preferred Settings (Vom Client bevorzugte Einstellungen) ermöglicht dem Client die Auswahl der Optionen, die zur besten RPD-Erfahrung führen.</p> <p>Sie können auch Ihre eigene benutzerdefinierte Kombination von Optionen auswählen.</p>
Warning Timeout (Warnungs-Zeitlimit)	<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>TIPP: HP empfiehlt, den Wert des Zeitlimits für Netzwerke, die regelmäßig hoch belastet oder zeitweise überlastet sind bzw. ausfallen, zu erhöhen.</p>
Recovery Timeout (Zeitlimit für Wiederherstellung)	Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der Client auf die Wiederherstellung der Verbindung wartet, bevor eine bestimmte Maßnahme eingeleitet wird. Am Ende dieser Frist versucht der Client kurz erneut eine Verbindung mit der Sitzung aufzubauen.
Error Timeout (Fehler-Zeitlimit)	Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der Client wartet, bevor er aufhört zu versuchen die Verbindung mit diesem Server wiederherzustellen.



HINWEIS: Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen über die verfügbaren Einstellungen auf der letzten Seite des RDP7 Connection Manager.


Verwenden von RemoteFX mit RDP


RemoteFX (RFX) ist ein erweitertes Grafikanzeigeprotokoll, das dazu entwickelt wurde, die Grafikkomponente herkömmlicher RDP-Protokolle zu ersetzen. Es nutzt die Hardwarebeschleunigungsfähigkeiten der Server-GPU zur Codierung der Bildschirm Inhalte über das RFX-Codec und um Bildschirmaktualisierungen an den Client zu senden. RFX verwendet erweiterte Pipelining-Technologien und adaptive Grafiken, um sicherzustellen, dass die bestmögliche Erfahrung basierend auf dem Inhaltstyp, der CPU und der Verfügbarkeit der Netzwerkbandbreite und der Darstellungsgeschwindigkeit geliefert wird.

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

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

- `root/ConnectionType/freerdp/connections/{UUID}/remoteFx`

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

 **HINWEIS:** Einige Windows RDP-Server senden keine RemoteFX-Inhalte an Clients, die für RDP 7.1 aktiviert sind, ohne eine Änderung der Gruppenrichtlinien. Überprüfen Sie die Einstellung für die folgende Richtlinie:


Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment > Enable RemoteFX encoding for RemoteFX clients designed for Windows Server 2008 R2 SP1 (Lokale Computer-Richtlinie > Computer-Konfiguration > Administratorvorlagen > Windows-Komponenten > Remote Desktop Services > Remote Desktop-Sitzung Host > Remote-Sitzung Umgebung > RemoteFX-Kodierung aktivieren für RemoteFX-Clients, die speziell für Windows Server 2008 R2 SP1 ausgerichtet sind)


Verwenden von Multi-Monitor-Sitzungen mit RDP

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

Standardmäßig sind alle RDP-Sitzungen Vollbildsitzungen und decken alle Monitore ab, um die Virtualisierungserfahrung zu verbessern. Zusätzliche Fensteroptionen stehen im RDP7 Connection Manager zur Verfügung.

 **HINWEIS:** Wenn RFX verwendet wird, wird nur die Bildschirmauflösung 1280x768 unterstützt. Dies führt zu kleinen schwarzen Balken auf den Seiten der Verbindung.

 **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.

Verwenden der Multimedia-Umleitung mit RDP

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 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. Ein 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 darüber Aufschluss gibt, ob der Client den vom Remote-Host angeforderten Codec unterstützt, bevor versucht wird, ihn umzuleiten. Das Ergebnis ist, dass nur unterstützte Codecs umgeleitet werden, und alle nicht unterstützten Codecs für die serverseitige Darstellung zurückbleiben.

Um MMR auf dem Client für alle RDP-Verbindungen zu deaktivieren, setzen Sie den Wert des folgenden Registrierungsschlüsselwerts auf 0:

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

Da RemoteFX bereits akzeptable Multimedia-Leistung bietet, können Sie MMR mit RFX 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.

Verwenden der Geräteumleitung mit RDP

Die Geräteumleitung stellt sicher, dass beim Anschließen eines Gerätes am Client dieses Gerät automatisch erkannt wird und dass in der Remotesitzung darauf zugegriffen werden kann. RDP unterstützt die Umleitung von vielen verschiedene Arten von Geräten.

Verwenden einer USB-Umleitung mit RDP

Die USB-Umleitung erfolgt durch Übermittlung von Low-Level-USB-Protokoll-Anrufen über das Netzwerk an den Remote-Host. Alle am lokalen Host angeschlossenen USB-Geräte werden innerhalb des Remote-Hosts als native USB-Geräte angezeigt, als wären sie lokal angeschlossen. Standard-Windows-Treiber unterstützen das Gerät in der Remotesitzung, und alle Gerätetypen werden unterstützt, ohne dass zusätzliche Treiber auf dem 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 Remote-Sitzung erwartet, dass die Eingabe vom Client kommt. Einige Geräte wie z. B. Massenspeicher, Drucker und Audiogeräte verwenden möglicherweise zusätzliche Optionen für die Umleitung.

Beachten Sie die folgende zusätzliche Informationen über die USB-Umleitung mit RDP:

- Der Server muss die USB-Umleitung unterstützen, um für den 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 eingestellt werden.
- Für RDP-Verbindungen legen die Steuerungen im USB-Manager fest, ob ein USB-Gerät umgeleitet wird. Die Einstellungen für die einzelnen Verbindung bestimmen, wie ein USB-Gerät umgeleitet wird.

Verwenden der Massenspeicherumleitung mit RDP

Standardmäßig leitet die RDP-Sitzung alle Massenspeichergeräte an den Remote-Host weiter und verwendet dabei eine Laufwerksumleitung höchster Ebene. Wenn ein Gerät wie ein USB-Flash-Laufwerk, ein USB-DVD-ROM-Laufwerk oder eine externe USB-Festplatte am System angeschlossen wird, erkennt der Client diese Geräte und stellt diese im lokalen Dateisystem bereit. RDP erkennt dann ein bereitgestelltes Laufwerk und leitet es zum Remote-Host um. Innerhalb des Remote-Host erscheint es als neue Festplatte im Windows-Explorer und erhält den Namen `<device label> on <client hostname>`; beispielsweise `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 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.

Tabelle 7-7 USB-Umleitung deaktivieren

Registrierungseintrag	Einzurichtender Wert	Beschreibung
root/USB/root/holdProtocolStatic	1	Stellen Sie sicher, dass der USBR-Typ nicht automatisch geändert wird, wenn eine Verbindung festgelegt oder deren Festlegung aufgehoben wird.
root/USB/root/protocol	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 die Umleitung von USB-Massenspeichergeräten zu deaktivieren, jedoch andere Geräte zur Umleitung zuzulassen, löschen Sie im Client-Dateisystem die udev-Regel `/etc/udev/rules.d/010_USBDRIVE.Regeln`.

Verwenden der Druckerumleitung mit RDP

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 redirection** (High-Level-Umleitung) – Wenn entweder keine USB-Umleitung verfügbar auf dem Remote-Host ist oder 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 wird automatisch einen Remote-Drucker einrichten, der Druckspoolingbefehle über einen virtuellen Kanal vom Remote-Host an den Client sendet.

Diese Methode setzt voraus, dass der Drucker auf dem Client konfiguriert und ein Treiber auf dem Client angegeben wurde, da der RDP-Client an den Remote-Host weitergeben muss, welcher Treiber für den Remote-Drucker verwendet werden soll. Dieser Windows-Treiber muss mit dem Treiber übereinstimmen, den der Drucker bei einem lokalen Anschluss an ein Windows-Betriebssystem verwenden würde. Diese Informationen finden Sie normalerweise unter **Modell** (Modell) in den Druckereigenschaften.

 **HINWEIS:** Weitere Informationen finden Sie unter [Konfigurieren eines seriellen oder parallelen Druckers auf Seite 68](#).

Audioumleitung mit RDP verwenden

Standardmäßig wird die High-Level-Audioumleitung Audio vom Remote-Host an den Client umleiten. Es muss möglicherweise eine grundlegende Sprachsteuerung eingerichtet werden und RDP 7.1 enthält eine Anzahl von erweiterten Audioumleitungsfunktionen, die zusätzliche Konfigurationen erfordern.

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 Client angepasst werden. Die Einstellungen älterer Windows RDP-Server müssen geändert werden, um einen Audioeingang zu aktivieren.
- Sowohl die lokalen wie die Remote-Lautstärkeeinstellungen haben Auswirkungen auf die endgültige Lautstärke. HP empfiehlt, die lokale Lautstärke auf das Maximum einzustellen und die Lautstärke innerhalb des Remote-Host anzupassen.

Smart Card-Umleitung mit RDP verwenden

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 im RDP7 Connection Manager **Allow Smartcard Login** (Smart Card-Anmeldung erlauben).

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

Diese Technologie erfordert, dass Treiber für das Smart Card-Lesegerät auf dem Client installiert werden. Standardmäßig werden die CCID-und Gemalto-Treiber installiert, die Unterstützung für die Mehrheit der Smart Card-Lesegeräte hinzufügen. Zusätzliche Treiber können durch Hinzufügen zu `/usr/lib/pkcs11/` installiert werden.



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

8 VMware Horizon View-Verbindungen

- [VMware Horizon View-Einstellungen](#)
- [Verwenden von Multi-Monitor Sitzungen mit VMware Horizon View](#)
- [Verwenden von Tastaturkürzeln mit VMware Horizon View](#)
- [Verwenden der Multimedia-Umleitung mit VMware Horizon View](#)
- [Geräte-Umleitung mit VMware Horizon View verwenden](#)
- [Ändern des VMware Horizon View Protokolltyps](#)
- [Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung](#)
- [VMware Horizon View-USB-Gerätfamilien](#)

VMware Horizon View-Einstellungen

Die folgenden Tabellen beschreiben die Einstellungen, die im VMware Horizon View Connection Manager verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die VMware Horizon View-Verbindung, die Sie derzeit konfigurieren.



HINWEIS: Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 8-1 VMware Horizon View Connection Manager > Seite 1

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

Tabelle 8-2 VMware Horizon View Connection Manager > Seite 2

Option	Beschreibung
Automatic login (Automatische Anmeldung)	Wenn aktiviert, wird der Benutzer automatisch angemeldet, wenn die Verbindung hergestellt ist. HINWEIS: HP empfiehlt das Aktivieren dieser Option.
Allow Smartcard login (Smart Card-Anmeldung zulassen)	Aktiviert die Smart Card-Anmeldung. HINWEIS: Weitere Informationen zu Smart Cards finden Sie unter Smart Card-Umleitung mit VMware Horizon View verwenden auf Seite 50 .

Tabelle 8-2 VMware Horizon View Connection Manager > Seite 2 (Fortsetzung)

Option	Beschreibung
Nach Verbindungsunterbrechung schließen	<p>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.</p> <p>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.</p> <p>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.</p>
Hide top Menu bar (Obere Menüleiste ausblenden)	<p>Macht die obere Menüleiste für Benutzer unsichtbar.</p> <p>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.</p>
Connection Security Levels (Verbindungs-Sicherheitsstufen)	<p>Verwenden Sie die Connection Security Level (Sicherheitsstufe Verbindung) zum Einstellen der Sicherheitsstufe, die der VMware Horizon View-Client bei der Verbindung zum Server verwendet.</p> <p>HINWEIS: Nähere Informationen über das Verhalten von Verbindungs-Sicherheitsstufen finden Sie unter Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung auf Seite 51.</p>
Befehlszeilenargumente	<p>Geben Sie alle gewünschten Befehlszeilenargumente ein, die für die Verbindung verwendet werden sollen.</p> <p>Führen Sie eine der folgenden Optionen aus, um weitere Hilfe zur Verwendung von erweiterten Befehlszeilenargumenten zu erhalten:</p> <ul style="list-style-type: none">• Geben Sie in der Befehlszeile <code>vmware-view--help</code> ein.• Siehe die Linux Horizon View-Client-Dokumentation von VMware unter http://www.vmware.com. <p>HINWEIS: Diese Option gilt nicht für den Teradici-beschleunigten PCoIP Client.</p>

Tabelle 8-3 VMware Horizon View Connection Manager > Seite 3

Option	Beschreibung
Enable motion events (Bewegungseignisse aktivieren)	Aktiviert das Senden von Bewegungen für diese Verbindung.
Enable data compression (Datenkomprimierung aktivieren)	Aktiviert die Datenkomprimierung für diese Verbindung.
Enable encryption (Verschlüsselung aktivieren)	Aktiviert die Verschlüsselung für diese Verbindung.
Enable offscreen cache (Offscreen-Cache aktivieren)	Wenn aktiviert, wird der Offscreen-Speicher verwendet, um Bitmaps zu cachen.
Attach to admin console (An Administratorkonsole anheften)	Fügt die Verbindung zum Administrator-Konsolenanschluss hinzu.
Hostname to send (Hostname für Sendevorgang)	Sendet den Hostnamen zum Remote-System für diese Verbindung.

Tabelle 8-3 VMware Horizon View Connection Manager > Seite 3 (Fortsetzung)

Option	Beschreibung
Remote computer sound (Sounds auf dem Remotecomputer)	Gibt an, wo der Remotecomputer-Sound wiedergegeben werden sollte (remote oder lokal), oder ob er überhaupt nicht wiedergegeben werden sollte.
Enable port mapping (Portzuweisung aktivieren)	Ordnet der Remotesitzung die seriellen und parallelen Schnittstellen des Clients zu.
Enable printer mapping (Druckerzuweisung aktivieren)	<p>Ordnet der Remotesitzung die lokale Druckwarteschlange zu. Verwenden Sie diese Option, wenn die USB-Umleitung entweder auf dem Remote-Host nicht verfügbar ist oder es sich bei dem Drucker um einen parallelen oder seriellen Drucker handelt. Konfigurieren Sie den Drucker für die Verwendung eines lokalen Druckerspoolers und der RDP-Client wird automatisch einen Remote-Drucker einrichten, der Druckspoolingbefehle über einen virtuellen Kanal vom Remote-Host an den Client sendet.</p> <p>Diese Methode setzt voraus, dass der Drucker auf dem Client konfiguriert und ein Treiber auf dem Client angegeben wurde, da der RDP-Client an den Remote-Host weitergeben muss, welcher Treiber für den Remote-Drucker verwendet werden soll. Dieser Windows-Treiber muss mit dem Treiber übereinstimmen, den der Drucker bei einem lokalen Anschluss an ein Windows-Betriebssystem verwenden würde. Diese Informationen finden Sie normalerweise unter Model (Modell) in den Druckereigenschaften.</p>

Tabelle 8-4 VMware Horizon View Connection Manager > Seite 4

Option	Beschreibung
Enable MMR (MMR aktivieren)	Aktiviert die Multimedia-Umleitung.
Choose your connection speed to optimize performance (Auswahl der Verbindungsgeschwindigkeit zur Optimierung der Leistung)	<p>Das Auswählen einer Verbindungsgeschwindigkeit (LAN, Broadband (Breitband) oder Modem) wird die folgenden Optionen aktivieren oder deaktivieren, um die Leistung zu optimieren:</p> <ul style="list-style-type: none">• Desktop background (Desktop-Hintergrund)• Font smoothing (Schriftglättung)• Desktop composition (Desktopgestaltung)• Show contents of window while dragging (Inhalte des Fensters beim Verschieben anzeigen)• Menu and window animation (Menü- und Fensteranimation)• Themes (Designs) <p>Die Auswahl von Client Preferred Settings (Vom Client bevorzugte Einstellungen) ermöglicht dem Client die Auswahl der zu verwendenden Optionen.</p> <p>Sie können auch Ihre eigene benutzerdefinierte Kombination von Optionen auswählen.</p>



HINWEIS: Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des VMware Horizon View Connection Manager.

Verwenden von Multi-Monitor Sitzungen mit VMware Horizon View

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.


Verwenden von Tastaturkürzeln mit VMware Horizon View

Windows-Tastenkombinationen

Zur Unterstützung der Windows-Systemverwaltung unterstützt VMware Horizon View die Tastaturkürzel 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 Tastaturkürzel wie **Strg+Alt+Tabulator** und **Strg+Alt+F4** nicht innerhalb der Remote-Sitzung funktionieren.

 **TIPP:** Um Sitzungen umschalten zu können, deaktivieren Sie die Optionen **Hide top Menu bar** (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 einer Remote-Desktop-Sitzung. Damit werden Multimediaprogramme wie z. B. Windows Media Player unterstützt.

Verwenden der Multimedia-Umleitung mit VMware Horizon View

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

Weitere Informationen hierzu finden Sie unter [Verwenden der Multimedia-Umleitung mit RDP auf Seite 41](#).

Geräte-Umleitung mit VMware Horizon View verwenden

USB-Umleitung mit VMware Horizon View verwenden

Um USB für VMware Horizon View-Verbindungen zu aktivieren, verwenden Sie **VMware Horizon View** als das Remote-Protokoll im USB-Manager.

Weitere Informationen zu USBR, einschließlich Geräte- und klassenspezifische Umleitung finden Sie unter [Verwenden einer USB-Umleitung mit RDP auf Seite 41](#)

Massenspeicher-Umleitung mit VMware Horizon View verwenden

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 - `xfreerdpoptions='/drive:$foldname,shared folder path, share device'` hinzu.

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

Weitere Einzelheiten finden Sie unter [Verwenden der Massenspeicherumleitung mit RDP auf Seite 42](#).

Drucker-Umleitung mit VMware Horizon View verwenden

Für Verbindungen mit dem PCoIP-Protokoll auf x86-Einheiten können unter Verwendung der VMware Horizon View High-Level-Druckerumleitung oder von USBR Drucker freigegeben werden. PCoIP-Verbindungen auf ARM-Einheiten unterstützen nur die USBR-Druckerumleitung. Für Verbindungen mit dem RDP-Protokoll, siehe [Verwenden der Druckerumleitung mit RDP auf Seite 43](#) für weitere Informationen.

Audiumleitung mit VMware Horizon View verwenden

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 USBR 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 View-Client verwendet eine High-Level Audiumleitung. Um das USB-Headset umzuleiten, verwenden Sie den USB Manager des Clients und wählen Sie das USB-Headset, das umgeleitet werden soll. Stellen Sie sicher, dass die **VMware Horizon View** als USBR-Protokoll

ausgewählt ist, und stellen Sie sicher, dass das Headset unter **Devices** (Geräte) zur Umleitung markiert ist.

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


Smart Card-Umleitung mit VMware Horizon View verwenden


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:** Zur Anmeldung am VMware Horizon View Manager-Administratorserver mit einer Smart Card müssen der lokale Smart Card-Treiber auf dem Client installiert sein. Weitere Informationen über die Smart Card Treiberinstallation finden Sie unter: [Smart Card-Umleitung mit RDP verwenden auf Seite 44](#). Nachdem Sie sich am Remote-Host angemeldet haben, wird die Smart Card über einen virtuellen Kanal an den Remote-Host weitergeleitet, nicht über USBR: Diese Weiterleitung über einen virtuellen Kanal stellt sicher, dass die Smart Card für Aufgaben wie E-Mail-Unterschriften, Bildschirmsperren usw. verwendet werden kann. Es könnte aber passieren, dass die Smart Card im Geräte-Manager von Windows nicht als Smart Card-Gerät erkannt wird.

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

Webcam-Umleitung mit VMware Horizon View verwenden

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 [Verwenden einer USB-Umleitung mit RDP auf Seite 41](#).


Ändern des VMware Horizon View Protokolltyps


Der VMware Horizon View-Client stellt mithilfe einer der folgenden Protokolltypen eine Verbindung her:

- (PCoIP)-Protokoll
- (RDP)-Protokoll

So ändern Sie den Verbindungstyp:

1. Wählen Sie im VMware Horizon View-Client unter **Desktop** einen Pool aus, der eines der folgenden Protokolle unterstützt:
 - PCoIP
 - RDP 2
2. Wählen Sie aus der Dropdown-Liste einen Verbindungstyp aus.

 **HINWEIS:** Verwenden Sie den VMware Horizon View-Manager, um zu konfigurieren, welches Verbindungsprotokoll für jeden Desktop-Pool 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 zu dem 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 erledigen:

- Verwenden Sie den Certificate 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 **Connection Security Level** (Sicherheitsstufe der Verbindung) auf **Allow all connections** (Alle Verbindungen zulassen).

Tabelle 8-5 VMware Horizon View Sicherheitsstufen von Zertifikaten

Sicherheitsstufen		
Unsichere Verbindungen verweigern	Warnen	Alle Verbindungen erlauben

Tabelle 8-5 VMware Horizon View Sicherheitsstufen von Zertifikaten (Fortsetzung)

		Sicherheitsstufen		
Vertrauenswürdigkeit des Zertifikats	Vertrauenswürdig	Vertrauenswürdig	Vertrauenswürdig	Vertrauenswürdig
	Selbst signiert	Fehler	Warnung	Nicht vertrauenswürdig
	Abgelaufen	Fehler	Warnung	Nicht vertrauenswürdig
	Nicht vertrauenswürdig	Fehler	Fehler	Nicht vertrauenswürdig

Tabelle 8-6 Definitionen für Sicherheitsstufe der Zertifikate

Stufe	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

VMware Horizon View-USB-Gerätefamilien

Tabelle 8-7 VMware Horizon View-USB-Gerätefamilien

Familie	Familienname
Vendor (Anbieter)	vendor
Unknown (Unbekannt)	unknown
Other (Sonstiges)	other
Audio In (Audioeingang)	audio-in
Audio Out (Audioausgang)	audio-out
Communications (Kommunikation)	comm
Human Interface Device (Schnittstelle für die Benutzerinteraktion)	hid
Bootable HID (Bootfähige HID)	hid-bootable
Force Feedback Device (Gerät zum Erzwingen von Feedback)	physical
Imaging	imaging
Printer (Drucker)	printer
Mass Storage (Massenspeicher)	storage
Smardcard Reader (Smart Card-Lesegerät)	smart-card

Tabelle 8-7 VMware Horizon View-USB-Gerätefamilien (Fortsetzung)

Familie	Familiename
Security (Sicherheit)	security
Video	video
Wireless Adapter (Wireless-Adapter)	wireless
Bluetooth	bluetooth
Wireless USB (Wireless-USB)	wusb
PDA (Handheld)	Pda

9 Web Browser-Verbindungen

- [Web Browser Allgemeine Einstellungen](#)
- [Web Browser – Verbindungsspezifische Einstellungen](#)

Web Browser Allgemeine Einstellungen

Die folgende Tabelle beschreibt die Einstellungen, die im Web Browser Connection General Settings Manager verfügbar sind. Diese Einstellungen sind universal und gelten für alle Web-Browser-Verbindungen.


 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 9-1 Web Browser Connection General Settings Manager

Option	Beschreibung
Web Browser preferences (Web Browser-Einstellungen)	Öffnet das Dialogfeld Firefox-Einstellungen.
Allow connections to manage their own settings (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 – Verbindungsspezifische Einstellungen

Die folgende Tabelle beschreibt die Einstellungen, die im Web Browser Connection Manager verfügbar sind. Diese Einstellungen sind verbindungsspezifisch und gelten nur für die Web Browser-Verbindung, die Sie derzeit konfigurieren.



 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 9-2 Web Browser Connection Manager > Seite 1

Option	Beschreibung
Name	Der Verbindungsname.
URL	Die URL für die Verbindung.
Enable kiosk mode (Kioskmodus aktivieren)	Aktiviert den Kioskmodus.
Enable full screen (Vollbild aktivieren)	Verwendet den Vollbildmodus für die Verbindung.
Enable print dialog (Dialogfeld Drucken aktivieren)	Aktiviert das Dialogfeld Drucken.


 **HINWEIS:** Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des Web Browser Connection Manager.

10 Zusätzliche Verbindungstypen (gilt nur für ThinPro-Konfiguration)

Die in diesem Kapitel aufgeführten Verbindungstypen sind nur verfügbar, wenn der Client auf die ThinPro-Konfiguration eingestellt ist. Weitere Informationen finden Sie unter [Vergleich von ThinPro und Smart Zero auf Seite 1](#).

- [TeemTalk Verbindungseinstellungen](#)
- [XDMCP Verbindungseinstellungen](#)
- [SSH Verbindungseinstellungen](#)
- [Telnet Verbindungseinstellungen](#)
- [Benutzerdefinierte Verbindungseinstellungen](#)

TeemTalk Verbindungseinstellungen

 **TIPP:** Weitere Informationen zu HP TeemTalk finden Sie im *HP TeemTalk Terminal Emulator Benutzerhandbuch*.

Die folgende Tabelle beschreibt die Einstellungen, die im TeemTalk Connection Manager verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die TeemTalk-Verbindung, die Sie derzeit konfigurieren.



 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 10-1 TeemTalk Connection Manager

Option	Beschreibung
Name	Der Verbindungsname.
TeemTalk Creation wizard (TeemTalk Erstellungsassistent)	Zum Öffnen des TeemTalk-Sitzungsassistenten. Weitere Informationen finden Sie in den anderen Tabellen in diesem Abschnitt.
System beep (System-Piepton)	Aktiviert den Systemton.

 **HINWEIS:** Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des TeemTalk Connection Manager.

Die folgenden Tabellen beschreiben die Einstellungen im TeemTalk-Sitzungsassistenten (Komponente des TeemTalk Connection Manager) verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die TeemTalk-Verbindung, die Sie derzeit konfigurieren.


 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Tabelle 10-1, „TeemTalk Connection Manager“, auf Seite 55](#).

Tabelle 10-2 TeemTalk-Sitzungsassistent > Seite 1

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

Tabelle 10-3 TeemTalk-Sitzungsassistent > Seite 2

Option	Beschreibung
Emulation Printer (Emulationsdrucker)	Die Druckereinstellungen für die HP TeemTalk-Emulation.
Auto Logon (Automatische Anmeldung)	Die Einstellungen für die automatische Anmeldung für HP TeemTalk.
Key Macros (Tastatur-Makros)	Die Einstellungen der Tasten-Makros für HP TeemTalk.
Mouse Actions (Mausaktionen)	Die Einstellungen für Mausaktionen für HP TeemTalk.
Soft Buttons (Softkey-Tasten)	Die Einstellungen der Soft-Tasten für HP TeemTalk.
Attributes (Attribute)	Die HP TeemTalk-Attributeinstellungen.
Auxiliary Ports (Zusätzliche Ports)	Die Einstellungen für HP TeemTalk-Hilfsanschlüsse.
Hotspots	Die Einstellungen für HP TeemTalk-Hotspots.

Tabelle 10-4 TeemTalk-Sitzungsassistent > Seite 3

Option	Beschreibung
Preferences (Einstellungen)	Zeigt die in Tabelle 10-5 , „ TeemTalk-Sitzungsassistent > Seite 3 > Einstellungen “, auf Seite 56 festgelegten Einstellungen an.
Start session connected (Verbundene Sitzung starten)	Startet diese Sitzung verbunden.
Show Status Bar (Statusleiste anzeigen)	Zeigt die Statusleiste für diese Verbindung an.

Tabelle 10-5 TeemTalk-Sitzungsassistent > Seite 3 > Einstellungen

Option	Beschreibung
Show Configuration Bar (Konfigurationsleiste anzeigen)	Zeigt die Konfigurationsleiste an.
Save Current Window Position (Aktuelle Fensterposition speichern)	Speichert die aktuelle Größe und Position des Fensters, wenn Sie auf Save Preferences (Einstellungen speichern) klicken. Sie werden beim nächsten Systemstart wiederhergestellt. HINWEIS: Klicken Sie jedes mal auf Save Preferences , wenn Sie die Fenstergröße oder Position ändern, um die neuen Werte zu speichern.

Tabelle 10-5 TeemTalk-Sitzungsassistent > Seite 3 > Einstellungen (Fortsetzung)

Option	Beschreibung
Run in Full Screen Mode (Im Vollbildmodus ausführen)	<p>Wählen Sie diese Option aus, damit das Fenster mit voller Bildschirmgröße angezeigt wird. Dies entfernt die Rahmen, die Soft-Buttons, das Menü und die Konfigurationsleisten.</p> <p>HINWEIS: Diese Option wird erst beim nächsten Systemstart aktiviert und überschreibt die Optionen Show Configuration Bar und Save Current Window Position.</p>
Browser Command (Browserbefehl)	<p>Geben Sie den Befehl in das Feld ein, mit dem Ihr Internetbrowser ausgeführt wird, wie z. B. :</p> <pre>/ display html links Firefox</pre>
Command Line Start Up Options (Startoptionen für Befehlszeile)	<p>Wird verwendet, um einen alternativen Speicherort für die Startoptionen anzugeben.</p> <p>HINWEIS: Für spezifische Informationen über die HP TeemTalk Befehlszeilen-Startoptionen siehe <i>HP TeemTalk Terminal Emulator Benutzerhandbuch</i>.</p>

Tabelle 10-6 TeemTalk-Sitzungsassistent > Seite 4

Komponente	Beschreibung
Summary Session Information (Zusammenfassung der Sitzungsinformationen)	Zeigt eine Zusammenfassung der zu erstellenden Sitzung an.

XDMCP Verbindungseinstellungen

XDMCP bietet die Möglichkeit, direkt Remoteverbindungen zu X-Servern herzustellen. X-Server werden auf den meisten UNIX-ähnlichen Betriebssystemen, z. B. Linux, Berkeley Software Distribution (BSD) und Hewlett Packard UniX (HP-UX), für die Grafikanzeige verwendet.

Die folgende Tabelle beschreibt die Einstellungen, die im XDMCP Connection Manager verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die XDMCP-Verbindung, die Sie derzeit konfigurieren.



 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 10-7 Konfigurationseinstellungen für neue XDMCP-Verbindungen

Option	Beschreibung
Name	Der Verbindungsname.
Type (Typ)	Der Typ der XDMCP-Verbindung. Gültige Optionen sind: chooser (Auswahlfunktion), query (Abfrage) und broadcast (Übertragung).
Address (Adresse)	Dieser Wert ist erforderlich, wenn der Wert für Type (Typ) auf Query (Abfrage) eingestellt ist.
Use font server (Schriftartenserver verwenden)	Anstelle der lokal installierten Schriftarten wird ein Remote-X-Fontserver für Schriftarten verwendet.

Tabelle 10-7 Konfigurationseinstellungen für neue XDMCP-Verbindungen (Fortsetzung)

Option	Beschreibung
Font server (Schriftartenserver)	"Font Server" ist nur aktiviert, wenn die Option Use font server (Fontserver verwenden) aktiviert ist.
Configure display (Anzeige konfigurieren)	Klicken Sie hier, um die Anzeigeconfiguration für die Verbindung einzurichten. Wenn Sie keine Konfiguration festlegen, wird die Standardkonfiguration verwendet.

 **HINWEIS:** Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des XDMCP Connection Manager.

SSH Verbindungseinstellungen

SSH (Secure Shell) ist die am häufigsten verwendete Möglichkeit, um Remote-Zugriff auf die Befehlszeile von UNIX-ähnlichen Betriebssystemen, z. B. Linux, BSD und HP-UX, zu erhalten. SSH ist außerdem verschlüsselt.

Die folgende Tabelle beschreibt die Einstellungen, die im SSH Connection Manager verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die SSH-Verbindung, die Sie derzeit konfigurieren.



 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 10-8 Konfigurationseinstellungen für neue SSH-Verbindungen

Option	Beschreibung
Name	Der Verbindungsname.
Address (Adresse)	Die IP-Adresse des Remote-Systems.
Port	Der Remote-Port, der für die Verbindung verwendet werden soll.
User name (Benutzername)	Der Benutzername, der für die Verbindung verwendet werden soll.
Run application (Anwendung ausführen)	Die Anwendung, die zum Herstellen der Verbindung ausgeführt werden soll.
Compression (Komprimierung)	Wählen Sie diese Option aus, wenn die zwischen dem Server und dem Thin Client gesendeten Daten komprimiert werden sollen.
X11 connection forwarding (X11-Verbindungsweiterleitung)	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.
Force TTY allocation (TTY-Zuweisung erzwingen)	Wählen Sie diese Option und geben Sie einen Befehl an, um eine temporäre Session zu starten, die den Befehl ausführt. Sobald der Befehl ausgeführt wird, geht die Session zu Ende. Wenn kein Befehl angegeben wird, wird die Session normal ausgeführt, als wäre die Option nicht ausgewählt worden.
Foreground color (Vordergrundfarbe)	Die Standardfarbe für den Text in der SSH-Session.
Background color (Hintergrundfarbe)	Die Standardfarbe für den Hintergrund in der SSH-Session.
Font (Schriftart)	Gültige Optionen sind: 7X14, 5X7, 5X8, 6X9, 6X12, 7X13, 8X13, 8X16, 9X15, 10X20 und 12X24 .

 **HINWEIS:** Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des SSH Connection Manager.

Telnet Verbindungseinstellungen

Bei Telnet handelt es sich um eine ältere Methode für den Remotezugriff auf Befehlszeilen. Die übertragenen Daten werden nicht verschlüsselt.

Die folgende Tabelle beschreibt die Einstellungen, die im Telnet Connection Manager verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die Telnet-Verbindung, die Sie derzeit konfigurieren.



 **HINWEIS:** Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 10-9 Konfigurationseinstellungen für neue Telnet-Verbindungen

Option	Beschreibung
Name	Der Name der Verbindung.
Address (Adresse)	Die IP-Adresse des Remote-Systems.
Port	Der Port, der auf dem Remote-System verwendet werden soll.
Foreground color (Vordergrundfarbe)	Die Vordergrundfarbe.
Background color (Hintergrundfarbe)	Die Hintergrundfarbe.
Font (Schriftart)	Gültige Optionen sind: 7X14, 5X7, 5X8, 6X9, 6X12, 6X13, 7X13, 8X13, 8X16, 9X15, 10X20 und 12X24 .

 **HINWEIS:** Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des Telnet Connection Manager.

Benutzerdefinierte Verbindungseinstellungen

Wenn Sie eine kundenspezifische Linux-Anwendung installieren möchten, können Sie die Verbindung "Custom" (Benutzerdefiniert) verwenden, damit diese Anwendung über den Connection Manager geöffnet werden kann.

Die folgende Tabelle beschreibt die Einstellungen, die im Custom Connection Manager verfügbar sind. Diese Einstellungen sind verbindungspezifisch und gelten nur für die Custom-Verbindung, die Sie derzeit konfigurieren.



HINWEIS: Wo Sie diese Einstellungen finden, erfahren Sie unter [Verwenden der Connection Manager-Bedienelemente auf Seite 6](#).

Tabelle 10-10 Konfigurationseinstellungen für neue benutzerdefinierte Verbindungen

Option	Beschreibung
Name	Der Verbindungsname.
Enter command to run (Auszuführenden Befehl eingeben)	Der Befehl, der zum Herstellen der Remote-Verbindung ausgeführt werden soll.



HINWEIS: Siehe [Gemeinsame Verbindungseinstellungen auf Seite 27](#) für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des Custom Connection Manager.

11 HP Smart Client Services

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

Clients erkennen einen Automatic Update-Server beim Hochfahren und konfigurieren sich selbst entsprechend. Dies vereinfacht die Geräteinstallation und Wartung.

- [Unterstützte Betriebssysteme](#)
- [Voraussetzungen für HP Smart Client Services](#)
- [Abrufen von HP Smart Client Services](#)
- [Anzeigen der Automatic Update-Website](#)
- [Ein Automatic Update-Profil erstellen](#)
- [Clients aktualisieren](#)

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** auf der Seite **Drivers, Software & Firmware** (Treiber, Software und Firmware).

Anzeigen der Automatic Update-Website

1. Auf dem Server Desktop, wählen Sie **Start > Control Panel** (Start > Systemsteuerung), und klicken Sie dann **Administrative Tools** (Verwaltungstools).
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`

Ein Automatic Update-Profil erstellen

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

1. Rufen Sie die MAC-Adresse des Clients über die Systeminfo ab. Zum Beispiel verwenden die folgenden Schritte die MAC-Adresse `00fcab8522ac`.
2. Verwenden Sie den Profile Editor zum Erstellen oder Ändern eines Client-Profiles (siehe [„Verwenden des Profile Editors“ auf Seite 65](#)), bevor Sie das Client-Profil speichern.
3. Klicken Sie im **Profile Editor** auf den Link **Finish** (Beenden) im linken Bereich, um auf den Bereich **Current Profile** (Aktuelles Profil) zuzugreifen.
4. Klicken Sie auf **Save profile as** (Profil speichern unter), um das Client-Profil folgendermaßen zu speichern:

`C:\Program Files (x86) Hewlett-Packard\HP Smart Client Service\auto-update\PersistentProfile\MAC\00fcab8522ac.xml`


5. Klicken Sie auf die Schaltfläche **Finish** (Beenden) im Bereich **Current profil** (Aktuelles Profil), um den Profile Editor zu beenden.
6. Starten Sie den Client neu, der die angegebene MAC-Adresse zum Initiieren des Automatic Update-Vorgangs verwendet.


Clients aktualisieren

- [Verwenden der Methode Aktualisierung per Übertragung](#)
- [Verwenden der Aktualisierungsmethode mit der DHCP-Kennung](#)
- [Verwenden der Aktualisierungsmethode mit DNS Alias](#)
- [Verwenden der manuellen Aktualisierungsmethode](#)

Verwenden der Methode Aktualisierung per Übertragung

Um eine Aktualisierung per Übertragung vorzunehmen, stecken Sie den Client an dasselbe Netzwerk wie den Aktualisierungsserver an. Eine Aktualisierung per Übertragung stützt sich auf HP Smart Client Services, das mittels IIS automatisch Aktualisierungen zum Client überträgt.

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


 **TIPP:** Um zu überprüfen, ob die Aktualisierung per Übertragung funktioniert, führen Sie den 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 71](#).

Verwenden der Aktualisierungsmethode mit der DHCP-Kennung

Auf Windows Server 2003- und Windows Server 2008-Systemen, ermöglicht die DHCP-Tagging einem Client die Aktualisierung. Verwenden Sie diese Methode zum Aktualisieren bestimmter Clients; wenn Sie allerdings nur einen oder zwei Clients aktualisieren möchten, sollten Sie stattdessen die manuelle Aktualisierung in Betracht ziehen. Generell empfiehlt HP die Methode 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. Klicken Sie im linken Fensterbereich des **DHCP**-Bildschirms auf die Domäne, mit der die Clients verbunden sind.
3. Erweitern Sie im rechten Fensterbereich des Bildschirms **DHCP** die Anzeige von **IPv4**, klicken Sie mit der rechten Maustaste darauf, und klicken Sie dann auf **Set Predefined Options** (Vordefinierte Optionen einstellen).
4. Klicken Sie im Dialogfeld **Predefined Options and Values** auf **Add** (Vordefinierte Optionen und Werte) (Hinzufügen).
5. Im Feld **Optionstyp** konfigurieren Sie die Optionen wie in der folgenden Tabelle beschrieben.

Tabelle 11-1 Beispieloptionen für DHCP-Kennung

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

6. Klicken Sie auf **OK**.
7. Im Dialogfeld **Predefined Options and Values** (Vordefinierte Optionen und Werte) geben Sie unter **Value (Wert) > String** die Update Server-Adresse im Format des folgenden Beispiels ein:

`http://auto-update.dominio.com:18287/auto-update`

8. Um das Einrichten abzuschließen, klicken Sie auf **OK**. Die DHCP-Kennung ist jetzt bereit für die Aktualisierung bestimmter Clients.

Verwenden der Aktualisierungsmethode mit DNS Alias


Während des Systemstarts versucht Automatic Update den DNS-Alias **auto-update** aufzulösen. Wenn dieser Host-Name aufgelöst werden kann, versucht es, die Updates unter **http://auto-update:18287** zu überprüfen. Diese Updatemethode ermöglicht es Clients, auf einen einzelnen Updateserver in der gesamten Domäne zuzugreifen, was 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 manuellen Aktualisierungsmethode

Verwenden Sie die manuelle Aktualisierungsmethode, um eine Verbindung zwischen einem Client und einem spezifische Server für eine Aktualisierung herzustellen. Verwenden Sie diese Methode auch, wenn Sie eine Aktualisierung auf einem einzelnen Client testen möchten, bevor Sie sie es auf viele Clients anwenden, oder wenn Sie bestimmte Aktualisierungen nur auf einem oder zwei Clients installieren möchten.

 **HINWEIS:** Stellen Sie sicher, dass Sie den Host-Namen des manuellen Server in dem Profil angegeben haben, den Sie aktualisieren. Andernfalls werden die Einstellungen beim Herunterladen des Profils auf automatisch zurückgesetzt. Verwenden Sie den **Profile Editor**, um diese Einstellungen bei `root/auto-update` zu ändern.

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

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

Eine manuelle Aktualisierung durchführen


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 das Feld **Server** den Update-Server-Hostnamen und Port im folgenden Format ein:
`<hostname>:18287`
5. Geben Sie im Feld **Path** (Pfad) Folgendes ein: `auto-update`
6. Klicken Sie auf **OK** und der Client wird sich die Updates holen.

12 Verwenden des Profile Editors

HP Smart Client Services beinhaltet den Profile Editor, mit dem Administratoren Client-Profil erstellen und in den Automatic Update-Server hochladen können. Das Client-Profil enthält Verbindungsinformationen, Einstellungen und Dateien, die die Smart Clients herunterladen und im Selbstkonfigurationsvorgang verwenden.

Dieser Abschnitt enthält die folgenden Themen:

- [Zugriff auf den Profile Editor](#)
- [Laden eines Client-Profiles](#)
- [Ändern eines Client-Profiles](#)
- [Konfigurieren eines seriellen oder parallelen Druckers](#)

 **HINWEIS:** Siehe „[Registrierungsschlüssel](#)“ auf Seite 87 für eine umfassende Liste und Beschreibung der Registrierungsschlüssel.

Zugriff auf den Profile Editor

- ▲ Klicken Sie auf **Start > All Programs (Alle Programme) > Hewlett-Packard > HP Automatic Update-Server > Profile Editor**.

Laden eines Client-Profiles

Der Profile Editor lädt automatisch das Standardprofil, das während des HP Smart Client Services-Installationsvorgangs erstellt wurde. Dies wird durch den Link `Profile.xml` im **Profile Editor**-Bereich angezeigt.

So laden Sie ein Profil:

1. Klicken Sie im Bereich **Profile Editor** auf **Profil.xml**.
2. Wählen Sie das gewünschte Profil und klicken Sie anschließend auf **Open** (Öffnen).

Ändern eines Client-Profiles

Verwenden Sie die verschiedenen Bildschirme im Profile Editor, um ein Client-Profil zu ändern, wie in den folgenden Themen besprochen:

- [Auswahl der Plattform eines Client-Profiles](#)
- [Auswahl des Verbindungstyps eines Client-Profiles](#)
- [Ändern der Einstellungen der Registrierung eines Client-Profil](#)
- [Hinzufügen von Dateien zu einem Client-Profil](#)
- [Speichern des Clients-Profiles](#)


Auswahl der Plattform eines Client-Profiles


Verwenden Sie den Link **Plattform** (Plattform) im Profile Editor für den Zugriff auf den Bereich **Plattform** (Plattform), der zum Konfigurieren der folgenden Einstellungen verwendet werden kann:

- Mit Ihrer Hardware kompatible Client-Softwareversionen
- Optionale Client-Kits, die zusätzliche Registrierungseinstellungen zur Verfügung stellen


So richten Sie die Client-Profilplattform ein:

1. Wählen Sie im Bereich **Plattform** (Plattform) unter **Smart Zero Client versions > OS Build ID** (Smart Zero Client-Versionen > Betriebssystem-Build-ID) eine Betriebssystem-Build-ID aus.

 **TIPP:** Erstellen Sie für jeden Hardwaretyp ein eigenes Profil.

 **HINWEIS:** Wenn Sie ein Client-Kit installieren, werden die zusätzlichen Registrierungseinstellungen automatisch im Feld Client-Kit und im Bereich Registry (Registrierung) angezeigt.

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

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

3. Klicken Sie nach Abschluss auf **Next** (Weiter).

Auswahl des Verbindungstyps eines Client-Profiles

Verwenden Sie den Link **Connection** (Verbindung) im Profile Editor für den Zugriff auf den Bereich **Remote Connection Server** (Remote-Verbindungsserver), der zum Einrichten des Verbindungstyps für das Client-Profil verwendet wird. Gehen Sie wie folgt vor:

1. Wählen Sie im Bereich **Remote Connection Server** (Remote-Verbindungsserver) unter **Type** (Typ) den gewünschten **Connection Type** (Verbindungstyp) aus.
2. Unter **Server** geben den Namen oder die IP-Adresse des Servers ein, der konfiguriert werden soll.
3. Klicken Sie nach Abschluss auf **Next** (Weiter).

Ändern der Einstellungen der Registrierung eines Client-Profil

Verwenden Sie den Link **Registry** (Registrierung) im Profile Editor für den Zugriff auf den **Registry Editor** (Registrierungseditor), der dazu verwendet werden kann, Standardwerte in den Client-Profil-Einstellungen zu ändern. Gehen Sie dazu wie folgt vor:

1. Erweitern Sie die Ordner in der Struktur **Registry settings** (Registrierungseinstellungen), um nach der zu ändernden Option zu suchen.
2. Klicken Sie auf die Option, und ändern Sie dann den Standardwert im Feld **Value** (Wert).

Aktivieren oder deaktivieren der Benutzerkonfigurationen auf Clients

1. In der Struktur **Registry settings** (Registrierungseinstellungen) navigieren Sie zu **root > users > user > apps**.
2. Erweitern Sie den Ordner für das Menüelement, das aktiviert oder deaktiviert werden soll und klicken Sie auf die Einstellung **authorized** (autorisiert).
3. Geben Sie die entsprechende Zahl im Feld **Value** (Wert) ein:

- 0 (deaktivieren)
- 1 (aktivieren)

Hinzufügen von Dateien zu einem Client-Profil


Verwenden Sie den Link **Files** (Dateien) im Profile Editor für den Zugriff auf den Bereich **Additional Configuration Files** (Zusätzliche Konfigurationsdateien), der dazu verwendet werden kann, Konfigurationsdateien hinzuzufügen, die automatisch auf dem Client installiert werden, wenn das Profil installiert wird. Dies wird normalerweise aus folgenden Gründen durchgeführt:

- 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 anlegen, die auf eine Datei zeigt, die bereits auf dem Client installiert ist. Verwenden Sie diese Option, wenn auf die Datei von mehr als einem Verzeichnis zugegriffen werden muss.

Hinzufügen einer Konfigurationsdatei zu einem Client-Profil


1. Klicken Sie im Bereich **Additional Configuration Files**(Zusätzliche Konfigurationsdateien) auf **Add a file** (Eine Datei hinzufügen).
2. Klicken Sie auf **Import File** (Datei importieren), suchen Sie die Datei an, die importiert werden soll, und klicken Sie dann **Open** (Öffnen).

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

3. Im Feld **Path** (Pfad) legen Sie den Pfad fest, wo die Datei auf dem Client installiert wird.
4. Im Bereich **File details** (Dateidetails) geben Sie in den Feldern **Owner** (Eigentümer), **Group** (Gruppe), und **Permissions** (Berechtigungen) die entsprechenden Werte ein.

 **HINWEIS:** In der Regel ist das Einstellen des Eigentümers und der Gruppe als **root** und der Berechtigungen auf **644** ausreichend. Wenn ein spezieller Eigentümer, eine spezielle Gruppe oder spezielle Berechtigungen erforderlich sind, beziehen Sie sich auf die Standard-Unix-Dateiberechtigungen, um Richtlinien zum Ändern der Dateidetails zu finden.

5. Klicken Sie auf **Save** (Speichern), um das Hinzufügen der Konfigurationsdatei zum Client-Profil 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 Werkzeugeinstellungen wiederhergestellt werden.

Zertifikate zu einem Client-Profil hinzufügen

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. Klicken Sie im Bereich **Additional Configuration Files** (Zusätzliche Konfigurationsdateien) auf **Add a file** (Datei hinzufügen).
2. Klicken Sie auf **Import File** (Datei importieren), ermitteln Sie das Zertifikat und klicken Sie auf **Open** (Öffnen).



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. Klicken Sie auf **Save** (Speichern), um das Hinzufügen des Zertifikats zum Client-Profil abzuschließen.
5. Verwenden Sie nach der Installation des Clients-Profiles den **Certificate Manager** um sicher zu gehen, dass das Zertifikat ordnungsgemäß importiert wurde.

Hinzufügen eines symbolischen Links zu einem Client-Profil

1. Klicken Sie im Bereich **Additional Configuration Files** (Zusätzliche Konfigurationsdateien) auf **Add a file** (Eine Datei hinzufügen).
2. Wählen Sie in der Dropdown-Liste **Type** (Typ) die Option **Link**.
3. Im Bereich **Symbolic link details** (Symbolische Link-Details) legen Sie den **Link** auf den Pfad der gewünschten Datei, die bereits auf dem Client installiert ist, fest.
4. Klicken Sie auf **Save** (Speichern) zum Hinzufügen des symbolischen Links.

Speichern des Clients-Profiles

1. Klicken Sie im **Profile Editor** auf den Link **Finish** (Beenden) im linken Bereich, um auf den Bereich **Current profile** (Aktuelles Profil) zuzugreifen.
2. Klicken Sie auf **Save Profile** (Profil speichern) zum Speichern des aktuellen Client-Profiles oder klicken Sie auf **Save Profile as** (Profil speichern unter), um es neues Client-Profil zu speichern.



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

3. Klicken Sie auf die Schaltfläche **Finish** (Beenden) im Bereich **Current profile** (Aktuelles Profil), um den Profile Editor zu beenden.

Konfigurieren eines seriellen oder parallelen Druckers

Verwenden Sie den Profile Editor zum Einrichten der seriellen oder parallelen Druckeranschlüsse. Ein USB-Drucker wird beim Anschließen automatisch zugeordnet.

Dieser Abschnitt enthält die folgenden Themen:

- [Abrufen der Druckereinstellungen](#)

- [Einrichten von Druckeranschlüssen](#)
- [Drucker auf dem Server installieren](#)

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** gedrückt, während das Gerät eingeschaltet wird.
2. Nach einigen Sekunden lassen Sie die **Feed**-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**-Taste nochmals drücken, damit die Diagnosesseite gedruckt wird.

Einrichten von Druckeranschlüssen


1. Wählen Sie im **Profile Editor** (Profil-Editor) **Registry** (Registrierung) aus, und klicken Sie dann auf **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** (Root > Verbindungstyp > freerdp). Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **New connection** (Neue Verbindung) aus und klicken Sie auf **OK**. Legen Sie den Registrierungsschlüssel **portMapping** auf den Wert **1** fest, um die Druckerportzuordnung zu aktivieren.
 - VMware Horizon View – Navigieren Sie zu **root > ConnectionType > view** (Root > Verbindungstyp > Ansicht). Klicken Sie mit der rechten Maustaste auf den Ordner **connections**, wählen Sie **New connection** (Neue Verbindung) aus und klicken Sie auf **OK**. Legen Sie unter dem Ordner **xfreerdpOptions** den Registrierungsschlüssel **portMapping** auf den Wert **1** fest, um die Druckerportzuordnung zu aktivieren.
3. Navigieren Sie zu **root > Serial** (Root > Seriell). Klicken Sie mit der rechten Maustaste auf den Ordner **Serial** (Seriell), wählen Sie **New UUID** (Neue UUID) und klicken Sie auf **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 69](#) 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`, 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.


Drucker auf dem Server installieren


1. Auf dem Windows-Desktop wählen Sie **Start > Printers and Faxes (Drucker und Faxgeräte)**.
2. Wählen Sie **Add Printer** (Drucker hinzufügen) und klicken Sie anschließend auf **Next** (Weiter).

3. Wählen Sie **Local Printer attached to this Computer** (Lokaler Drucker, der an den Computer angeschlossen ist) und bei Bedarf deaktivieren Sie **Automatically detect and install my Plug and Play printer** (Plug & Play-Drucker automatisch ermitteln und installieren).
4. Klicken Sie nach Abschluss auf **Next** (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 aufgefordert werden, den vorhandenen Treiber beizubehalten und dieser funktioniert, dann behalten Sie diesen Treiber bei und klicken Sie auf **Next** (Weiter).
8. Weisen Sie dem Drucker einen Namen zu. Um ihn als Standarddrucker zu verwenden, wählen Sie **Yes** (Ja), und klicken Sie dann **Next** (Weiter).
9. Wenn Sie den Drucker freigeben möchten, wählen Sie **Share name** (Freigabename) und weisen Sie dem Drucker einen Freigabennamen zu. Klicken Sie anderenfalls auf **Next** (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 Client die Verbindung zum Server trennt, muss der Drucker beim nächsten Verbindungsaufbau des Clients erneut eingerichtet werden.

13 Fehlerbeseitigung

In diesem Kapitel werden folgende Themen behandelt:

- [Fehlerbeseitigung der Netzwerkverbindung](#)
- [Fehlerbeseitigung bei Firmware-Beschädigung](#)
- [Fehlerbehebung bei abgelaufenen Citrix-Kennwörtern](#)
- [Verwenden Systemdiagnose für die Fehlerbeseitigung](#)

Fehlerbeseitigung der Netzwerkverbindung

1. "Ping" zusammen mit der IP-Adresse des Clients Server indem Sie Folgendes durchführen:
 - a. Klicken Sie auf die Schaltfläche Systeminformationen in der Taskleiste und klicken Sie dann auf die Registerkarte **Net Tools** (Netzwerktools).
 - b. Unter **Select Tool** (Tool auswählen) wählen Sie **Ping**.
 - c. Im Feld **Target Host** (Zielhost) geben Sie die Server-Adresse ein und klicken Sie dann **Start Process** (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=0.81 5 ms 64 bytes  
from 10.30.8.52: icmp_seq=2 ttl=64 time=0.735 ms
```

Wenn der Ping-Befehl nicht erfolgreich war, wurde der Client möglicherweise vom Netzwerk getrennt und es gab eine Verzögerung ohne Systemausgabe.

2. Falls der Client nicht auf den Ping reagiert, gehen Sie wie folgt vor:
 - a. Überprüfen Sie das Netzkabel und überprüfen Sie die Netzwerkeinstellungen in der Systemsteuerung.
 - b. Versuchen Sie, einen Ping-Befehl für andere Server oder Clients auszuführen.
 - c. Wenn Sie andere Netzwerk-Clients erreichen, überprüfen Sie, ob Sie die richtige Server-Adresse eingegeben haben.
 - d. Führen Sie einen Ping unter Verwendung der IP-Adresse durch anstelle des Domännennamens oder umgekehrt.
3. Überprüfen Sie die Systemprotokolle indem Sie Folgendes durchführen:
 - a. Klicken Sie auf die Schaltfläche Systeminformationen in der Taskleiste und klicken Sie dann auf die Registerkarte **System Logs** (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 Firmware-Beschädigung

Wenn Sie nach dem Einschalten des Geräts zwei Signaltöne hören oder das Gerät nicht zu starten scheint, ist möglicherweise die Gerätefirmware beschädigt. Es ist möglich, dieses Problem zu beheben. Dies geschieht durch Herunterladen des Clients-Image von <http://www.hp.com>, Kopieren des Image zu einem auswechselbaren USB-Flash-Laufwerk und Neustart des Clients von diesem Flash-Laufwerk.

Re-Imaging der Client-Firmware des Geräts


1. Laden Sie das Image von <http://www.hp.com> herunter.
2. Entpacken Sie das Image zu dem Pfad **C:\USBBoot**.
3. Formatieren Sie ein USB-Flash-Laufwerk.
4. Kopieren Sie alle Dateien von **C:\USBBoot** in den Stamm des USB-Flash-Laufwerks.
5. Client ausschalten.
6. Stecken Sie das USB-Flash-Laufwerk am Thin Client ein.
7. Client einschalten. Der Client wird über ein USB-Flash-Laufwerk gestartet.
8. Befolgen Sie die Bildschirmanweisungen, um ein Re-Imaging des Clients durchzuführen.
9. Wenn der Re-Imaging-Prozess abgeschlossen ist, entfernen Sie das USB-Flash-Laufwerk und drücken Sie die **Eingabetaste**.

Fehlerbehebung bei abgelaufenen Citrix-Kennwörtern

Wenn Benutzer nicht dazu aufgefordert werden, abgelaufene Citrix-Kennwörter zu ändern, sollten Sie sicherstellen, dass die XenApp Services-Site (Pnagent-Site) für die Authentifizierungsmethode **Prompt** konfiguriert ist, um es Benutzern zu ermöglichen, abgelaufene Kennwörter zu ändern. Wenn Sie Benutzern erlauben, ihre Passwörter über eine direkte Verbindung zum Domänencontroller zu ändern, sollten Sie außerdem die Synchronizität der Systemzeit von Client und Domänencontroller sicherstellen und darauf achten, 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 Systemdiagnose für die Fehlerbeseitigung

Die Systemdiagnose erstellt einen Snapshot des Clients, der verwendet wird, um Probleme zu lösen, ohne physischen Zugriff zum Client. Dieser Snapshot enthält Protokolldateien von BIOS-Informationen und die Prozesse, die zum Zeitpunkt der Ausführung der Systemdiagnose aktiv waren.

-  **TIPP:** Markieren Sie das Feld **Enable Debug Mode** (Debug-Mode aktivieren) auf der Registerkarte **System Logs** (Systemprotokolle) des Bildschirms **About the Client** (Über den Client), um mehr Informationen im Diagnosebericht zu generieren. Diese Informationen können von HP angefordert werden, um die Fehlerbeseitigung zu starten. Da beim Neustart Protokolldateien durch das System zurückgesetzt werden, sollten Protokolle vor einem Neustart gespeichert werden.


Speichern von Systemdiagnosedaten

1. Stecken Sie ein USB-Flash-Laufwerk am Thin Client ein.
2. Klicken Sie auf die Schaltfläche Systeminformationen in der Taskleiste und klicken Sie dann auf die Registerkarte **System Logs** (Systemprotokolle).
3. Klicken Sie auf **Diagnostic** (Diagnose), und speichern Sie dann die komprimierte Diagnosedatei **Diagnostic.tgz** 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 sie.
 **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.

Tabelle 13-1 Dateien im Ordner Befehle

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 USB-Updates aktiviert sind (siehe [Anpassungscenter auf Seite 19](#)), können Sie ganz einfach über ein USB-Flash-Laufwerk Add-ons installieren und Profile bereitstellen.

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. Markieren Sie die Kontrollkästchen neben den Updates, die Sie installieren möchten, und klicken Sie dann auf **Install** (Installieren).
4. Starten Sie den Thin Client nach der Installation neu, wenn Sie dazu aufgefordert werden.

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

BIOS-Tool für Einstellungen

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

Syntax	Beschreibung
<code>hptc-bios-cfg -g [options] [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 [options] [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. Die Optionen sind Plattform-abhängig, verwenden Sie also diesen Befehl, um die Optionen anzuzeigen, die für die betreffende Plattform zur Verfügung stehen.

BIOS Flashing-Tool

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

Syntax	Beschreibung
<code>hptc-bios-flash [options] <ImageName></code>	Flasht das BIOS mit dem spezifizierten BIOS-Image.
<code>hptc-bios-cfg -h</code>	Zeigt eine Liste der Optionen an. Die Optionen sind Plattform-abhängig, verwenden Sie also diesen Befehl, um die Optionen anzuzeigen, die für Ihre spezielle Plattform zur Verfügung stehen.

C Ändern der Größe der Flash-Laufwerk-Partition

Wenn ein Thin Client, auf dem HP ThinPro ausgeführt wird, ab Werk geliefert wird, hat das auf ihm geflashte Image eine Größe von 1 GB, unabhängig von der Gesamtgröße des Flash-Laufwerks. Dies macht es leichter, das Image benutzerdefiniert anzupassen und auf anderen Clients bereitzustellen, die möglicherweise über ein kleineres Flash-Laufwerk verfügen.

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 kann erreicht werden, indem man das Skript `resize-image` verwendet.

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. HINWEIS: Es ist nicht möglich, die Größe der Partition zu verringern. Der eingegebene Wert muss größer als die aktuelle Partitionsgröße sein.
<code>resize-image --size <size></code>	Mit dieser Syntax, können Sie die Ziel-Partitionsgröße direkt als Parameter angeben und die Änderung anschließend bestätigen.
<code>resize-image --no-prompt</code> – oder – <code>resize-image --no-prompt --size <size></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. TIPP: 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 Benutzerdefiniertes Anpassen des Smart Zero-Anmeldebildschirms

Anpassen des Bildschirmhintergrunds

Dieser Abschnitt beschreibt die gängigen Attribute und Elemente, die bei der Anpassung des Bildschirmhintergrunds für die Client-Anmeldung verwendet werden.

Es gibt je ein Verzeichnis pro Verbindungstyp, sowie einen Standardstil, zur Angabe der Stilelemente für das Hintergrundbild und des Anmeldefenster-Formats der Verbindung.

In einem Stilverzeichnis legt die Datei **bgConfig.rtf** die Elemente auf dem Hintergrundfenster des Desktops fest. Die Syntax einer **bgConfig.rtf**-Datei weist ein Stylesheet-ähnliches Format mit einigen oder allen der im Folgenden beschriebenen Elemente auf. Jedes Element beginnt mit dem Elementtyp, auf den ein Attributsatz in geschweifter Klammer folgt. Zum Beispiel:

```
global {  
color: 666666; # Dark gray  
padding: 20; # 20 pixels }
```

Es kann eine beliebige Anzahl von Bild- oder Textelementen festgelegt werden. Bei Festlegung von Farbverläufen wird nur der letzte für die Farbe des Desktop-Hintergrunds verwendet; andernfalls wird die im globalen Abschnitt festgelegte Farbe verwendet. Jede Zeile, die mit einem Nummernzeichen „#“ beginnt, wird als Kommentar angesehen und ebenso ignoriert wie leere Zeilen. Text, der auf einen Strichpunkt folgt und mit „#“ beginnt, wird ebenfalls als Kommentar behandelt, wie die vorherigen Beispiele.

Jedem Element wird ein Satz von Attributen wie Größe, Farbe und Position zugeordnet. Jedes Attribut wird durch den Attributnamen spezifiziert, auf den ein Doppelpunkt, die Werte des Attributs und ein Strichpunkt in derselben Zeile folgen. Einige dieser Attribute sind für viele Elementtypen gleich.

Hierzu gehören:

- Gemeinsame Attribute
- Elemente
- Image
- Text

Gemeinsame Attribute

Tabelle D-1 Anmeldebildschirm > Gemeinsame Attribute > Name

Typ	Beschreibung
Parameter	Eine Zeichenfolge
Beispiel	name: itemName;

Tabelle D-1 Anmeldebildschirm > Gemeinsame Attribute > Name (Fortsetzung)

Typ	Beschreibung
Standard	
Verwendung	Legt eine dem Element zuzuordnende Zeichenfolge fest. Wird nur bei einer Debug-Ausgabe verwendet, wenn zum Beispiel ein Syntax- oder Wertfehler bei der Attributanalyse gefunden wird.

Tabelle D-2 Anmeldebildschirm > Gemeinsame Attribute > padding

Typ	Beschreibung
Parameter	ein absoluter (Pixel-) oder ein prozentueller Wert
Beispiel	padding: 20;
Standard	
Verwendung	Ein Objekt wird auf dem Bildschirm positioniert, als ob der Bildschirm auf allen Seiten um den Abstandswert kleiner wäre. Wenn zum Beispiel die Position eines Elements normalerweise bei 0,0 wäre, würde es bei einem Abstand von 20 stattdessen bei 20,20 angeordnet. Wird er im globalen Element festgelegt, gilt er für alle nachfolgenden Elemente und lässt einen leeren Bundsteg um den Bildschirmrand herum, sofern diese Elemente den Abstand nicht durch ihren eigenen Abstandswert außer Kraft setzen.

Tabelle D-3 Anmeldebildschirm > Gemeinsame Attribute > color

Typ	Beschreibung
Parameter	RRGGBB, 6-stelliger Hexadezimalwert oder Format rrr,ggg,bbb 0-255,0-255,0-255
Beispiel	color: ff8800;
Standard	255,255,255 (weiß)
Verwendung	Legt die Farbe des Elements fest.

Tabelle D-4 Anmeldebildschirm > Gemeinsame Attribute > alpha

Typ	Beschreibung
Parameter	Ganze Zahl zwischen 0 und 255
Beispiel	alpha: 127;
Standard	255 (vollständig deckend)
Verwendung	Legt die Deckkraft eines Elements fest. 255 ist vollständig deckend; 0 ist vollständig transparent; Die Elemente werden in der Reihenfolge, in der sie definiert sind, auf dem Hintergrund übereinander gelagert.

Tabelle D-5 Anmeldebildschirm > Gemeinsame Attribute > size

Typ	Beschreibung
Parameter	WWxHH, wobei WW die Breite in absoluten Pixel oder einem Prozentsatz der Bildschirmbreite und HH die Höhe in absoluten Pixel oder einem Prozentsatz der Bildschirmhöhe ist.
Beispiel	size: 256x128;
Standard	Die natürliche Größe des Elements; Wenn zum Beispiel die pixelgröße von einem Bild.
Verwendung	Legt die Größe des Elements fest. Die Elemente werden skaliert, um der festgelegten Größe zu entsprechen.

Tabelle D-6 Anmeldebildschirm > Gemeinsame Attribute > position

Typ	Beschreibung
Parameter	XX,YY wobei XX und YY Positionen in absoluten Pixeln oder in Prozenten der Bildschirmbreite und -höhe sind.
Beispiel	position: 50%,90%;
Standard	0,0 (oben links)
Verwendung	Legt die Position eines Elements fest. Siehe auch die Tabelle alignment (Ausrichtung).

Tabelle D-7 Anmeldebildschirm > Gemeinsame Attribute > alignment

Typ	Beschreibung
Parameter	[left hcenter right] [top vcenter bottom]
Beispiel	alignment: left bottom;
Standard	hcenter vcenter – das Element wird an der angegebenen Position zentriert.
Verwendung	Die Kombination von Position und Ausrichtung legt sowohl den Ankerpunkt für das Element als auch die Ausrichtung des Elements in Bezug auf diesen Ankerpunkt fest. Zum Beispiel wird bei einer Position von 90%,70% und der Ausrichtung „rechts unten“ das Element so positioniert, dass seine rechte Kante bei 90 % der Bildschirmbreite und seine obere Kante bei 70 % der Bildschirmhöhe ist.

Tabelle D-8 Anmeldebildschirm > Gemeinsame Attribute > context

Typ	Beschreibung
Parameter	[login desktop all]
Beispiel	context: login;

Tabelle D-8 Anmeldebildschirm > Gemeinsame Attribute > context (Fortsetzung)

Typ	Beschreibung
Standard	all
Verwendung	Legt fest, ob das Element nur auf dem Anmeldebildschirm für das Protokoll bzw. auf dem Desktopbildschirm für das Protokoll (wenn vorhanden) oder auf beiden angezeigt werden soll. Nur einige Protokolle (z. B. Citrix XenDesktop) haben einen Desktopbildschirm.

Elemente

Tabelle D-9 Anmeldebildschirm > Elemente > Benutzerdefiniert > Global

Typ	Beschreibung
Verwendung	Legt globale Hintergrund- oder Abstandswerte fest.
Erkannte gemeinsame Attribute:	name, color, padding <ul style="list-style-type: none"> color – legt die Volltonfarbe für den Hintergrund des Bildschirms fest, wenn keine Farbverläufe spezifiziert sind padding – legt den Standardabstand für alle nachfolgenden Elemente fest

Tabelle D-10 Anmeldebildschirm > Elemente > Benutzerdefiniert > Gradient

Typ	Beschreibung
Verwendung	Legt den Vollbildfarbverlauf zur Verwendung im Hintergrund fest.
Erkannte gemeinsame Attribute:	name, context

Tabelle D-11 Anmeldebildschirm > Elemente > Benutzerdefiniert > Type

Typ	Beschreibung
Parameter	Legt den Vollbildfarbverlauf zur Verwendung im Hintergrund fest.
Beispiel	Type: linear;
Standard	linear
Verwendung	Lineare Farbverläufe können entweder horizontal oder vertikal orientiert sein; die in den Farben angegebenen Koordinaten sind eine Bruchzahl der Breite oder Höhe. Radiale Farbverläufe werden in der Bildschirmmitte zentriert; die Koordinaten sind eine Bruchzahl der Distanz zum Bildschirmrand (oben und unten oder links und rechts).

Tabelle D-12 Anmeldebildschirm > Elemente > Benutzerdefiniert > Axis

Typ	Beschreibung
Parameter	[height width]
Beispiel	axis: width;
Standard	height
Verwendung	Für lineare Farbverläufe legt die Achse die Richtung des Farbverlaufs fest (von oben nach unten oder von links nach rechts). Für radiale Farbverläufe legt sie fest, ob der Radius des Farbverlaufs die halbe Bildschirmhöhe oder die halbe Bildschirmbreite ist.

Tabelle D-13 Anmeldebildschirm > Elemente > Benutzerdefiniert > Metric

Typ	Beschreibung
Parameter	[linear squared]
Beispiel	metric: linear;
Standard	squared
Verwendung	Für radiale Farbverläufe legt die Metrik fest, ob die Farbinterpolation zwischen Punkten anhand einer dx ² +dy ² -Distanzberechnung (quadratisch) oder der Quadratwurzel der Zahl (linear) erfolgt. Die quadratische Interpolation ist zum Zeichnen etwas schneller.

Tabelle D-14 Anmeldebildschirm > Elemente > Benutzerdefiniert > colors

Typ	Beschreibung
Parameter	Eine durch Leerzeichen getrennte Liste von [Wert,Farbe]-Paaren, wobei der Wert eine Fließkommabruhzahl 0,0-1,0 der Messachse ist (z. B. die Breite des Bildschirms in einem linearen Breite-Achse-Farbverlauf) und die Farbe eine Farbe des Farbverlaufs an diesem Punkt ist. Der Wert verläuft für vertikale lineare Farbverläufe von oben nach unten; für horizontale Farbverläufe von links nach rechts; und für radiale Farbverläufe von der Mitte zum Rand. Die Farben werden entweder in 6-stelligen Hexadezimalwerten oder drei durch Komma getrennte Werten zwischen 0 und 255 festgelegt.
Beispiel	colors: 0.0,000000 0.5,996600 0.9,255,255,255;
Standard	Nicht zutreffend
Verwendung	Die Farben werden entlang der linearen und der radialen Achse zwischen den festgelegten Punkten und Farben interpoliert. Wenn keine Werte angegeben werden, wird davon ausgegangen, dass die Farben auf der Achse zwischen 0,0 und 1,0 gleichmäßig beabstandet sind. Wenn der erste Bruchwert größer als 0,0 ist, wird die erste Farbe im Raum zwischen dem Bildschirmrand und dem ersten Wert verwendet. Gleichermaßen wird die letzte Farbe zwischen dem letzten Wert und dem Bildschirmrand verwendet, wenn der letzte Wert kleiner als 1,0 ist. Die Werte

Tabelle D-14 Anmeldebildschirm > Elemente > Benutzerdefiniert > colors (Fortsetzung)

Typ	Beschreibung
	müssen in aufsteigender Reihenfolge geordnet sein, obwohl ein Wert für einen scharfen Übergang wiederholt werden kann. Zum Beispiel würden „0.0,CCCCCC 0.5,EEEEEE 0.5,660000 1.0,330000“ in einem vertikalen linearen Farbverlauf einen Farbverlauf zwischen hellen Grautönen in der oberen Hälfte und dunklen Rottönen in der unteren Hälfte festlegen.

Tabelle D-15 Anmeldebildschirm > Elemente > Benutzerdefiniert > dithered

Typ	Beschreibung
Parameter	[true false]
Beispiel	dithered: true;
Standard	false
Verwendung	Wenn der Farbverlauf Anzeichen von Farbstreifenbildung zeigt, kann dieses visuelle Artefakt mit Dithering beseitigt werden. Dithering wird für radiale Farbverläufe mit der quadratischen Metrik nicht unterstützt.

Image

Tabelle D-16 Anmeldebildschirm > Image

Typ	Beschreibung
Verwendung	Legt ein Bild fest, das über einem Abschnitt des Hintergrunds einzublenden ist.
Erkannte gemeinsame Attribute:	name, size, alpha, position, alignment, context
Gemeinsame Attribute	Siehe die folgenden Tabellen.

Tabelle D-17 Anmeldebildschirm > Benutzerdefinierte Attribute > Source

Typ	Beschreibung
Parameter	Dateipfad
Beispiel	source: /writable/misc/Company_logo.png;
Standard	Nicht zutreffend
Verwendung	Legt den absoluten Pfadnamen für die Bilddatei fest. Es werden viele Formate unterstützt. darunter png, jpg oder gif. Das Bild kann transparente Bereiche aufweisen.

Tabelle D-18 Anmeldebildschirm > Benutzerdefinierte Attribute > Proportional

Typ	Beschreibung
Parameter	[true false]
Beispiel	proportional: false;
Standard	true
Verwendung	Wenn das Bild zum Erreichen der festgelegten Größe skaliert werden muss, wird bei true sein Seitenverhältnis beibehalten, um es innerhalb des spezifizierten Rechtecks einzupassen. Bei false erfolgt eine nichtproportionale Skalierung, damit das Bild genau der festgelegten Größe entspricht.

Text

Tabelle D-19 Anmeldebildschirm > Text

Typ	Beschreibung
Verwendung	Legt eine Textzeichenfolge fest, die über dem Hintergrund einzublenden ist.
Erkannte gemeinsame Attribute:	name, size, color, alpha, position, alignment, context
Gemeinsame Attribute	Siehe die Tabellen unten.

Tabelle D-20 Anmeldebildschirm > Text > text-locale

Typ	Beschreibung
Parameter	Lokalisierter Text
Beispiel	text-de_DE: Dieser Text ist in Deutsch.;
Standard	Nicht zutreffend
Verwendung	<p>Wenn der Text im übereinstimmenden Gebietschema ist, wird er für die Zeichenfolge verwendet. Die unterstützten Textzeichenfolgen lauten:</p> <ul style="list-style-type: none"> • de_DE (Deutsch) • en_US (Englisch) • es_ES (Spanisch) • fr_FR (Französisch) • ja_JP (Japanisch) • zh_CN (Vereinfachtes Chinesisch) <p>HINWEIS: Die Dateicodierung ist UTF-8.</p>

Tabelle D-21 Anmeldebildschirm > Text > text

Typ	Beschreibung
Parameter	Standard text text:
Beispiel	Wird auf dem Bildschirm angezeigt.;
Standard	Nicht zutreffend
Verwendung	Wenn kein übereinstimmender lokalisierter Text festgelegt wird, wird stattdessen diese Textzeichenfolge verwendet. HINWEIS: Die Textdarstellungsmaschine unterstützt kein Markup im HTML-Stil.

Tabelle D-22 Anmeldebildschirm > Text > font-locale

Typ	Beschreibung
Parameter	gebietsschemaspezifische Schriftart
Beispiel	font-ja_JP: kochi-gothic;
Standard	Nicht zutreffend
Verwendung	Wenn die Schriftart im übereinstimmenden Gebietsschema ist, wird sie bei der Darstellung der Zeichenfolge verwendet. Siehe vorstehende Beschreibung für Text-Gebietsschema. Der Name muss mit einer der Schriftarten unter /usr/share/fonts/truetype übereinstimmen. Für japanischen Text muss möglicherweise kochi-gothic ausgewählt werden; für Text in vereinfachtem Chinesisch: u mi ng.

Tabelle D-23 Anmeldebildschirm > Text > font

Typ	Beschreibung
Parameter	Schriftart
Beispiel	font: DejaVuSerif-Bold
Standard	; DejaVuSerif
Verwendung	Wenn keine übereinstimmende lokalisierte Schriftart festgelegt wird, wird stattdessen diese Schriftart verwendet. Der Name muss mit einer der Schriftarten unter /usr/share/fonts/truetype übereinstimmen.

Tabelle D-24 Anmeldebildschirm wird > Text > font-size

Typ	Beschreibung
Parameter	Pixel (z.B. 20) oder Prozente der Bildschirmhöhe (z.B. 5 %) oder Punkte (z.B. 12pt)
Beispiel	font-size: 12pt;

Tabelle D-24 Anmeldebildschirm > Text > font-size (Fortsetzung)

Typ	Beschreibung
Standard	Nicht zutreffend
Verwendung	Legt die Standardgröße der Schrift fest. Der Text kann weiter skaliert werden, wenn die Größe, die max. Breite und/oder die max. Höhe festgelegt werden.

Tabelle D-25 Anmeldebildschirm > Text > max-width

Typ	Beschreibung
Parameter	Größe in Pixeln oder in Prozenten der Bildschirmbreite
Beispiel	max-width: 90%;
Standard	Nicht zutreffend
Verwendung	Wenn die Zeichenfolge andernfalls größer als die angegebene Größe wäre, wird sie verkleinert, um innerhalb der festgelegten Breite eingepasst zu werden.

Tabelle D-26 Anmeldebildschirm > Text > max-height


Typ	Beschreibung
Parameter	Größe in Pixeln oder in Prozenten der Bildschirmhöhe
Beispiel	max-height: 64;
Standard	Nicht zutreffend
Verwendung	Wenn der Text andernfalls höher als die angegebene Größe wäre, wird er verkleinert, um der festgelegten zu Höhe zu entsprechen.

E Registrierungsschlüssel

Die Tabellen in diesem Anhang beschreiben die Pfade, Funktionen und Optionen für die Registrierungsschlüssel des HP ThinPro.

Die Einstellungen dieser Registrierungsschlüssel können auf zwei verschiedene Weisen geändert werden:

- Mithilfe der Komponente Registry Editor des Profile Editors und der anschließenden Bereitstellung des neuen Profils
- Mithilfe des Registry Editors in der Client-Benutzeroberfläche, der durch die Eingabe `regeditor` im X Terminal geöffnet wird.

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

Die Registrierungsschlüssel sind in die folgenden Überordner unterteilt:

- [root > Audio](#)
- [root > CertMgr](#)
- [root > ConnectionManager](#)
- [root > ConnectionType](#)
- [root > DHCP](#)
- [root > Dashboard](#)
- [root > Display](#)
- [root > Network](#)
- [root > SCIM](#)
- [root > Serial](#)
- [root > SystemInfo](#)
- [root > TaskMgr](#)
- [root > USB](#)
- [root > auto-update](#)
- [root > background](#)
- [root > config-wizard](#)
- [root > desktop](#)
- [root > entries](#)
- [root > keyboard](#)
- [root > logging](#)
- [root > mouse](#)

- [root > screensaver](#)
- [root > security](#)
- [root > sshd](#)
- [root > time](#)
- [root > touchscreen](#)
- [root > translation](#)
- [root > usb-update](#)
- [root > users](#)
- [root > vncserver](#)

root > Audio

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > Audio**.

Tabelle E-1 root > Audio

Registrierungsschlüssel	Beschreibung
root/Audio/AdjustSoundPath	Gibt den vollständigen Pfad zum Standard-Sound an, der ausgegeben wird, wenn die Wiedergabelautstärke über das Audiomixer-Bedienfeld oder die Taskleiste geändert wird. Standardmäßig ist dies ein Dreifach-Ping.
root/Audio/OutputMute	1 – Stummschalten der internen Lautsprecher und Kopfhörerbuchse. 0 – Nicht Stummschalten der internen Lautsprecher und Kopfhörerbuchse.
root/Audio/OutputScale	Gibt die Einstellung der Lautstärkeskalierung (1–400) für die internen Lautsprecher und Kopfhörerbuchse an.
root/Audio/OutputScaleAuto	Bei der Einstellung 1 (automatischer Modus) ist OutputScale für t610 und t610 PLUS auf 130, für t5565 und t510 auf 63 und für die gesamte übrige Hardware auf 100 eingestellt. 1 – Richtet den OutputScale-Wert gemäß dem Hardwaretyp ein. 0 – Stellt den OutputScale-Wert nicht gemäß dem Hardwaretyp ein.
root/Audio/OutputVolume	Zeigt die Lautstärkeeinstellung für den internen Lautsprecher und die Kopfhörerbuchse an, Skalierung von 1 bis 100.
root/Audio/PlaybackDevice	Gibt das für die Wiedergabe zu verwendende Gerät an. 1 ist der interne Audio-Controller. 2 und 3 sind für zusätzliche Geräte gedacht, z. B. ein USB-Headset.
root/Audio/RecordDevice	Gibt das für die Aufzeichnung zu verwendende Gerät an. 0 ist automatisch. 1 ist der interne Audio-Controller.

Tabelle E-1 root > Audio (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	2 und 3 sind für zusätzliche Geräte gedacht, z. B. ein USB-Headset.
root/Audio/RecordMute	1 – Stummschalten der Mikrofonbuchse. 0 – Nicht Stummschalten der Mikrofonbuchse.
root/Audio/RecordScale	Gibt die Einstellung der Lautstärkeskalierung (1–400) für die Mikrofonbuchse an.
root/Audio/RecordScaleAuto	Bei der Einstellung 1 (automatischer Modus) ist RecordScale auf 100 eingestellt. 1 – Richtet den RecordScale-Wert gemäß dem Hardwaretyp ein. 0 – Stellt den RecordScale-Wert nicht gemäß dem Hardwaretyp ein.
root/Audio/RecordVolume	Zeigt die Lautstärkeeinstellung für die Mikrofonbuchse an, Skalierung von 1 bis 100.
root/Audio/VisibleInSystray	Gibt an, ob ein Lautsprechersymbol in der Taskleiste sichtbar ist. 0 – Symbol ist nicht sichtbar 1 – Symbol ist sichtbar

root > CertMgr

Diese Kategorie wird intern verwendet und braucht keine benutzerdefinierten Einträge aufzuweisen.

root > ConnectionManager

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > ConnectionManager**.

Tabelle E-2 root > ConnectionManager

Registrierungsschlüssel	Beschreibung
root/ConnectionManager/customLogoPath	
root/ConnectionManager/defaultConnection	Dies muss auf eine gültige Verbindung mit dem Format "[type]:[label]" eingestellt sein, um beim Start eine Verbindung ordnungsgemäß starten zu können. Zum Beispiel: "xen:Default Connection"
root/ConnectionManager/minHeight	Die Standardeinstellung ist 260.
root/ConnectionManager/minWidth	Die Standardeinstellung ist 400.
root/ConnectionManager/splashLogoPath	Zeigt den vollständigen Pfad zum Standard-Image an, während eine Verbindung geladen wird. Dies ist der Startbildschirm, der angezeigt wird, nachdem Sie in der HP ThinPro-Systemsteuerung auf Connect (Verbinden) geklickt haben.

Tabelle E-2 root > ConnectionManager (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionManager/useKioskMode	
root/ConnectionManager/useSplashOnConnectionStartup	Standardmäßig ist diese Option für Smart Zero deaktiviert und für ThinPro aktiviert. Richten Sie dies auf 1 ein, damit das Bild für den Begrüßungsbildschirm, das unter "splashLogoPath" angegeben wurde, beim Verbindungsstart angezeigt wird.

root > ConnectionType

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen in den Ordnern **root > ConnectionType** wie folgt.

root > ConnectionType > custom

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > custom**.

Tabelle E-3 root > ConnectionType > custom

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/custom/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/custom/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung ausgeführt werden soll.
root/ConnectionType/custom/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/custom/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf 1 für Erlauben, 0 für Verweigerung des Zugriffs. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf 0 eingerichtet ist.
root/ConnectionType/custom/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung an. Einrichten auf 1 für Erlauben, 0 für Verweigerung des Zugriffs. HINWEIS: Diese Verbindung wird immer im Administratormodus zum Starten verfügbar sein.

Tabelle E-3 root > ConnectionType > custom (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/connections/{UUID}/autoReconnect	Bei der Einstellung auf 1 , wird die Verbindung neu gestartet, falls sie geschlossen oder getrennt ist. Dies ist häufig nützlich für Anwendungen im Kiosk-Stil. Bei der Einstellung auf 0 , wird die Verbindung nicht neu gestartet, falls sie geschlossen oder getrennt ist.
root/ConnectionType/custom/connections/{UUID}/autoReconnectDelay	Gibt die Zeit in Sekunden an, bevor die Verbindung neu gestartet wird. Der Standardwert von 0 wird die Verbindung sofort nach dem Schließen oder Trennen neu starten. Diese Einstellung ist nur wirksam, wenn "autoReconnect" auf 1 eingestellt ist.
root/ConnectionType/custom/connections/{UUID}/autostart	Bei der Einstellung auf 1 , wird die Verbindung automatisch beim Systemstart gestartet. Dies ist nützlich für Anwendungen im Kiosk-Stil. Standardmäßig werden Verbindungen nicht automatisch gestartet.
root/ConnectionType/custom/connections/{UUID}/autostartDelay	Gibt die Zeit in Sekunden an, bis die Verbindung beim Starten gestartet wird. Der Standardwert von 0 wird die Verbindung sofort beim Starten starten. Diese Einstellung ist nur wirksam, wenn "autostart" 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 realen auszuführenden Befehl für die benutzerdefinierte Verbindung an.
root/ConnectionType/custom/connections/{UUID}/connectionEndAction	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/custom/connections/{UUID}/coord	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/custom/connections/{UUID}/dependConnectionId	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/custom/connections/{UUID}/extraEnvValues/{UUID}/key	Gibt die zusätzliche Umgebungsvariable für eine benutzerdefinierte Verbindung an.
root/ConnectionType/custom/connections/{UUID}/extraEnvValues/{UUID}/value	Gibt den Wert der zusätzlichen Umgebungsvariablen für eine benutzerdefinierte Verbindung an.
root/ConnectionType/custom/connections/{UUID}/fallBackConnection	Bei der Einstellung auf die UUID einer anderen verfügbaren Verbindung, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Ausweichverbindung ist normalerweise aufzufinden, indem man "connection-mgr list" auf dem Client ausführt oder indem man zu <code>root/ConnectionType/<type>/connections/</code> navigiert. Dies kann in der Benutzeroberfläche der SSH-Verbindung eingestellt werden.
root/ConnectionType/custom/connections/{UUID}/hasDesktopIcon	Aktiviert oder deaktiviert das Desktop-Symbol für eine Telnet-Verbindung.
root/ConnectionType/custom/connections/{UUID}/label	Der Name der Verbindung. Für Smart Zero ist dies normalerweise auf "Default Connection" (Standardverbindung) eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/custom/connections/{UUID}/startMode	Wenn die Standardeinstellung Fokus lautet und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung mit dem

Tabelle E-3 root > ConnectionType > custom (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Hinweis zurückgegeben, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/custom/connections/{UUID}/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf einem langsamen Netzwerk die Verbindung so lange nicht gestartet wird, bis das Netzwerk verfügbar ist, und somit keine Probleme auftreten.
root/ConnectionType/custom/coreSettings/appName	Der interne Name der Anwendung, der zum Nachverfolgen der PID verwendet wird, um den Verbindungsstatus zu überwachen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/className	Der interne Klassenname der X-Windows Anwendung, der verwendet wird, wenn die PID der Verbindung für die Statusüberwachung nachverfolgt wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/editor	Der interne Name der Anwendung, der verwendet wird, wenn der Verbindungseditor für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der verwendet wird, wenn der Editor für die allgemeinen Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/icon16Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 16x16 Pixel für diese Anwendung. Dieses Symbol ist das kleine Symbol links neben dem Namen für die Verbindung im Verbindungsdialog.
root/ConnectionType/custom/coreSettings/icon32Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 32x32 Pixel für diese Anwendung.
root/ConnectionType/custom/coreSettings/icon48Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 48x48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/custom/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/custom/coreSettings/serverRequired	Gibt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/custom/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection_mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist diese close . Damit wird ein Standard-Kill-Signal an den Vorgang gesendet. Bei der Einstellung auf kill wird der von "appName" angegebene Prozess zwangsweise geschlossen. Bei der Einstellung auf custom wird ein vom "wrapperScript" angegebene, benutzerdefiniertes Ausführungsskript ausgeführt, das mit dem Argument "stop" den Prozess beendet.
root/ConnectionType/custom/coreSettings/watchPid	Wenn auf 1 eingestellt, wird die durch den "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.

Tabelle E-3 root > ConnectionType > custom (Fortsetzung)

Registrierungsschlüssel	Beschreibung
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	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/gui/CustomManager/status	Der aktive Status der Einstellungseditor für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/gui/CustomManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/gui/CustomManager/widgets/ autoReconnect	Zum Einstellen des Status für das Widget Auto reconnect (Automatische Neuverbindung) im Custom Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/ autostart	Zum Einstellen des Status für das Widget Auto start priority (Autostart-Priorität) im Custom Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/ command	Zum Einstellen des Status für das Widget Enter command to run (Auszuführenden Befehl eingeben) im Custom Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/ fallBackConnection	Zum Einstellen des Status für das Widget Fallback Connection (Ausweichverbindung) im Custom Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/ hasDesktopIcon	Zum Einstellen des Status für das Widget Show icon on desktop (Symbol auf Desktop anzeigen) im Custom Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/ label	Zum Einstellen des Status für das Widget Name im Custom Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der

Tabelle E-3 root > ConnectionType > custom (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/custom/gui/CustomManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Wait for network before connection (Auf Netzwerk warten vor Verbindungsaufbau) im Custom Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.

root > ConnectionType > firefox

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > firefox**.

Tabelle E-4 root > ConnectionType > firefox

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/firefox/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/firefox/connections/{UUID}/address	Die IP oder der Hostname des Remote-Hosts, zu dem die Verbindung hergestellt werden soll.
root/ConnectionType/firefox/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung ausgeführt werden soll.
root/ConnectionType/firefox/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/firefox/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf 0 eingestellt ist.
root/ConnectionType/firefox/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung hat. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.

Tabelle E-4 root > ConnectionType > firefox (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	HINWEIS: Die Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/firefox/connections/{UUID}/autoReconnect	Bei Einstellung auf den Wert 1 wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde. Dies ist häufig nützlich für Anwendungen im Kiosk-Stil. Bei Einstellung auf den Wert 0 wird die Verbindung nicht neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/firefox/connections/{UUID}/autoReconnectDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Beenden oder Trennen neu gestartet. Diese Einstellung wird nur wirksam, wenn "autoReconnect" auf 1 eingestellt ist.
root/ConnectionType/firefox/connections/{UUID}/autostart	Bei Einstellung auf den Wert 1 wird die Verbindung automatisch beim Systemstart gestartet. Dies ist nützlich für Anwendungen im Kiosk-Stil. Standardmäßig werden Verbindungen nicht automatisch gestartet.
root/ConnectionType/firefox/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 "autostart" auf 1 eingestellt ist.
root/ConnectionType/firefox/connections/{UUID}/beforeStartingCommand	Der Befehl zu starten, bevor die Verbindung gestartet wird.
root/ConnectionType/firefox/connections/{UUID}/connectionEndAction	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/firefox/connections/{UUID}/coord	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/firefox/connections/{UUID}/dependConnectionId	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/firefox/connections/{UUID}/enablePrintDialog	Zeigt an, ob der Benutzer die Erlaubnis hat, den Dialog Drucken des Webbrowsers zu verwenden.
root/ConnectionType/firefox/connections/{UUID} / extraEnvValues/{UUID}/key	Die zusätzliche Umgebungsvariable für die Verbindung.
root/ConnectionType/firefox/connections/{UUID} / extraEnvValues/{UUID}/value	Der zusätzliche Umgebungsvariablen-Wert für die Verbindung.
root/ConnectionType/firefox/connections/{UUID}/fallBackConnection	Bei der Einstellung auf die UUID einer anderen verfügbaren Verbindung, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Ausweichverbindung ist normalerweise aufzufinden, indem man "Connection-mgr List" auf dem Client ausführt oder indem man zu root/ConnectionType/<type>/connections/ navigiert.
root/ConnectionType/firefox/connections/{UUID}/fullscreen	Ermöglicht dem Web Browser im Vollbildmodus zu starten.
root/ConnectionType/firefox/connections/{UUID}/hasDesktopIcon	Bei Einstellung des Werts auf 1 wird ein Symbol für die Verbindung auf dem Desktop angezeigt. Nicht zutreffend für Smart Zero.
root/ConnectionType/firefox/connections/{UUID}/kioskMode	Aktiviert den Kioskmodus des Web Browsers.

Tabelle E-4 root > ConnectionType > firefox (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/connections/{UUID}/label	Der Name der Verbindung. Für Smart Zero ist dies normalerweise auf "Default Connection" (Standardverbindung) eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/firefox/connections/{UUID}/startMode	Wenn die Standardeinstellung focus 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/appName	Der interne Name der Anwendung zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/className	Der interne X-Windows Anwendungs-Klassenname zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/editor	Der interne Name der Anwendung, der zum Starten des Verbindungseditors für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der zum Starten des Editors für allgemeine Einstellungen für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/coreSettings/icon16Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 16 x 16 Pixel für diese Anwendung. Dieses Symbol ist das kleine Symbol links neben dem Verbindungsnamen im Verbindungsdialog.
root/ConnectionType/firefox/coreSettings/icon32Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 32 x 32 Pixel für diese Anwendung.
root/ConnectionType/firefox/coreSettings/icon48Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 48 x 48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungseditors für diesen Verbindungstyp.
root/ConnectionType/firefox/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlm Menü der Verbindungstypen angezeigt wird.
root/ConnectionType/firefox/coreSettings/restartIdleTime	Die Leerlauf-Zeit in Minuten, bevor der Browser neu gestartet wird. Bei Einstellung des Standardwerts 0 ist der Neustart nicht aktiviert.
root/ConnectionType/firefox/coreSettings/serverRequired	Zeigt an, ob ein Servername oder eine Serveradresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/firefox/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist dies close , wodurch ein standardmäßiges Abbrechen-

Tabelle E-4 root > ConnectionType > firefox (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Signal an den Vorgang gesendet wird. Wenn kill eingestellt ist, wird der durch den "appName" angegebene Prozess zum Abbruch gezwungen. Wenn custom eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch "wrapperScript", mit dem Argument "stop" ausgeführt, um den Prozess 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	Behält die Einstellungen des Benutzers nach jeder Sitzung bei.
root/ConnectionType/firefox/gui/FirefoxManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/gui/FirefoxManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/gui/FirefoxManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Zum Einstellen des Status für das Widget URL im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Auto reconnect (Automatische Neuverbindung) im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart	Zum Einstellen des Status für das Widget Auto start priority (Autostart-Priorität) im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog	Zum Einstellen des Status für das Widget Enable print dialog (Dialogfeld Drucken aktivieren) im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget Fallback Connection (Ausweichverbindung) im Web Browser Connection Manager. Durch die Einstellung active wird das

Tabelle E-4 root > ConnectionType > firefox (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Show icon on desktop (Symbol auf Desktop anzeigen) im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/kioskMode	Zum Einstellen des Status für das Widget Enable kiosk mode (Kioskmodus aktivieren) im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/label	Zum Einstellen des Status für das Widget Name im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/startMode	Dieser Schlüssel hat keine Funktion.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Wait for network before connection (Auf Netzwerk warten vor Verbindungsaufbau) im Web Browser Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.

root > ConnectionType > freerdp

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > freerdp**.

Tabelle E-5 root > ConnectionType > freerdp

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/freerdp/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/freerdp/connections/{UUID}/ExtraArgs	Zusätzliche Argumente zum Xfreerdp-Client angeben. Führen Sie "xfreerdp —help" über ein Terminal aus, um alle verfügbaren Argumente zu sehen.
root/ConnectionType/freerdp/connections/{UUID}/SingleSignOn	
root/ConnectionType/freerdp/connections/{UUID}/address	Die IP oder der Hostname des Remote-Hosts, zu dem die Verbindung hergestellt werden soll.
root/ConnectionType/freerdp/connections/{UUID}/application	Gibt eine alternativ zu verwendende Shell an. Dabei kann es sich auch um den Namen einer verfügbaren Anwendung handeln.
root/ConnectionType/freerdp/connections/{UUID}/attachToConsole	
root/ConnectionType/freerdp/connections/{UUID}/audioLatency	Der durchschnittliche Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln.
root/ConnectionType/freerdp/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf 1 für Erlauben, 0 für Verweigerung des Zugriffs. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf 0 eingestellt ist.
root/ConnectionType/freerdp/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung an. Einrichten auf 1 für Erlauben, 0 für Verweigerung des Zugriffs. HINWEIS: Diese Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/freerdp/connections/{UUID}/autoReconnect	Bei der Einstellung auf 1 , wird die Verbindung neu gestartet, falls sie geschlossen oder getrennt ist. Dies ist häufig nützlich für Anwendungen im Kiosk-Stil. Bei der Einstellung auf 0 , wird die Verbindung nicht neu gestartet, falls sie geschlossen oder getrennt ist.
root/ConnectionType/freerdp/connections/{UUID}/autoReconnectDelay	Gibt die Zeit in Sekunden an, bevor die Verbindung neu gestartet wird. Der Standardwert von 0 wird die Verbindung sofort nach dem Schließen oder Trennen neu starten. Diese Einstellung ist nur wirksam, wenn "autoReconnect" auf 1 eingestellt ist.
root/ConnectionType/freerdp/connections/{UUID}/autostart	Bei der Einstellung auf 1 , wird die Verbindung automatisch beim Systemstart gestartet. Dies ist nützlich für Anwendungen im Kiosk-Stil. Standardmäßig werden Verbindungen nicht automatisch gestartet.
root/ConnectionType/freerdp/connections/{UUID}/autostartDelay	Gibt die Zeit in Sekunden an, bis die Verbindung beim Starten gestartet wird. Der Standardwert von 0 wird die Verbindung sofort beim Starten starten. Diese Einstellung ist nur wirksam, wenn "autostart" auf 1 eingestellt ist.

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/{UUID}/certificateCheck	Bei der Einstellung auf den Standardwert 1 werden Zertifikate geprüft. Bei der Einstellung auf 0 werden Zertifikate ignoriert.
root/ConnectionType/freerdp/connections/{UUID}/clipboardExtension	Wenn der Standardwert 0 eingestellt ist, ist die RDP-Zwischenablage-Funktionen der Intersitzung deaktiviert. Bei Einstellung des Werts auf 1 ist die Zwischenablage sowohl zwischen RDP-Sitzungen als auch RDP-Sitzungen und dem lokalen System aktiviert.
root/ConnectionType/freerdp/connections/{UUID}/compression	Bei Einstellung des Werts auf 1 ist die Komprimierung von RDP-Daten zwischen dem Client und Server aktiviert. Die Einstellung 0 deaktiviert die Komprimierung. Die Komprimierung ist standardmäßig aktiviert.
root/ConnectionType/freerdp/connections/{UUID}/dependConnectionId	
root/ConnectionType/freerdp/connections/{UUID}/directory	Gibt das Systemstart-Verzeichnis an, in dem eine alternative Shell-Anwendung ausgeführt werden soll.
root/ConnectionType/freerdp/connections/{UUID}/disableMMRwithRFX	Wenn die Einstellung nicht 0 ist, wird die Multimedia-Umleitung deaktiviert, falls eine gültige RemoteFX-Sitzung aufgebaut wurde.
root/ConnectionType/freerdp/connections/{UUID}/domain	Die Standarddomäne zur Versorgung des Remote-Host während der Anmeldung. Wenn eine Domäne nicht angegeben ist, wird die Standard-Domäne für den Remote-Host verwendet.
root/ConnectionType/freerdp/connections/{UUID}/extraEnvValues/{UUID}/key	
root/ConnectionType/freerdp/connections/{UUID}/extraEnvValues/{UUID}/value	
root/ConnectionType/freerdp/connections/{UUID}/fallBackConnection	Wenn die Einstellung auf die UUID einer anderen verfügbaren UUID-Verbindung erfolgte, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Fallback-Verbindung finden Sie normalerweise durch Ausführen von "connection-mgr list" auf dem Client oder indem Sie zu <code>root/ConnectionType/<type>/connections/</code> navigieren.
root/ConnectionType/freerdp/connections/{UUID}/frameAcknowledgeCount	Die Anzahl der Videoframes, die der Server pushen kann, ohne auf eine Bestätigung vom Client zu warten. Niedrigere Zahlen führen zu einem schneller reagierenden Desktop, jedoch einer niedrigen Bildfrequenz. Bei Einstellung des Werts auf 0 , wird die Frame-Bestätigung bei den Client-Server-Interaktionen nicht verwendet.
root/ConnectionType/freerdp/connections/{UUID}/gatewayAddress	Identifiziert den RD-Gateway-Servernamen oder die Adresse.
root/ConnectionType/freerdp/connections/{UUID}/gatewayDomain	Gibt die Standarddomäne an, die das Gateway während der Anmeldung benötigt. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn "GatewayUsesSameCredentials" auf 1 eingestellt ist, wird dieser Wert deaktiviert.

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
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 "GatewayUsesSameCredentials" 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 "GatewayUsesSameCredentials" auf 1 eingestellt ist, wird dieser Wert deaktiviert.
root/ConnectionType/freerdp/connections/{UUID}/gatewayUsesSameCredentials	Bei Einstellung des Werts auf 1 verwendet das Gerät zur Herstellung einer Verbindung zum Gateway dieselben Anmeldeinformationen, die auch zur Verbindung mit dem endgültigen Server verwendet werden.
root/ConnectionType/freerdp/connections/{UUID}/hasDesktopIcon	Bei Einstellung des Werts auf 1 wird ein Symbol für die Verbindung auf dem Desktop angezeigt. Nicht zutreffend für Smart Zero.
root/ConnectionType/freerdp/connections/{UUID}/label	Der Name der Verbindung im Kontrollzentrum. Für Smart Zero ist dies normalerweise auf "Default Connection" (Standardverbindung) eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/freerdp/connections/{UUID}/localPartitionRedirection	Bei Einstellung des Werts auf 0 ist die Speichererweiterung für lokale nicht-USB-Speicherpartitionen – andere als die von HP ThinPro verwendeten – deaktiviert. Bei Einstellung des Werts auf 1 werden die lokalen nicht-USB-Speicherpartitionen über die Speichererweiterung in der RDP-Verbindung umgeleitet.
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.
root/ConnectionType/freerdp/connections/{UUID}/offScreenBitmaps	Bei der Einstellung auf 0 werden Off-Screen-Bitmaps deaktiviert. Dies kann die Leistung etwas erhöhen, wird aber dazu führen, dass Blocks des Bildschirms asynchron aktualisiert werden, wodurch Übergänge nicht gleichmäßig aktualisiert werden.
root/ConnectionType/freerdp/connections/{UUID}/password	Das Standardkennwort, das der Remote-Host während der Anmeldung benötigt. Dieser Wert wird verschlüsselt gespeichert. 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	Bei Einstellung des Werts auf 1 wird die Desktopkomposition erlaubt, wie durchscheinende Rahmen, falls vom Server

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	unterstützt. Wenn Sie es ausschalten, könnte dies die Leistung für Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagFontSmoothing	Bei Einstellung des Werts auf 1 wird die Schriftglättungsfunktion erlaubt, wenn dies vom Server unterstützt wird und aktiviert ist. Wenn Sie es ausschalten, könnte dies die Leistung für Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoCursorSettings	Falls der Wert auf 1 eingerichtet ist, ist das Blinken des Cursors deaktiviert. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoCursorShadow	Bei Einstellung des Werts auf 1 werden dadurch die Mauszeigerschatten ausgeschaltet. Dies kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoMenuAnimations	Bei Einstellung des Werts auf 1 werden die Menüanimationen ausgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoTheming	Bei Einstellung des Werts auf 1 werden die Themen der Benutzeroberfläche abgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWallpaper	Bei Einstellung des Werts auf 1 werden die Desktop-Hintergrundbilder abgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/freerdp/connections/{UUID}/perfFlagNoWindowDrag	Bei Einstellung des Werts auf 1 wird das Ziehen des vollständigen Fensters abgeschaltet. Dies kann die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessern. Statt dessen werden die Fensterumrisse verwendet.
root/ConnectionType/freerdp/connections/{UUID}/port	Die Portnummer, die zum Kontaktieren des RDP-Servers zu verwenden ist. Standardmäßig ist diese Option auf 3389 eingerichtet und muss nur selten geändert werden.
root/ConnectionType/freerdp/connections/{UUID}/portMapping	Bei Einstellung des Werts auf 1 werden die folgenden lokalen seriellen und parallelen Anschlüsse zum Remote-Host umgeleitet: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/freerdp/connections/{UUID}/printerMapping	Bei Einstellung des Werts auf 1 wird das Umleitungs-Plugin für CUPS-Drucker aktiviert, wodurch alle Drucker lokal über CUPS definiert werden, um an den Remote-Host weitergeleitet zu werden.
root/ConnectionType/freerdp/connections/{UUID}/rdpEncryption	Bei Einstellung des Werts auf 1 wird die Standard-RDP-Verschlüsselung zum Verschlüsseln aller Daten zwischen dem Client und dem Server verwendet.
root/ConnectionType/freerdp/connections/{UUID}/remoteApp	Gibt den Namen einer verfügbaren Anwendung an, die im Modus RemoteApp oder RAIL ausgeführt werden soll.
root/ConnectionType/freerdp/connections/{UUID}/remoteFx	Verwenden Sie RemoteFX, falls verfügbar.
root/ConnectionType/freerdp/connections/{UUID}/seamlessWindow	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.

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/{UUID}/securityLevel	
root/ConnectionType/freerdp/connections/{UUID}/sendHostname	<p>Der angegebene Text wird als Client-Hostname zum Remote-Host gesendet. Wenn das Feld leer bleibt, wird der System-Hostname an den Hostnamen gesendet.</p> <p>HINWEIS: Der Schlüssel für allgemeine Einstellungen 'root/ConnectionType/freerdp/coreSettings/sendHostname' muss für diesen Schlüssel zur Verwendung auf 'hostname' eingestellt sein.</p>
root/ConnectionType/freerdp/connections/{UUID}/smartcard	Bei Einstellung des Werts auf 1 wird die lokale Smart Card-Authentifizierung auf dem Remote-Host erlaubt. Dadurch wird die NLA (Network Level Authentication) deaktiviert.
root/ConnectionType/freerdp/connections/{UUID}/sound	<p>Durch die Einstellung 0 wird die Audio-Umleitung deaktiviert. Durch die Einstellung 1 werden die Wiedergabe- und Aufnahmegeräte zur RDP-Verbindung umgeleitet. Durch die Einstellung 2 werden USB-Audiogeräte entsprechend der Angaben im USB-Manager weitergeleitet.</p> <p>HP empfiehlt die Einstellung dieses Werts auf 1, sodass USB-Audiogeräte nicht zum Host umgeleitet werden. Dadurch wird die Audioqualität verbessert und sichergestellt, dass Client-Audio, das mittels anderer Methoden umgeleitet wird (wie zum Beispiel Multimedia-Umleitung), den lokalen Audioeinstellungen entspricht.</p>
root/ConnectionType/freerdp/connections/{UUID}/startMode	Wenn die Standardeinstellung Fokus lautet und die Verbindung bereits gestartet wurde, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung mit dem Hinweis zurückgegeben, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/freerdp/connections/{UUID}/timeoutError	Die gewünschte Anzahl von Millisekunden, die nach dem Verlust einer Verbindung mit dem Server gewartet wird, bevor Ihnen der Server ein Dialogfeld mit einer Fehlermeldung anzeigt und die Verbindung schließt. Deaktiviert, wenn 0 ausgewählt ist.
root/ConnectionType/freerdp/connections/{UUID}/timeoutRecovery	Die Anzahl von Millisekunden, 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	Die Anzahl von Millisekunden, die nach dem Ausfall einer Verbindung mit dem Server vergehen, bevor der Benutzer gewarnt wird, dass die Verbindung getrennt wurde. Ist bei Einstellung auf 0 deaktiviert.
root/ConnectionType/freerdp/connections/{UUID}/usbMiscRedirection	Bei Einstellung des Werts auf 0 ist die Umleitung für alle USB-Geräte deaktiviert, ausgenommen jener, die über sound, printerMapping, portMapping, usbStorageRedirection und localPartitionRedirection gehandhabt werden. Bei Einstellung des Werts auf 2 werden alle anderen USB-Geräte in der RDP-Verbindung dem USB-Manager entsprechend umgeleitet.
root/ConnectionType/freerdp/connections/{UUID}/usbStorageRedirection	Bei Einstellung des Werts auf 0 ist die Speichererweiterung für die USB-Speichergeräte deaktiviert. Bei Einstellung des Werts auf 1 werden die USB-Speichergeräte in der RDP-Verbindung der Speichererweiterung entsprechend

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	umgeleitet. Bei Einstellung des Werts auf 2 werden USB-Speichergeräte in der RDP-Verbindung dem USB-Manager entsprechend umgeleitet.
root/ConnectionType/freerdp/connections/{UUID}/username	Der Standard-Benutzername, 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/freerdp/connections/{UUID}/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf einem langsamen Netzwerk die Verbindung so lange nicht gestartet wird, bis das Netzwerk verfügbar ist, und somit keine Probleme auftreten.
root/ConnectionType/freerdp/connections/{UUID}/windowMode	Bei der Einstellung auf Remote-Anwendung wird RDP im RAIL-Modus (Remote Application Integrated Locally) ausgeführt. Dafür muss der Remote-Anwendungsserver die Ausführung einer benannten Anwendung als Remote-Anwendung zulassen. Die Anwendung wird in einem eigenen Fenster in der Desktop-Umgebung angezeigt, sodass es wirkt, als wäre die Anwendung ein Teil der lokalen Umgebung. Siehe Einstellung remoteApp. Falls der Wert auf Alternative Shell eingerichtet ist, wird der Aufruf einer nicht standardmäßigen Shell zugelassen. Siehe Anwendungs- und Verzeichniseinstellungen.
root/ConnectionType/freerdp/connections/{UUID}/windowSizeHeight	
root/ConnectionType/freerdp/connections/{UUID}/windowSizePercentage	
root/ConnectionType/freerdp/connections/{UUID}/windowSizeWidth	
root/ConnectionType/freerdp/connections/{UUID}/windowType	
root/ConnectionType/freerdp/connections/{UUID}/xkbLayoutId	Wenn nicht leer, geben Sie eine XKB-Layout-ID an, um die System-Tastatur zu umgehen. Um Zugriff auf die Liste der verfügbaren IDs zu erhalten, geben Sie Folgendes in ein Terminal ein: <code>xfreerdp --kbd-list</code> .
root/ConnectionType/freerdp/coreSettings/appName	Der interne Name der Anwendung, der zum Nachverfolgen der PID verwendet wird, um den Verbindungsstatus zu überwachen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/className	Der interne Klassenname der X-Windows Anwendung, der verwendet wird, wenn die PID der Verbindung für die Statusüberwachung nachverfolgt wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning	Bei Einstellung des Werts auf 1 muss Zero-Login keinen Dialog ausführen, wenn ein Networklink getrennt wird, da das Protokoll solche Situationen bearbeitet.
root/ConnectionType/freerdp/coreSettings/editor	Der interne Name der Anwendung, der verwendet wird, wenn der Verbindungseditor für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der verwendet wird, wenn der Editor für die allgemeinen Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/icon16Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 16x16 Pixel für diese Anwendung. Dieses Symbol ist das kleine Symbol links neben dem Namen für die Verbindung im Verbindungsdialog.
root/ConnectionType/freerdp/coreSettings/icon32Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 32x32 Pixel für diese Anwendung.
root/ConnectionType/freerdp/coreSettings/icon48Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 48x48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	Die Anzahl der Sekunden, die auf eine erste Antwort vom RDP-Server gewartet wird, bis aufgegeben wird.
root/ConnectionType/freerdp/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/freerdp/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist diese close . Damit wird ein Standard-Kill-Signal an den Vorgang gesendet. Bei der Einstellung auf kill wird der von "appName" angegebene Prozess zwangsweise geschlossen. Bei der Einstellung auf custom wird ein vom "wrapperScript" angegebenes, benutzerdefiniertes Ausführungsskript ausgeführt, das mit dem Argument "stop" den Prozess beendet.
root/ConnectionType/freerdp/coreSettings/watchPid	Bei Einstellung des Werts auf 1 wird die von "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/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 bearbeitet. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/general/autoReconnectDialogTimeout	Wenn "autoReconnect" aktiviert ist, ist dies die Anzahl der Sekunden, bevor Fehlerdialoge für die Verbindung ein Zeitlimit erreichen. Stellen Sie diesen Wert auf 0 ein, um unbegrenzt zu pausieren, bis eine Benutzerinteraktion erfolgt.
root/ConnectionType/freerdp/general/disablePasswordChange	Wenn eine Remote-Anmeldung aufgrund fehlerhafter Anmeldeinformationen fehlschlägt, wird dem Benutzer eine Schaltfläche angezeigt, die ein Dialogfeld öffnet, um das Kennwort zu aktualisieren. Bei Auswahl des Werts 1 werden die Schaltfläche und das Dialogfeld nicht angezeigt.
root/ConnectionType/freerdp/general/enableMMR	Bei Einstellung des Werts auf 1 wird das MMR-Plugin 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.

Tabelle E-5 root > ConnectionType > freerdp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/general/preferredAudio	Einstellen, um das Standard-Audio-Back-End, sowohl Ein- als auch Ausgang, für High-Level Audio-Umleitungen zu ändern.
root/ConnectionType/freerdp/general/sendHostname	Wenn der standardmäßige Hostname eingestellt ist, wird der System-Hostname an den Remote-Host gesendet. Dies wird in der Regel von einem Administrator verwendet, um den mit einer bestimmten RDP-Sitzung verknüpften Client-Rechner zu identifizieren. Der gesendete Hostname kann überschrieben werden, indem der Schlüssel "SendHostname" in den verbindungs-spezifischen Einstellungen angegeben wird. Bei der Einstellung mac wird die MAC-Adresse des ersten verfügbaren Netzwerkadapters anstelle des Hostnamen gesendet.
root/ConnectionType/freerdp/general/sttyInitialSettings	Identifiziert die Anfangseinstellungen der seriellen Ports, wie sie vom Stty-Tool festgelegt wurden.

root > ConnectionType > ssh

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > ssh**.

Tabelle E-6 root > ConnectionType > ssh

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/ssh/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/ssh/connections/{UUID}/address	Gibt die IP oder den Hostnamen des Remote-SSH-Hosts an, zu dem die Verbindung hergestellt werden soll. Diese Einstellung ist bei jeder Verbindung angegeben.
root/ConnectionType/ssh/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung ausgeführt werden soll.
root/ConnectionType/ssh/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/ssh/connections/{UUID}/application	Gibt die Anwendung an, die ausgeführt werden soll.
root/ConnectionType/ssh/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf 1 für Erlauben des Zugriffs, 0 zur Verweigerung des Zugriffs. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf 0 eingerichtet ist.

Tabelle E-6 root > ConnectionType > ssh (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung an. Einrichten auf 1 für Erlauben des Zugriffs, 0 zur Verweigerung des Zugriffs. HINWEIS: Diese Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/ssh/connections/{UUID}/autoReconnect	Bei Einstellung des Werts auf 1 wird das System versuchen, die Verbindung automatisch neu zu starten, nachdem sie geschlossen wurde. <code>Autostart</code> (Automatisch starten) wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/ssh/connections/{UUID}/autoReconnectDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Beenden oder Trennen neu gestartet. Diese Einstellung wird nur wirksam, wenn <code>autoReconnect</code> (Automatische Neuverbindung) auf 1 eingestellt ist.
root/ConnectionType/ssh/connections/{UUID}/autostart	Wenn der Wert größer als 0 ist, versucht das System, die Verbindung automatisch zu starten, wenn der Client hochgefahren wird. <code>AutoReconnect</code> (Automatische Neuverbindung) wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/ssh/connections/{UUID}/autostartDelay	Gibt die Zeit in Sekunden an, bis die Verbindung beim Starten gestartet wird. Der Standardwert von 0 wird die Verbindung sofort beim Starten starten. Diese Einstellung ist nur wirksam, wenn "autostart" auf 1 eingestellt ist.
root/ConnectionType/ssh/connections/{UUID}/backgroundColor	Gibt die Hintergrundfarbe für eine SSH-Verbindung an.
root/ConnectionType/ssh/connections/{UUID}/beforeStartingCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/ssh/connections/{UUID}/compression	Aktiviert die Komprimierung für eine SSH-Verbindung.
root/ConnectionType/ssh/connections/{UUID}/connectionEndAction	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/ssh/connections/{UUID}/coord	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/ssh/connections/{UUID}/dependConnectionId	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/ssh/connections/{UUID}/extraEnvValues/{UUID}/key	Die zusätzliche Umgebungsvariable für eine SSH-Verbindung.
root/ConnectionType/ssh/connections/{UUID}/extraEnvValues/{UUID}/value	Der zusätzliche Umgebungsvariablen-Wert für eine SSH-Verbindung.
root/ConnectionType/ssh/connections/{UUID}/fallBackConnection	Wenn die Einstellung auf die UUID einer anderen verfügbaren UUID-Verbindung erfolgte, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Fallback-Verbindung finden Sie normalerweise durch Ausführen von "connection-mgr list" auf dem Client oder indem Sie zu <code>root/ConnectionType/<Type>/connections/</code> navigieren.
root/ConnectionType/ssh/connections/{UUID}/font	Gibt die Schriftgröße für eine SSH-Verbindung an.

Tabelle E-6 root > ConnectionType > ssh (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/connections/{UUID}/foregroundColor	Gibt die Vordergrundfarbe für eine SSH-Verbindung an.
root/ConnectionType/ssh/connections/{UUID}/fork	Aktiviert das Verschieben eines Prozesses in den Hintergrund für eine SSH-Verbindung.
root/ConnectionType/ssh/connections/{UUID}/hasDesktopIcon	Aktiviert das Desktop-Symbol für eine SSH-Verbindung.
root/ConnectionType/ssh/connections/{UUID}/isInMenu	Dieser Schlüssel ist reserviert und nicht funktionsfähig.
root/ConnectionType/ssh/connections/{UUID}/label	Der Name der Verbindung. Dies wird von 'root/ConnectionManager/defaultConnection' verwendet, um anzugeben, welche Verbindung sowohl beim Systemstart als auch im Connection Manager gestartet wird.
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 focus 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	Aktiviert die TTY-Zuordnung, die für eine SSH-Verbindung erzwungen wird.
root/ConnectionType/ssh/connections/{UUID}/username	Gibt den Standard-Benutzernamen an, den der Remote-Host während der Anmeldung benötigt.
root/ConnectionType/ssh/connections/{UUID}/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf einem langsamen Netzwerk die Verbindung so lange nicht gestartet wird, bis das Netzwerk verfügbar ist, und somit keine Probleme auftreten.
root/ConnectionType/ssh/connections/{UUID}/x11	Aktiviert die X11-Weiterleitung für eine SSH-Verbindung.
root/ConnectionType/ssh/coreSettings/appName	Der interne Name der Anwendung zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/coreSettings/className	Der interne X-Windows Anwendungs-Klassenname zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/coreSettings/editor	Der interne Name der Anwendung, der verwendet wird, wenn der Verbindungseditor für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/coreSettings/icon16Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 16x16 Pixel für diese Anwendung. Dies ist das kleine Symbol links neben dem Namen für die Verbindung in der connection Dialog.
root/ConnectionType/ssh/coreSettings/icon32Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 32x32 Pixel für diese Anwendung.

Tabelle E-6 root > ConnectionType > ssh (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/coreSettings/icon48Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 48x48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/ssh/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/ssh/coreSettings/serverRequired	Gibt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/ssh/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection_mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist diese close . Damit wird ein Standard-Kill-Signal an den Vorgang gesendet. Bei der Einstellung auf kill wird der von "appName" angegebene Prozess zwangsweise geschlossen. Bei der Einstellung auf custom wird ein benutzerdefiniertes Ausführungsskript (angegeben durch "wrapperscript") mit dem Argument "stop" ausgeführt, um den Prozess sanft zu beenden.
root/ConnectionType/ssh/coreSettings/watchPid	Bei Einstellung des Werts auf 1 wird die von "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/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 bearbeitet. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/gui/SshManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/gui/SshManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/gui/SshManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/gui/SshManager/widgets/address	Zum Einstellen des Status für das Widget Address (Adresse) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/application	Zum Einstellen des Status für das Widget Run application (Anwendung ausführen) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Auto reconnect (Automatische Neuverbindung) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit

Tabelle E-6 root > ConnectionType > ssh (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/autostart	Zum Einstellen des Status für das Widget Auto start priority (Autostart-Priorität) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor	Zum Einstellen des Status für das Widget Background color (Hintergrundfarbe) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/compression	Zum Einstellen des Status für das Widget Compression (Komprimierung) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget Fallback Connection (Ausweichverbindung) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/font	Zum Einstellen des Status für das Widget Font (Schriftart) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/foregroundColor	Zum Einstellen des Status für das Widget Foreground color (Vordergrundfarbe) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/fork	Zum Einstellen des Status für das Widget Fork into background (In den Hintergrund verschieben) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.

Tabelle E-6 root > ConnectionType > ssh (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/gui/SshManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Show icon on desktop (Symbol auf Desktop anzeigen) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/isInMenu	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/ssh/gui/SshManager/widgets/label	Zum Einstellen des Status für das Widget Name im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/port	Zum Einstellen des Status für das Widget Port im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/tty	Zum Einstellen des Status für das Widget Force TTY allocation (TTY-Zuweisung erzwingen) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/username	Zum Einstellen des Status für das Widget User name (Benutzername) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Wait for network before connection (Auf Netzwerk warten vor Verbindungsaufbau) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/ssh/gui/SshManager/widgets/x11	Zum Einstellen des Status für das Widget X11 connection forwarding (X11-Verbindungsweiterleitung) im Secure Shell Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.

root > ConnectionType > teemtalk

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > teemtalk**.

Tabelle E-7 root > ConnectionType > teemtalk

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/teemtalk/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/teemtalk/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Auf '1' einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, selbst wenn dieser Schlüssel auf '0' eingestellt ist.
root/ConnectionType/teemtalk/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung hat. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/teemtalk/connections/{UUID}/autoReconnect	Wenn 1 eingestellt ist, wird das System automatisch versuchen, die Verbindung neu zu starten, nachdem sie geschlossen wurde. Falls erforderlich, sollten über das Feld <code>zero-login/defaultCredentials</code> die Anmeldeinformationen bereitgestellt werden. "autostart" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/teemtalk/connections/{UUID}/autostart	Wenn die Einstellung größer als 0 ist, versucht das System die Verbindung automatisch zu starten, wenn der Client hochgefahren wird. Falls erforderlich, sollten über das Feld <code>zero-login/defaultCredentials</code> die Anmeldeinformationen bereitgestellt werden. "autoReconnect" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/teemtalk/connections/{UUID}/beforeStartingCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/teemtalk/connections/{UUID}/connectionEndAction	Dieser Schlüssel ist zur Verwendung reserviert.

Tabelle E-7 root > ConnectionType > teemtalk (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/connections/{UUID}/coord	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/teemtalk/connections/{UUID}/dependConnectionId	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/teemtalk/connections/{UUID}/extraEnvValues/{UUID}/key	Die zusätzliche Umgebungsvariable für die Verbindung.
root/ConnectionType/teemtalk/connections/{UUID}/extraEnvValues/{UUID}/value	Der zusätzliche Umgebungsvariablen-Wert für die Verbindung.
root/ConnectionType/teemtalk/connections/{UUID}/fallBackConnection	Bei der Einstellung auf die UUID einer anderen verfügbaren Verbindung, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Ausweichverbindung ist normalerweise aufzufinden, indem man "connection-mgr list" auf dem Client ausführt oder indem man zu root/ConnectionType/<Type>/connections/ navigiert.
root/ConnectionType/teemtalk/connections/{UUID}/hasDesktopIcon	Bei Einstellung des Werts auf 1 wird die Verbindung auf dem ThinPro-Desktop angezeigt. Nicht zutreffend für Smart Zero.
root/ConnectionType/teemtalk/connections/{UUID}/isInMenu	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/teemtalk/connections/{UUID}/label	Der Name der Verbindung. Dies wird von 'root/ConnectionManager/defaultConnection' verwendet, um anzugeben, welche Verbindung sowohl beim Systemstart als auch im Connection Manager gestartet wird.
root/ConnectionType/teemtalk/connections/{UUID}/startMode	Wenn die Standardeinstellung focus 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	Aktiviert den System-Piepton für die Verbindung.
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/appName	Der interne Name der Anwendung zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/className	Der interne X-Windows Anwendungs-Klassenname zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/editor	Der interne Name der Anwendung, der zum Starten des Verbindungseditors für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der zum Starten des Editors für allgemeine Einstellungen für diesen

Tabelle E-7 root > ConnectionType > teemtalk (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/icon16Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 16 x 16 Pixel für diese Anwendung. Dies ist das kleine Symbol links neben den Verbindungsnamen im Verbindungsdialog.
root/ConnectionType/teemtalk/coreSettings/icon32Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 32 x 32 Pixel für diese Anwendung.
root/ConnectionType/teemtalk/coreSettings/icon48Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 48 x 48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/teemtalk/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/teemtalk/coreSettings/serverRequired	Zeigt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/teemtalk/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist dies close , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn kill eingestellt ist, wird der durch den "appName" angegebene Prozess zum Abbruch gezwungen. Wenn custom eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch "wrapperScript", mit dem Argument "stop" 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	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/gui/TeemtalkManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/gui/TeemtalkManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Auto reconnect (Automatische Neuverbindung) im TeemTalk Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autostart	Zum Einstellen des Status für das Widget Auto start priority (Autostart-Priorität) im TeemTalk Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das

Tabelle E-7 root > ConnectionType > teemtalk (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Show icon on desktop (Symbol auf Desktop anzeigen) im TeemTalk Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/isInMenu	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/label	Zum Einstellen des Status für das Widget Name im TeemTalk Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Wait for network before connection (Auf Netzwerk warten vor Verbindungsaufbau) im TeemTalk Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.

root > ConnectionType > telnet

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > telnet**.

Tabelle E-8 root > ConnectionType > telnet

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/telnet/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/telnet/connections/{UUID}/address	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll.
root/ConnectionType/telnet/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung werden soll.

Tabelle E-8 root > ConnectionType > telnet (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung werden soll.
root/ConnectionType/telnet/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Auf '1' einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, selbst wenn dieser Schlüssel auf '0' eingestellt ist.
root/ConnectionType/telnet/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung hat. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/telnet/connections/{UUID}/autoReconnect	Wenn 1 eingestellt ist, wird das System automatisch versuchen, die Verbindung neu zu starten, nachdem sie geschlossen wurde. Falls erforderlich, sollten über das Feld <code>zero-login/defaultCredentials</code> die Anmeldeinformationen bereitgestellt werden. "autostart" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/telnet/connections/{UUID}/autostart	Wenn die Einstellung größer als 0 ist, versucht das System die Verbindung automatisch zu starten, wenn der Client hochgefahren wird. Falls erforderlich, sollten über das Feld <code>zero-login/defaultCredentials</code> die Anmeldeinformationen bereitgestellt werden. "autoReconnect" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/telnet/connections/{UUID}/backgroundColor	Gibt die Hintergrundfarbe der Verbindung an.
root/ConnectionType/telnet/connections/{UUID}/beforeStartingCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/telnet/connections/{UUID}/connectionEndAction	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/telnet/connections/{UUID}/coord	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/telnet/connections/{UUID}/dependConnectionId	Dieser Schlüssel ist zur Verwendung reserviert.
root/ConnectionType/telnet/connections/{UUID}/extraEnvValues/{UUID}/key	Die zusätzliche Umgebungsvariable für die Verbindung.
root/ConnectionType/telnet/connections/{UUID}/extraEnvValues/{UUID}/value	Der zusätzliche Umgebungsvariablen-Wert für die Verbindung.
root/ConnectionType/telnet/connections/{UUID}/fallBackConnection	Bei der Einstellung auf die UUID einer anderen verfügbaren Verbindung, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Ausweichverbindung ist normalerweise aufzufinden, indem man "connection-mgr list" auf dem Client ausführt oder indem man zu <code>root/ConnectionType/<Type>/connections/</code> navigiert.

Tabelle E-8 root > ConnectionType > telnet (Fortsetzung)

Registrierungsschlüssel	Beschreibung
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	Aktiviert das Desktop-Symbol für die Verbindung.
root/ConnectionType/telnet/connections/{UUID}/label	Der Name der Verbindung. Dies wird von 'root/ConnectionManager/defaultConnection' verwendet, um anzugeben, welche Verbindung sowohl beim Systemstart als auch im Connection Manager gestartet wird.
root/ConnectionType/telnet/connections/{UUID}/locale	Gibt das Gebietsschema der Verbindung an.
root/ConnectionType/telnet/connections/{UUID}/port	Gibt den Server-Port für die Verbindung an. Die Standardeinstellung ist 23 .
root/ConnectionType/telnet/connections/{UUID}/startMode	Wenn die Standardeinstellung focus 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/appName	Der interne Name der Anwendung zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/className	Der interne X-Windows Anwendungs-Klassenname zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/editor	Der interne Name der Anwendung, der zum Starten des Verbindungseditors für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der zum Starten des Editors für allgemeine Einstellungen für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/icon16Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 16 x 16 Pixel für diese Anwendung. Dies ist das kleine Symbol links neben den Verbindungsnamen im Verbindungsdialog.
root/ConnectionType/telnet/coreSettings/icon32Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 32 x 32 Pixel für diese Anwendung.
root/ConnectionType/telnet/coreSettings/icon48Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 48 x 48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungseditors für diesen Verbindungstyp.

Tabelle E-8 root > ConnectionType > telnet (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/telnet/coreSettings/serverRequired	Zeigt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/telnet/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist dies close , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn kill eingestellt ist, wird der durch den "appName" angegebene Prozess zum Abbruch gezwungen. Wenn custom eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch "wrapperScript", mit dem Argument "stop" 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	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/gui/TelnetManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/gui/TelnetManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/gui/TelnetManager/widgets/address	Zum Einstellen des Status für das Widget Address (Adresse) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Auto reconnect (Automatische Neuverbindung) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart	Zum Einstellen des Status für das Widget Auto start priority (Autostart-Priorität) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor	Zum Einstellen des Status für das Widget Background color (Hintergrundfarbe) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch

Tabelle E-8 root > ConnectionType > telnet (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection	Zum Einstellen des Status für das Widget Fallback Connection (Ausweichverbindung) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor	Zum Einstellen des Status für das Widget Foreground color (Vordergrundfarbe) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon	Zum Einstellen des Status für das Widget Show icon on desktop (Symbol auf Desktop anzeigen) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/label	Zum Einstellen des Status für das Widget Name im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/port	Zum Einstellen des Status für das Widget Port im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork	Zum Einstellen des Status für das Widget Wait for network before connection (Auf Netzwerk warten vor Verbindungsaufbau) im Telnet Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.

root > ConnectionType > view

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > view**.

Tabelle E-9 root > ConnectionType > view

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/view/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/view/connections/{UUID}/ExtraArgs	Gibt zusätzliche Argumente zum VMware Horizon View-Client an. Führen Sie <code>view_client --help</code> oder <code>vmware-view --help</code> über ein Terminal aus, um alle verfügbaren Argumente anzuzeigen.
root/ConnectionType/view/connections/{UUID}/SingleSignOn	
root/ConnectionType/view/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung ausgeführt wird.
root/ConnectionType/view/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/view/connections/{UUID}/appInMenu	
root/ConnectionType/view/connections/{UUID}/appOnDesktop	
root/ConnectionType/view/connections/{UUID}/attachToConsole	
root/ConnectionType/view/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Auf '1' einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, selbst wenn dieser Schlüssel auf '0' eingestellt ist.
root/ConnectionType/view/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung hat. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/view/connections/{UUID}/autoReconnect	Wenn 1 eingestellt ist, wird das System automatisch versuchen, die Verbindung neu zu starten, nachdem sie geschlossen wurde. Falls erforderlich, sollten über das Feld <code>zero-login/defaultCredentials</code> die Anmeldeinformationen bereitgestellt werden. "autostart" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/view/connections/{UUID}/autoReconnectDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Beenden oder Trennen neu gestartet. Diese Einstellung wird nur wirksam, wenn "autoReconnect" auf 1 eingestellt ist.

Tabelle E-9 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/{UUID}/automaticLogin	Wenn aktiviert, versucht der VMware Horizon View-Client sich automatisch anzumelden, wenn alle Felder zur Verfügung stehen. Wenn dies nicht aktiviert ist, müssen Benutzer im VMware Horizon View-Client auf Connect (Verbinden) klicken, um eine Verbindung mit dem VMware Horizon View-Verbindungsserver herzustellen, sich anmelden und einen Desktop auswählen.
root/ConnectionType/view/connections/{UUID}/autostart	Wenn die Einstellung größer als 0 ist, versucht das System die Verbindung automatisch zu starten, wenn der Client hochgefahren wird. Falls erforderlich, sollten über das Feld <code>zero-login/defaultCredentials</code> die Anmeldeinformationen bereitgestellt werden. "autoReconnect" wird häufig in Verbindung mit dieser Einstellung verwendet.
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 "autostart" auf 1 eingestellt ist.
root/ConnectionType/view/connections/{UUID}/beforeStartingCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die 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 getrennt wurde. Wenn dies nicht aktiviert ist, 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 lassen, nachdem sie sich abgemeldet haben.
root/ConnectionType/view/connections/{UUID}/coord	
root/ConnectionType/view/connections/{UUID}/dependConnectionId	
root/ConnectionType/view/connections/{UUID}/desktop	Wenn angegeben, wird der benannte Desktop beim Anmelden automatisch gestartet. HINWEIS: Standardmäßig wird, wenn nur ein Desktop verfügbar ist, dieser Desktop automatisch gestartet, ohne dass er angegeben werden muss.
root/ConnectionType/view/connections/{UUID}/directory	
root/ConnectionType/view/connections/{UUID}/domain	Die Domäne, die für den VMware Horizon View-Server bereitgestellt wird. Wenn keine Domäne angegeben ist, wird die Standarddomäne verwendet.
root/ConnectionType/view/connections/{UUID}/enableSingleMode	
root/ConnectionType/view/connections/{UUID}/extraEnvValues/{UUID}/key	
root/ConnectionType/view/connections/{UUID}/extraEnvValues/{UUID}/value	
root/ConnectionType/view/connections/{UUID}/fallBackConnection	Bei der Einstellung auf die UUID einer anderen verfügbaren Verbindung, wird diese Verbindung automatisch gestartet,

Tabelle E-9 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Ausweichverbindung ist normalerweise aufzufinden, indem man "connection-mgr list" auf dem Client ausführt oder indem man zu <code>root/ConnectionType/<Type>/connections/</code> navigiert.
<code>root/ConnectionType/view/connections/{UUID}/fullscreen</code>	Bei Einstellung des Werts auf 1 wird der VMware Horizon View-Client im Vollbildmodus gestartet.
<code>root/ConnectionType/view/connections/{UUID}/hasDesktopIcon</code>	Bei Einstellung des Werts auf 1 wird die Verbindung auf dem ThinPro-Desktop angezeigt. Nicht zutreffend für Smart Zero.
<code>root/ConnectionType/view/connections/{UUID}/hideMenuBar</code>	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. Standardmäßig wird sie für ThinPro angezeigt und für Smart Zero ausgeblendet.
<code>root/ConnectionType/view/connections/{UUID}/isInMenu</code>	Bei Einstellung des Werts auf 1 wird die Verbindung in der HP ThinPro-Taskleiste angezeigt. Nicht zutreffend für Smart Zero.
<code>root/ConnectionType/view/connections/{UUID}/label</code>	Der Name der Verbindung. Dies wird von 'root/ConnectionManager/defaultConnection' verwendet, um anzugeben, welche Verbindung sowohl beim Systemstart als auch im Connection Manager gestartet wird.
<code>root/ConnectionType/view/connections/{UUID}/password</code>	Das Standardkennwort, das der Remote-Host während der Anmeldung benötigt. Dieser Wert wird verschlüsselt gespeichert. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
<code>root/ConnectionType/view/connections/{UUID}/saveCredentials</code>	
<code>root/ConnectionType/view/connections/{UUID}/server</code>	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll. In der Regel ist dies eine URL, wie z. B. 'https://server.domain.com'.
<code>root/ConnectionType/view/connections/{UUID}/sessionEndAction</code>	
<code>root/ConnectionType/view/connections/{UUID}/singleDesktop</code>	
<code>root/ConnectionType/view/connections/{UUID}/smartcard</code>	Bei Aktivierung werden hierdurch alle lokal angeschlossenen Smart Cards an dem Remote-Host weitergeleitet, damit sie von Anwendungen auf dem Remote-Host verwendet werden können. Hierdurch wird nicht die Smart Card-Anmeldung für die VMware Horizon View-Serveranmeldung aktiviert, sondern nur für den Remote-Host.
<code>root/ConnectionType/view/connections/{UUID}/startMode</code>	Wenn die Standardeinstellung focus eingestellt ist und die Verbindung bereits gestartet wurde, erhält sie den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
<code>root/ConnectionType/view/connections/{UUID}/username</code>	Der Standard-Benutzername, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet,

Tabelle E-9 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/{UUID}/viewSecurityLevel	bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/view/connections/{UUID}/waitForNetwork	Wenn der Standard Refuse insecure connections (Unsichere Verbindungen zurückweisen) 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 Warn (Warnen) 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 Allow all connections (Alle Verbindungen zulassen) ist, wird das Serverzertifikat nicht überprüft und Verbindungen zu jedem beliebigen Server werden zugelassen.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/attachToConsole	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/audioLatency	Der durchschnittliche Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln.
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. Dies wird häufig verwendet, um die Netzwerkbandbreite zu reduzieren. HINWEIS: 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. Eine Einstellung auf '0' deaktiviert die Komprimierung. Die Komprimierung ist standardmäßig aktiviert.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/disableMMRwithRFX	Wenn die Einstellung nicht 0 ist, wird die Multimedia-Umleitung deaktiviert, wenn eine gültige RemoteFX-Sitzung aufgebaut wurde.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/frameAcknowledgeCount	Dies ist die Anzahl der Videoframes, 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	Eine Einstellung auf 1 aktiviert das Multimedia-Umleitungs-Plugin, wodurch unterstützte Codecs, die über den Windows Media Player wiedergegeben werden, an den Client umgeleitet werden. Dies verbessert die Videowiedergabe im Vollbild- und High-Definition-Modus für Codes wie z. B. WMV9, VC1 und MPEG4.

Tabelle E-9 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/general/sendHostname	Bei der Standardeinstellung hostname wird der System-Hostnamen an den Remote-Host gesendet. Dies wird in der Regel von einem Administrator verwendet, um den mit einer bestimmten RDP-Sitzung verknüpften Client-Rechner zu identifizieren. Der gesendete Hostname kann überschrieben werden, indem der Schlüssel "SendHostname" in den verbindungs-spezifischen Einstellungen festgelegt wird. Bei der Einstellung mac wird die MAC-Adresse des ersten verfügbaren Netzwerkadapters anstelle des Hostnamen gesendet.
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.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/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/view/connections/{UUID}/xfreerdpOptions/perfFlagDesktopComposition	Die Einstellung des Werts 1 ermöglicht die Desktopgestaltung, wie z. B. durchsichtige Rahmen, wenn dies vom Server unterstützt wird. Ein Ausschalten dieser Option kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagFontSmoothing	Die Einstellung des Werts 1 ermöglicht eine Schriftglättung, wenn dies vom Server unterstützt wird und aktiviert ist. Es Ausschalten dieser Option kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoCursorSettings	Die Einstellung des Werts 1 deaktiviert das Blinken des Cursors, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoCursorShadow	Die Einstellung des Werts 1 schaltet die Mauscursor-Schatten aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoMenuAnimations	Die Einstellung des Werts 1 schaltet Menüanimationen aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoTheming	Die Einstellung des Werts 1 schaltet die Designs der Benutzeroberfläche aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/perfFlagNoWallpaper	Die Einstellung des Werts 1 schaltet die Desktop-Hintergrundbilder aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/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.

Tabelle E-9 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/portMapping	Bei Einstellung des Werts auf 1 werden die folgenden lokalen seriellen und parallelen Ports zum Remote-Host umgeleitet: ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/printerMapping	Bei Einstellung des Werts auf 1 wird das Umleitungs-Plugin für CUPS-Drucker aktiviert, wodurch alle Drucker, die lokal über CUPS definiert sind, an den Remote-Host umgeleitet werden.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/rdpEncryption	Bei Einstellung des Werts auf 1 wird die Standard-RDP-Verschlüsselung zum Verschlüsseln aller Daten zwischen dem Client und Server verwendet.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/remoteFx	Falls verfügbar, RemoteFX verwenden.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/sendHostname	Der angegebene Text wird als Client-Hostnamen zum Remote-Host gesendet. Wenn das Feld leer bleibt, wird der System-Hostname an den Hostnamen gesendet. HINWEIS: Der Schlüssel für allgemeine Einstellungen 'root/ConnectionType/freerdp/coreSettings/sendHostname' muss für diesen Schlüssel zur Verwendung auf 'hostname' eingestellt sein.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/sound	Durch die Standardeinstellung Bring to this computer (Auf diesem Computer wiedergeben) wird der Sound mithilfe eines virtuellen Kanals vom Remote-Host zum Client umgeleitet. Durch die Einstellung Leave at remote computer (Auf dem Remotecomputer wiedergeben) 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. HP empfiehlt die Einstellung von Sound auf Bring to this computer (Auf diesem Computer wiedergeben), da dies die Audioqualität verbessert und sicherstellt, dass die gesamte Client-Audio-Umleitung über andere virtuelle Kanäle, wie beispielsweise MMR, mit den lokalen Audioeinstellungen übereinstimmt.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/timeoutError	Die Anzahl von Millisekunden, die nach dem Verlust einer Verbindung mit dem Server gewartet wird, bevor ein Fehler-Dialogfeld angezeigt und die Verbindung beendet wird. Ist bei Einstellung auf 0 deaktiviert.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/timeoutWarning	Die Anzahl von Millisekunden, die nach dem Ausfall einer Verbindung mit dem Server vergehen, bevor der Benutzer gewarnt wird, dass die Verbindung getrennt wurde. Ist bei Einstellung auf 0 deaktiviert.
root/ConnectionType/view/connections/{UUID}/xfreerdpOptions/xkbLayoutId	Wenn nicht leer, geben Sie eine XKB-Layout-ID an, um die System-Tastatur zu umgehen. Um Zugriff auf die Liste der verfügbaren IDs zu erhalten, geben Sie Folgendes in ein Terminal ein: <code>xfreerdp --kbd-list</code> .
root/ConnectionType/view/coreSettings/appName	Der interne Name der Anwendung zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.

Tabelle E-9 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/coreSettings/className	Der interne X-Windows Anwendungs-Klassenname zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/coreSettings/editor	Der interne Name der Anwendung, der zum Starten des Verbindungseditors für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/coreSettings/icon16Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 16 x 16 Pixel für diese Anwendung. Dies ist das kleine Symbol links neben den Verbindungsnamen im Verbindungsdialog.
root/ConnectionType/view/coreSettings/icon32Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 32 x 32 Pixel für diese Anwendung.
root/ConnectionType/view/coreSettings/icon48Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 48 x 48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungseditors für diesen Verbindungstyp.
root/ConnectionType/view/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlménü der Verbindungstypen angezeigt wird.
root/ConnectionType/view/coreSettings/serverRequired	Zeigt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/view/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist dies close , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn kill eingestellt ist, wird der durch den "appName" angegebene Prozess zum Abbruch gezwungen. Wenn custom eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch "wrapperScript", mit dem Argument "stop" ausgeführt, um den Prozess ordnungsgemäß zu beenden.
root/ConnectionType/view/coreSettings/watchPid	Durch Einstellen des Werts 1 wird die durch "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/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/view/general/rdpOptions	Die hier angegebenen Optionen werden direkt an den RDP-Client weitergeleitet, wenn RDP als Anzeigeprotokoll für die VMware Horizon View-Verbindung verwendet werden soll. Um eine vollständige Liste der Optionen anzuzeigen, geben Sie im Client-Terminal "rdesktop--help" ein.
root/ConnectionType/view/gui/viewManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/gui/viewManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.

Tabelle E-9 root > ConnectionType > view (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/gui/viewManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/view/gui/viewManager/widgets/autostart	
root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection	
root/ConnectionType/view/gui/viewManager/widgets/label	

root > ConnectionType > xdmcp

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > xdmcp**.

Tabelle E-10 root > ConnectionType > xdmcp

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/xdmcp/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/xdmcp/connections/{UUID}/address	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll.
root/ConnectionType/xdmcp/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung ausgeführt werden soll.
root/ConnectionType/xdmcp/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/xdmcp/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Einrichten auf 1 für Erlauben, 0 für Verweigerung des Zugriffs. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf 0 eingerichtet ist.
root/ConnectionType/xdmcp/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung an. Einrichten auf 1 für Erlauben, 0 für Verweigerung des Zugriffs. HINWEIS: Diese Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/xdmcp/connections/{UUID}/autoReconnect	Bei Einstellung des Werts auf 1 wird das System versuchen, die Verbindung automatisch neu zu starten, nachdem sie

Tabelle E-10 root > ConnectionType > xdmcp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	geschlossen wurde. Falls erforderlich, sollten im Feld <code>zero-login/defaultCredentials</code> Anmeldeinformationen bereitgestellt werden. "autostart" wird häufig in Verbindung mit dieser Einstellung verwendet.
<code>root/ConnectionType/xdmcp/connections/{UUID}/autostart</code>	Wenn dies größer als 0 ist, wird das System versuchen, die Verbindung automatisch herzustellen, wenn der Client gestartet wird. Falls erforderlich, sollten im Feld <code>zero-login/defaultCredentials</code> Anmeldeinformationen bereitgestellt werden. "autoReconnect" wird häufig in Verbindung mit dieser Einstellung verwendet.
<code>root/ConnectionType/xdmcp/connections/{UUID}/beforeStartingCommand</code>	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die vor dem Starten der Verbindung ausgeführt werden soll.
<code>root/ConnectionType/xdmcp/connections/{UUID}/color</code>	Die Farbtiefe für die GUI oder die Anzeige der Verbindung.
<code>root/ConnectionType/xdmcp/connections/{UUID}/connectionEndAction</code>	Dieser Schlüssel hat keine Funktion.
<code>root/ConnectionType/xdmcp/connections/{UUID}/coord</code>	Die Fensterposition der Verbindung.
<code>root/ConnectionType/xdmcp/connections/{UUID}/dependConnectionId</code>	Dieser Schlüssel hat keine Funktion.
<code>root/ConnectionType/xdmcp/connections/{UUID}/extraEnvValues/{UUID}/key</code>	Der Schlüssel für den ExtraEnv-Wert der Verbindung.
<code>root/ConnectionType/xdmcp/connections/{UUID}/extraEnvValues/{UUID}/value</code>	Der Wert, der dem Schlüssel für die ExtraEnv der Verbindung entspricht.
<code>root/ConnectionType/xdmcp/connections/{UUID}/fallBackConnection</code>	Wenn die Einstellung auf die UUID einer anderen verfügbaren UUID-Verbindung erfolgte, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Fallback-Verbindung finden Sie normalerweise durch Ausführen von "connection-mgr list" auf dem Client oder indem Sie zu <code>root/ConnectionType/<type>/connections/</code> navigieren.
<code>root/ConnectionType/xdmcp/connections/{UUID}/fontServer</code>	Wenn UserFontServer auf den Wert 1 eingestellt ist, wird die Registrierung verwendet, um diese Schriftartartenserver-Adresse anzugeben.
<code>root/ConnectionType/xdmcp/connections/{UUID}/hasDesktopIcon</code>	Bei Einstellung des Werts auf 1 wird ein Symbol für die Verbindung auf dem Desktop angezeigt.
<code>root/ConnectionType/xdmcp/connections/{UUID}/isInMenu</code>	Bei Einstellung des Werts auf 1 wird ein Menüelement für die Verbindung erstellt. Dieser Schlüssel funktioniert noch nicht.
<code>root/ConnectionType/xdmcp/connections/{UUID}/label</code>	Der Name der Verbindung. Dies wird von <code>root/ConnectionManager/defaultConnection</code> verwendet, um anzugeben, welche Verbindung sowohl beim Systemstart als auch im Connection Manager gestartet wird.
<code>root/ConnectionType/xdmcp/connections/{UUID}/refreshRate</code>	Die Bildwiederholungsrate für das Display der Verbindung.
<code>root/ConnectionType/xdmcp/connections/{UUID}/startMode</code>	Wenn die Standardeinstellung auf focus eingerichtet ist und die Verbindung bereits gestartet ist, erhält die Verbindung den Fokus. Andernfalls wird eine Fehlermeldung mit dem Hinweis Verbindung ist bereits gestartet zurückgegeben.

Tabelle E-10 root > ConnectionType > xdmcp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/connections/{UUID}/type	Gibt den XDMCP-Verbindungstyp an. Durch die Einstellung chooser werden alle verfügbaren Hosts aufgelistet und der Benutzer kann wählen, zu welchem eine Verbindung hergestellt werden soll. Durch die Einstellung query wird eine XDMCP-Anforderung direkt zum angegebenen Host gesendet. Durch die Einstellung broadcast 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 nicht gestartet, bis das Netzwerk verfügbar ist. Somit wird sichergestellt, dass auf einem langsamen Netzwerk die Verbindung so lange nicht gestartet wird, bis das Netzwerk verfügbar ist, und somit keine Probleme auftreten.
root/ConnectionType/xdmcp/connections/{UUID}/windowSize	Die Client-Fenstergröße für die Verbindung.
root/ConnectionType/xdmcp/coreSettings/appName	Der interne Name der Anwendung zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/coreSettings/audio	Die Audio-Einstellung für den Verbindungstyp. Es gibt keine Audio-Unterstützung für XDMCP.
root/ConnectionType/xdmcp/coreSettings/className	Der interne Klassenname der X-Windows Anwendung, der verwendet wird, wenn die PID der Verbindung für die Statusüberwachung nachverfolgt wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/coreSettings/desktopButton	Eine benutzerdefinierte Desktop-Schaltfläche für XDMCP. Dieser Schlüssel wird nicht unterstützt.
root/ConnectionType/xdmcp/coreSettings/editor	Der interne Name der Anwendung, der zum Starten des Verbindungseditors für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der verwendet wird, wenn der Editor für die allgemeinen Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/coreSettings/icon16Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 16x16 Pixel für diese Anwendung. Dieses Symbol ist das kleine Symbol links neben dem Namen für die Verbindung im Verbindungsdialo.
root/ConnectionType/xdmcp/coreSettings/icon32Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 32x32 Pixel für diese Anwendung.
root/ConnectionType/xdmcp/coreSettings/icon48Path	Der interne Pfad für das Anwendungssymbol für das Symbol mit 48x48 Pixel für diese Anwendung. Dies ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/xdmcp/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.

Tabelle E-10 root > ConnectionType > xdmcp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/coreSettings/serverRequired	Gibt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/xdmcp/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist diese close . Damit wird ein Standard-Kill-Signal an den Vorgang gesendet. Bei der Einstellung auf kill wird der von "appName" angegebene Prozess zwangsweise geschlossen. Bei der Einstellung auf custom wird ein vom "wrapperScript" angegebenes, benutzerdefiniertes Ausführungsskript ausgeführt, das mit dem Argument "stop" den Prozess beendet.
root/ConnectionType/xdmcp/coreSettings/watchPid	Bei Einstellung des Werts auf 1 wird die von "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/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 bearbeitet. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/gui/XdmcpManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/gui/XdmcpManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/gui/XdmcpManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/address	Zum Einstellen des Status für das Widget Address (Adresse) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect	Zum Einstellen des Status für das Widget Auto reconnect (Automatische Neuverbindung) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autostart	Zum Einstellen des Status für das Widget Auto start priority (Autostart-Priorität) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/color	Dieser Schlüssel hat keine Funktion.

Tabelle E-10 root > ConnectionType > xdmcp (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ fontServer	Zum Einstellen des Status für das Widget Font server (Schriftartenserver) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ hasDesktopIcon	Zum Einstellen des Status für das Widget Show icon on desktop (Symbol auf dem Desktop anzeigen) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ isInMenu	Dieser Schlüssel hat keine Funktion.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ label	Zum Einstellen des Status für das Widget Name im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ refreshRate	Dieser Schlüssel hat keine Funktion.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ type	Zum Einstellen des Status für das Widget Type (Typ) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ useFontServer	Zum Einstellen des Status für das Widget Use font server (Schriftartenserver verwenden) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ waitForNetwork	Zum Einstellen des Status für das Widget Wait for network before connection (Auf Netzwerk warten vor Verbindungsaufbau) im XDMCP Connection Manager. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/ windowSize	Dieser Schlüssel hat keine Funktion.

root > ConnectionType > xen

Dieser Abschnitt beschreibt die Registrierungsschlüssel und Funktionen im Ordner **root > ConnectionType > xen**.

Tabelle E-11 root > ConnectionType > xen

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/authorizations/user/add	Zeigt an, ob der Benutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über das Kontrollzentrum hat. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/xen/authorizations/user/general	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über das Kontrollzentrum besitzt. Nicht zutreffend für Smart Zero. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern.
root/ConnectionType/xen/connections/{UUID}/SingleSignOn	
root/ConnectionType/xen/connections/{UUID}/address	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll. In der Regel ist dies eine URL, wie z. B. 'http://server.domain.com'.
root/ConnectionType/xen/connections/{UUID}/afterStartedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach dem Start der Verbindung ausgeführt werden soll.
root/ConnectionType/xen/connections/{UUID}/afterStoppedCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die nach Beendigung der Verbindung ausgeführt werden soll.
root/ConnectionType/xen/connections/{UUID}/applnMenu	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung im Dashboard-Menü angezeigt.
root/ConnectionType/xen/connections/{UUID}/appOnDesktop	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung auf dem Desktop angezeigt.
root/ConnectionType/xen/connections/{UUID}/authorizations/user/edit	Zeigt an, ob der Benutzer die Berechtigung zum Ändern der Einstellungen für diese Verbindung hat. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung kann im Administratormodus bearbeitet werden, auch wenn dieser Schlüssel auf 0 eingestellt ist.
root/ConnectionType/xen/connections/{UUID}/authorizations/user/execution	Zeigt an, ob der Benutzer die Berechtigung zum Ausführen der Verbindung hat. Auf 1 einstellen, um Zugriff zu erlauben, und auf 0 einstellen, um Zugriff zu verweigern. HINWEIS: Die Verbindung wird immer im Administratormodus zum Starten verfügbar sein.
root/ConnectionType/xen/connections/{UUID}/autoLaunchSingleApp	Wenn dieser Wert auf 1 eingestellt ist und es wird nur eine einzige Anwendung oder ein Desktop vom Citrix-Server zurückgemeldet, startet diese Ressource automatisch.
root/ConnectionType/xen/connections/{UUID}/autoReconnect	Bei Einstellung des Werts auf 1 versucht das System die Verbindung automatisch neu zu starten, nachdem sie beendet wurde. Falls erforderlich, sollten über das Feld <code>Zero-Login/DefaultCredentials</code>

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Anmeldeinformationen bereitgestellt werden. "autostart" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/xen/connections/{UUID}/autoReconnectAppsOnLogin	Bei Einstellung des Werts auf 1 versucht das System nach einer Erstanmeldung alle aktiven oder getrennten Citrix-Sitzungen wiederherzustellen.
root/ConnectionType/xen/connections/{UUID}/autoReconnectDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Beenden oder Trennen neu gestartet. Diese Einstellung wird nur wirksam, wenn "autoReconnect" auf 1 eingestellt ist.
root/ConnectionType/xen/connections/{UUID}/autoStartDesktop	Um beim Starten einer Citrix-Verbindung automatisch den ersten verfügbaren Desktop zu starten, stellen Sie den Wert des Schlüssels auf 1 ein.
root/ConnectionType/xen/connections/{UUID}/autoStartResource	Um beim Starten einer Citrix-Verbindung automatisch einen Desktop oder eine Anwendung zu starten, stellen Sie den Wert des folgenden Schlüssels auf den Namen des Desktops oder der Anwendung, die Sie starten möchten, ein.
root/ConnectionType/xen/connections/{UUID}/autostart	Wenn die Einstellung größer als 0 ist, versucht das System die Verbindung automatisch zu starten, wenn der Client hochgefahren wird. Falls erforderlich, sollten über das Feld <code>Zero-Login/DefaultCredentials</code> Anmeldeinformationen bereitgestellt werden. "autoReconnect" wird häufig in Verbindung mit dieser Einstellung verwendet.
root/ConnectionType/xen/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 "autostart" auf 1 eingestellt ist.
root/ConnectionType/xen/connections/{UUID}/beforeStartingCommand	Der vollständige Pfad zu einem Skript oder einer Binärdatei, das bzw. die vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/xen/connections/{UUID}/connectionEndAction	
root/ConnectionType/xen/connections/{UUID}/coord	
root/ConnectionType/xen/connections/{UUID}/dependConnectionId	
root/ConnectionType/xen/connections/{UUID}/disableSaveCredentials	
root/ConnectionType/xen/connections/{UUID}/domain	Die Domäne, die für den XenDesktop-Server bereitgestellt wird. Wenn keine Domäne angegeben ist, wird die Standarddomäne für den Server verwendet.
root/ConnectionType/xen/connections/{UUID}/enablePNADesktopIcons	
root/ConnectionType/xen/connections/{UUID}/enablePNASStartMenuItems	
root/ConnectionType/xen/connections/{UUID}/extraEnvValues/{UUID}/key	

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/connections/{UUID}/extraEnvValues/{UUID}/value	
root/ConnectionType/xen/connections/{UUID}/fallBackConnection	Bei der Einstellung auf die UUID einer anderen verfügbaren Verbindung, wird diese Verbindung automatisch gestartet, falls die aktuelle Verbindung fehlschlägt oder wenn ein Fehler auftritt und sie nicht gestartet werden kann. Die UUID der gewünschten Ausweichverbindung ist normalerweise aufzufinden, indem man "connection-mgr list" auf dem Client ausführt oder indem man zu root/ConnectionType/<type>/connections/ navigiert.
root/ConnectionType/xen/connections/{UUID}/folder	
root/ConnectionType/xen/connections/{UUID}/fullscreen	Bei Einstellung des Werts auf 1 wird der ICA-Client im Vollbildmodus gestartet.
root/ConnectionType/xen/connections/{UUID}/hasDesktopIcon	Bei Einstellung des Werts auf 1 wird ein Symbol für die Verbindung auf dem Desktop angezeigt. Nicht zutreffend für Smart Zero.
root/ConnectionType/xen/connections/{UUID}/isInMenu	
root/ConnectionType/xen/connections/{UUID}/label	Der Name der Verbindung. Dies wird von root/ConnectionManager/defaultConnection verwendet, um anzugeben, welche Verbindung sowohl beim Systemstart als auch im Connection Manager gestartet wird.
root/ConnectionType/xen/connections/{UUID}/logOnMethod	
root/ConnectionType/xen/connections/{UUID}/password	Falls festgelegt, wird dieses Kennwort als Standardeinstellung im Anmeldedialog bereitgestellt, wenn der Benutzer und die Domäne hier ihren Standardeinstellungen entsprechen. Wird in der Regel bei Verbindungen mit automatischem Start verwendet.
root/ConnectionType/xen/connections/{UUID}/requireCredentialsDirectConnect	Stellen Sie den Wert auf 0 ein, um eine Eingabeaufforderung für die Anmeldeinformationen zu verhindern, wenn Sie eine direkte Verbindung verwenden. Standardmäßig wird der Benutzer vom Server aufgefordert, Zugangsdaten einzugeben, wenn eine Anwendung gestartet wird.
root/ConnectionType/xen/connections/{UUID}/savePassword	
root/ConnectionType/xen/connections/{UUID}/smoothRoamWhenAutostartResource	Bei Einstellung des Werts auf 1 wird die Ressource automatisch gestartet, wenn ein reibungsloses Roaming möglich ist. Stellen Sie zum Deaktivieren den Wert 0 ein.
root/ConnectionType/xen/connections/{UUID}/startMode	Wenn die Standardeinstellung focus eingestellt ist und die Verbindung bereits gestartet wurde, erhält sie den Fokus. Andernfalls wird eine Fehlermeldung ausgegeben, die darauf hinweist, dass die Verbindung bereits gestartet wurde.
root/ConnectionType/xen/connections/{UUID}/storeFrontConn	
root/ConnectionType/xen/connections/{UUID}/useCredentials	
root/ConnectionType/xen/connections/{UUID}/username	Der Standard-Benutzername, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet,

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/xen/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/xen/coreSettings/appName	Der interne Name der Anwendung zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch	Diese Einstellung gilt für Citrix-Server mit mehreren veröffentlichten Apps oder Desktops. Bei einem Wert unter 0 wird keine automatische Abmeldung ausgeführt. Andernfalls ist dies die Anzahl der Sekunden zwischen dem Schließen der letzten Xen-Anwendung und dem Zeitpunkt, zu dem der Xen-Desktop automatisch beendet wird. Citrix-Prozessverzögerungen können die Zeit bis zur automatischen Abmeldung verlängern.
root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch	Diese Einstellung gilt für Citrix-Server mit mehreren veröffentlichten Apps oder Desktops. Bei einem Wert unter 0 wird keine automatische Abmeldung ausgeführt. Andernfalls ist dies die Anzahl der Sekunden zwischen dem Schließen der letzten Xen-Anwendung und dem Zeitpunkt, zu dem der Xen-Desktop automatisch beendet wird. Citrix-Prozessverzögerungen können die Zeit bis zur automatischen Abmeldung verlängern.
root/ConnectionType/xen/coreSettings/autoLogoutDelaySingleApp	Diese Einstellung gilt für Citrix Server mit einer bzw. einem einzigen veröffentlichten App oder Desktop. Bei einem Wert unter 0 wird keine automatische Abmeldung ausgeführt. Andernfalls ist dies die Anzahl der Sekunden zwischen dem Schließen der letzten Xen-Anwendung und dem Zeitpunkt, zu dem der Xen-Desktop automatisch beendet wird. Citrix-Prozessverzögerungen können die Zeit bis zur automatischen Abmeldung verlängern.
root/ConnectionType/xen/coreSettings/className	Der interne X-Windows Anwendungs-Klassenname zum Nachverfolgen der PID der Verbindung zur Überwachung des Verbindungsstatus. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/editor	Der interne Name der Anwendung, der zum Starten des Verbindungseditors für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/generalSettingsEditor	Der interne Name der Anwendung, der zum Starten des Editors für allgemeine Einstellungen für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/icon16Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 16 x 16 Pixel für diese Anwendung. Dieses Symbol ist das kleine Symbol links neben dem Verbindungsnamen im Verbindungsdialog.
root/ConnectionType/xen/coreSettings/icon32Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 32 x 32 Pixel für diese Anwendung.

Table E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/coreSettings/icon48Path	Der interne Anwendungssymbol-Pfad für das Symbol mit 48 x 48 Pixel für diese Anwendung. Dieses Symbol ist das große Symbol im oberen linken Bereich des Verbindungeditors für diesen Verbindungstyp.
root/ConnectionType/xen/coreSettings/label	Der Name, der für diesen Verbindungstyp im Auswahlmenu der Verbindungstypen angezeigt wird.
root/ConnectionType/xen/coreSettings/serverRequired	Zeigt an, ob ein Servername oder eine Adresse unbenutzt, optional oder für diesen Verbindungstyp erforderlich ist.
root/ConnectionType/xen/coreSettings/stopProcess	Das Verhalten, das auftreten sollte, wenn "connection-mgr stop" für diese Verbindung angefordert wird. Standardmäßig ist dies close , wodurch ein standardmäßiges Abbrechen-Signal an den Vorgang gesendet wird. Wenn kill eingestellt ist, wird der durch den "appName" angegebene Prozess zum Abbruch gezwungen. Wenn custom eingestellt ist, wird ein benutzerdefiniertes Ausführungsskript, angegeben durch "wrapperScript", mit dem Argument "stop" ausgeführt, um den Prozess zu beenden.
root/ConnectionType/xen/coreSettings/watchPid	Durch Einstellen des Werts 1 wird die durch "appName" angegebene Anwendung überwacht, um die Verbindung zu erkennen. 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/general/TWIMode	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>TWIMode=boolean</code> , die den nahtlosen Modus für veröffentlichte Anwendungen steuert. Die Standardeinstellung ist 1 .
root/ConnectionType/xen/general/TWIModeResizeType	Die Standardeinstellung ist 1 .
root/ConnectionType/xen/general/allowReadOn{AthruZ}	Stellen Sie den Wert 1 ein, um dem Benutzer das Lesen des zugeordneten Laufwerks vom Remote-Host zu ermöglichen. Wenn hier der Wert 0 eingestellt wird, werden keine Dateien in dem zugeordneten Laufwerk auf dem Remote-Host angezeigt.
root/ConnectionType/xen/general/allowWriteOn{AthruZ}	Stellen Sie den Wert 1 ein, um dem Benutzer zu erlauben, auf das zugeordnete Laufwerke vom Remote-Host zu schreiben. Wenn hier der Wert 0 eingestellt wird, kann der Benutzer Dateien außerhalb des Laufwerks lesen und kopieren, ist jedoch nicht in der Lage Änderungen vorzunehmen oder neue Dateien zum Laufwerk hinzuzufügen.
root/ConnectionType/xen/general/async	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>CommPollSize=boolean</code> , die das asynchrone Aufrufen aktiviert. Der Standardwert lautet 0 für "Off" (Aus).
root/ConnectionType/xen/general/autoReconnect	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>TransportReconnectEnabled=boolean</code> , die eine automatische Neuverbindung der Sitzung aktiviert. Die Standardeinstellung ist 0 .

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	HINWEIS: Dies ist nicht identisch mit dem verbindungs-spezifischen "autoReconnect". Diese Neuverbindung findet intern statt, innerhalb des Citrix-Clients, ohne Neustart der Verbindung.
root/ConnectionType/xen/general/bitmapCacheSize	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>PersistentCacheMinBitmap=integer</code> , welches die Mindestgröße der Bitmap zum Cachen ist. Die Standardeinstellung ist 8192 . Auf allen Clients ist dies auf eine Standardeinstellung von 2048 eingestellt.
root/ConnectionType/xen/general/colorDepth	Zwingt die ICA, eine bestimmte Farbtiefe für alle Verbindungen zu verwenden. 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	Stellen Sie zum Aktivieren Shared - Approximate Colors (Freigegeben – Angenäherte Farben) ein, und zum Deaktivieren Private - Exact Colors (Individuell – Exakte Farben) ein. Standardmäßig aktiviert. Zuordnung zu der Citrix-INI-Dateieinstellung <code>ApproximateColors=boolean</code> , welche angenäherte Farben aus der Standard-Farbzordnungstabelle anstatt einer individuellen Farbzordnungstabelle und präziser Farben verwendet. Wird nur verwendet, wenn der <code>DesiredColor</code> -Wert 2 (256 Farben) ist. Die Standardeinstellung ist False (Falsch).
root/ConnectionType/xen/general/defaultBrowserProtocol	Standardmäßig auf TCP/IP HTTP Browser eingestellt. Kann auf SSL/TLS HTTPS Browser oder TCP/IP Browser eingestellt werden. Zuordnung zu der Citrix-INI-Dateieinstellung <code>BrowserProtocol=[UDP HTTPonTCP]</code> , die das Protokoll zum Auffinden des ICA-Hosts für die Verbindung steuert. Wenn kein Wert angegeben wird, wird der Standardwert vom [WFClient]-Abschnitt der <code>wfclient.ini</code> verwendet.
root/ConnectionType/xen/general/drivePathMappedOn{AthruZ}	Das Verzeichnis des lokalen Dateisystems zur Zuordnung zum Remote-Host. In der Regel ist dies auf /media eingestellt, damit alle angeschlossenen USB-Laufwerke über einen einzigen Laufwerksbuchstaben dem Remote-Host zugeordnet werden können.
root/ConnectionType/xen/general/enableAlertSound	Stellen Sie den Standardwert 1 ein, um die Windows-Warntöne zu aktivieren. Stellen Sie zum Deaktivieren den Wert 0 ein. Indirekte Zuordnung zu der Citrix-INI-Dateieinstellung <code>DisableSound=boolean</code> , welche die Windows-Warntöne deaktiviert. Die Standardeinstellung ist False (Falsch).
root/ConnectionType/xen/general/enableAudioInput	Stellen Sie den Standardwert 1 ein, um den Audioeingang zu aktivieren. Dadurch werden beide Einstellungen, sowohl 'AllowAudioInput' (Audioeingang zulassen) als auch 'EnableAudioInput' (Audioeingang deaktivieren) in der <code>wfclient.ini</code> und der <code>appsrv.ini</code> auf den Wert 1 eingestellt.
root/ConnectionType/xen/general/enableCursorColors	Auf den Wert 0 einstellen, um die Verwendung der X11-Render-Erweiterung, die für Farbcursor erforderlich ist, zu deaktivieren. Dies kann in einigen Fällen grafische Cursorstörungen beheben.

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/enableDataCompression	Stellen Sie den Standardwert 1 ein, um die Datenkomprimierung zu aktivieren, oder den Wert 0 , um sie zu deaktivieren. Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>Compress=boolean</code> , welche die Datenkomprimierung steuert.
root/ConnectionType/xen/general/enableDriveMapping	Damit können Verzeichnisse auf dem lokalen Dateisystem über ein virtuelles Laufwerk zum Remote-Host weitergeleitet werden. Typischerweise würde /media zu Z 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 oder ext3.
root/ConnectionType/xen/general/enableDynamicDriveMapping	Wenn aktiviert, werden USB-Speichergeräte dynamisch dem Citrix-Server zugeordnet und statische Laufwerkszuordnungen sind nicht erforderlich.
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	Stellen Sie den Wert 0 ein, um die Codec-Unterstützung für starke Komprimierung und die Text-Nachverfolgung zu deaktivieren. Wenn die H264Compression aktiviert ist, bietet dies mehr Leistung bei umfangreichen und professionellen Grafikanwendungen auf WAN-Netzwerken im Vergleich zum JPEG-Codec.
root/ConnectionType/xen/general/enableHDXFlashRedirection	Regelung des Verhaltens der HDX Flash-Umleitung durch Einstellung auf Always , Ask oder Never . Die Standardeinstellung ist "Always", was bedeutet, dass die HDX Flash-Umleitung verwendet wird, sofern dies möglich ist, und der Benutzer keine Eingabeaufforderung erhält. Bei "Ask" erhält der Benutzer während der Sitzung eine dynamische Eingabeaufforderung. Durch "Never" wird die Funktion deaktiviert.
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	Regelung des Verhaltens für das serverseitige Abrufen der HDX Flash-Inhalte anhand der Einstellung Enabled (Aktiviert) oder Disabled (Deaktiviert). Die Standardeinstellung ist Disabled (Deaktiviert), wobei der Client Inhalte abruft.
root/ConnectionType/xen/general/enableHDXMediaStream	Stellen Sie den Wert 0 ein, um HDX MediaStream zu deaktivieren. Wenn HDX MediaStream deaktiviert ist, werden Mediendateien weiterhin über Standard-Streaming wiedergegeben, aber die Qualität ist möglicherweise nicht so gut.
root/ConnectionType/xen/general/enableMapOn{AthruZ}	Ermöglicht die Durchführung von Laufwerkszuordnungen mithilfe des angegebenen Laufwerks auf dem Remote-Host. Muss auf ein gültiges lokales Verzeichnis eingestellt werden, damit die Laufwerkszuordnung einwandfrei funktioniert. Andere Laufwerksbuchstaben sind ebenfalls verfügbar, wenn alle Schlüssel angezeigt werden.
root/ConnectionType/xen/general/enableOffScreenSurface	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>EnableOSS=boolean</code> ; damit kann der Server X-Pixmaps

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	für Offscreen-Zeichnungen erstellen und verwenden. Reduziert die Bandbreite in 15-Bit- und 24-Bit-Farbe auf Kosten des X-Serverspeichers und der Prozessorzeit. Die Standardeinstellung ist On (Ein).
root/ConnectionType/xen/general/enableSmartCard	Bei Einstellung des Werts auf 1 wird "DisableCtrlAltDel" (StrgAltDel deaktivieren) auf "Off" (Aus) gesetzt und die Smart Card-Anmeldung wird aktiviert. Bei Einstellung des Werts auf 0 wird "SmartCardAllowed" auf "Off" (Aus) gesetzt und Smart Card-Anmeldung deaktiviert.
root/ConnectionType/xen/general/enableWindowsAlertSounds	
root/ConnectionType/xen/general/encryptionLevel	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung EncryptionLevelSession=[None Basic RC5 (128 bit - Login Only) RC5 (40 bit) RC5 (56 bit) RC5 (128 bit)], welche die Verschlüsselungsstufe auf der Basis pro-Verbindung angibt. Die Verschlüsselungsprotokolle für alle Stufen sind im Abschnitt [EncryptionLevelSession] der module.ini definiert.
root/ConnectionType/xen/general/fontSmoothingType	Gibt die Art der Schriftartglättung für die Sitzung an.
root/ConnectionType/xen/general/hotKey{1 thru 15}Char	Das zur Remote-Sitzung weiterzuleitende fn-Tasten-Zeichen. Zum Beispiel: F1 für hotKey1Char.
root/ConnectionType/xen/general/hotKey{1 thru 15}Shift	Der Status der Umschalttaste in der Tastenkombination zum Aktivieren des gewählten fn-Tasten-Zeichens. Ist standardmäßig Ctrl+Shift (Strg+Umschalttaste). Kann eingestellt werden auf Shift (Umschalttaste), Ctrl (Strg), Alt , Alt+Shift (Alt+Umschalttaste), Alt+Ctrl (Alt+Strg) oder Ctrl+Shift (Strg+Umschalttaste).
root/ConnectionType/xen/general/httpAddresses/{UUID}/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung KeyPassthroughEscapeChar=string; dies ist die Taste für den Tastaturbefehl zum Deaktivieren des transparenten Tastaturmodus. Die Standardeinstellung ist F2 . Alle Clients sind standardmäßig auf F1 eingestellt.
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung KeyPassthroughEscapeShift=string; dies ist die Taste für den Tastaturbefehl zum Deaktivieren des transparenten Tastaturmodus. Die Standardeinstellung ist Ctrl (Strg). Alle Clients sind standardmäßig auf Alt eingestellt.
root/ConnectionType/xen/general/lastComPortNum	Die Anzahl der zugeordneten seriellen Ports. Stellen Sie den Wert auf 0 ein, um die Zuordnung der seriellen Ports zu deaktivieren.
root/ConnectionType/xen/general/localTextEcho	Kann eingestellt werden auf On (Ein), Off (Aus) oder auf die Standardeinstellung Auto (Automatisch). Indirekte Zuordnung zu der Citrix-INI-Dateieinstellung ZLKeyboardMode=[0 1 2], die die Tastatur-Latenz-Reduktion steuert. 0 = aus 1 = immer an

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	2 = dynamische Auswahl basierend auf der tatsächlichen Latenz
root/ConnectionType/xen/general/monitorNetwork	Überwachung der Netzwerkkonnektivität. Auf Off (Aus) stellen, um nichts zu überwachen. Durch die Einstellung Local network link status only (Nur Status der lokalen Netzwerkverbindung), wird nur der Status der lokalen Netzwerkverbindung überwacht. Durch die Einstellung Server online status (Server-Onlinestatus), wird sowohl der Status der lokalen Netzwerkverbindung als auch die Serverkonnektivität überwacht. Wenn sie abgebrochen wurde, melden Sie sich in der GUI für den Client an oder trennen Sie die Verbindung für HP ThinPro.
root/ConnectionType/xen/general/mouseClickFeedback	Kann eingestellt werden auf On (Ein), Off (Aus) oder auf die Standardeinstellung Auto (Automatisch). Indirekte Zuordnung zu der Citrix-INI-Dateieinstellung <code>ZLKeyboardMode=[0 1 2]</code> , die die Tastatur-Latenz-Reduktion steuert. 0 = aus 1 = immer an 2 = dynamische Auswahl basierend auf der tatsächlichen Latenz
root/ConnectionType/xen/general/mouseMiddleButtonPaste	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>MouseSendsControlV=boolean</code> , die eine Einfügen-Emulationsfunktion der mittleren Maustaste für Windows-Sitzungen aktiviert. Die Standardeinstellung ist False (Falsch). Alle Clients sind standardmäßig auf 0 eingestellt.
root/ConnectionType/xen/general/noInfoBox	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>PopupOnExit=boolean</code> , die bewirkt, dass der Client Manager-wfcmgr angezeigt wird, wenn eine Clientsitzung beendet wird.
root/ConnectionType/xen/general/printerAutoCreation	Stellen Sie den Wert 0 ein, um die Druckerzuordnung zu deaktivieren.
root/ConnectionType/xen/general/proxyAddress	Die zu verwendende Proxy-Adresse, wenn eine manuelle Proxy-Einstellung über "ProxyType" ausgewählt ist.
root/ConnectionType/xen/general/proxyPassword	Das zu verwendende Proxy-Kennwort, wenn eine manuelle Proxy-Einstellung über "ProxyType" ausgewählt ist. Dieses Feld wird mithilfe der rc4-Verschlüsselung verschlüsselt.
root/ConnectionType/xen/general/proxyPort	Der zu verwendende Proxy-Port, wenn eine manuelle Proxy-Einstellung über "ProxyType" ausgewählt ist.
root/ConnectionType/xen/general/proxyType	Wählt den Proxy-typ, der für die XenDesktop-Verbindungen verwendet wird. "Use Browser settings" (Browser-Einstellungen verwenden) wird nur unterstützt, wenn ein lokaler Browser installiert ist.
root/ConnectionType/xen/general/proxyUser	Der zu verwendende Proxy-Benutzer, wenn eine manuelle Proxy-Einstellung über "ProxyType" ausgewählt ist.
root/ConnectionType/xen/general/serverCheckTimeout	
root/ConnectionType/xen/general/sessionSharingClient	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>EnableSessionSharingClient=boolean</code> , die Anforderungen zum Freigeben der Sitzung an andere ICA-

Table E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Sitzungen auf dem gleichen X-Display sendet. Die Standardeinstellung ist False (Falsch). Alle Clients sind standardmäßig auf 1 eingestellt.
root/ConnectionType/xen/general/sound	Kann auf die Standardeinstellung High Quality (hohe Qualität), Med Quality (Mittlere Qualität), Low Quality (Niedrige Qualität) oder Disabled (Deaktiviert) eingestellt werden. Die Qualität ist indirekt zu der Citrix-INI-Dateieinstellung <code>AudioBandwidthLimit=[0 1 2]</code> zugeordnet. 0 = hoch 1 = mittel 2 = niedrig
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/{UUID}/address	
root/ConnectionType/xen/general/transparentKeyPassthrough	Kann eingestellt werden auf Translated (Übersetzt) (Local), Direct in full screen desktops only (Nur direkt in Vollbild-Desktops) (FullScreenOnly) oder Direct (Direkt) (Remote). Indirekte Zuordnung zu der Citrix-INI-Dateieinstellung <code>TransparentKeyPassthrough=string</code> , die die Tastaturkürzel-Sequenzen aktiviert, die durch den lokalen Windows Manager in der Sitzung definiert sind. Die Schlüsselwörter sind: Local, Remote und FullScreenOnly. Die Standardeinstellung ist FullScreenOnly .
root/ConnectionType/xen/general/twRedundantImageItems	Regelt die Anzahl der Display-Bereiche, die in Thinwire 2 nachverfolgt werden, um ein überflüssiges Zeichnen von Bitmap-Bildern zu verhindern. Ein angemessener Wert für eine Sitzung mit einer Auflösung von 1024 x 768 ist 300. Sie verwenden mit <code>EnableOSS = False</code> (Falsch), Standard = 0.
root/ConnectionType/xen/general/useAlternateAddress	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>UseAlternateAddress=boolean</code> , die eine alternative Adresse für Firewall-Verbindungen verwendet. Die Standardeinstellung ist False (Falsch). Alle Clients sind standardmäßig auf 0 eingestellt.
root/ConnectionType/xen/general/useBitmapCache	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>PersistentCacheEnabled=boolean</code> . Die Standardeinstellung ist False (Falsch). Alle Clients sind standardmäßig auf 0 eingestellt.
root/ConnectionType/xen/general/useEUKS	Regelt die Verwendung von Extended Unicode Keyboard Support (Erweiterte Unicode-Tastaturunterstützung) auf Windows-Servern. Die Standardeinstellung ist 0 . 0 – Kein EUKS 1 – EUKS als Ausweichoption 2 – EUKS immer verwenden, wenn es möglich ist
root/ConnectionType/xen/general/useLocalIME	Direkte Zuordnung zu der Citrix-INI-Dateieinstellung <code>UseLocalIME=boolean</code> , welche die lokale X-Eingabemethode zur Interpretation der Tastatureingabe

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	verwendet. Dies wird nur für europäische Sprachen unterstützt. Die Standardeinstellung ist True (Wahr). Alle Clients sind standardmäßig auf 1 eingestellt.
root/ConnectionType/xen/general/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/xen/general/webcamSupport	Wählen Sie die geeignete Option für die Verwendung der Webcam. Aktivierung der HDX-Optimierung für die Webcam, Umleitung der Webcam auf VMware Horizon View oder vollständige Deaktivierung der Option.
root/ConnectionType/xen/general/windowHeight	Wenn "windowSize" auf Fixed Size (Feste Größe) eingestellt ist, wird dieser Schlüssel verwendet, um die Höhe des Fensters in Pixel festzulegen.
root/ConnectionType/xen/general/windowPercent	Wenn "WindowType" auf Percentage of Screen Size (Prozentsatz der Bildschirmgröße) eingestellt ist, wird dieser Schlüssel verwendet, um die Größe des Fensters festzulegen. Gültige Werte sind: 0 bis 100.
root/ConnectionType/xen/general/windowSize	Wenn Full Screen (Im Vollbildmodus) (Standard) eingestellt ist, wird die Verbindung auf allen verfügbaren Bildschirmen ohne Ränder maximiert. Wenn Percentage of Screen Size (Prozentsatz der Bildschirmgröße) eingestellt ist, kann der Schlüssel "WindowSizePercentage" verwendet werden, um die Größe des Fensters als Prozentsatz des gesamten Bildschirmbereichs anzugeben. Bei der Einstellung auf Fixed Size (Feste Größe) können die Schlüssel "windowSizeWidth" und "windowSizeHeight" verwendet werden, um die Größe des Fensters in Pixel anzugeben. Damit "Percentage of Screen Size" (Prozentsatz der Bildschirmgröße) wirksam wird, muss "enableForceDirectConnect" auf 1 und "seamlessWindow" auf 0 eingestellt werden. HINWEIS: Diese Einstellung wird nur bei XenApp funktionieren und nur, wenn der Server direkte Verbindungen erlaubt.
root/ConnectionType/xen/general/windowWidth	Wenn "windowSize" auf "Fixed Size" (Feste Größe) eingestellt ist, wird dieser Schlüssel verwendet, um die Breite des Fensters in Pixel festzulegen.
root/ConnectionType/xen/gui/XenDesktopPanel/disabled	Stellen Sie den Wert 1 ein, um den Xen-Desktop-Bedienfeld und seine Taskleiste zu deaktivieren. Wird in der Regel auf 1 eingestellt, wenn AutoStartResource (Ressource automatisch starten) oder AutoStartDesktop (Desktop automatisch starten) aktiviert ist.
root/ConnectionType/xen/gui/XenManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/gui/XenManager/status	Der aktive Status des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/gui/XenManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.

Tabelle E-11 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/gui/XenManager/widgets/address	
root/ConnectionType/xen/gui/XenManager/widgets/applnMenu	
root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop	
root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop	
root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource	
root/ConnectionType/xen/gui/XenManager/widgets/autostart	
root/ConnectionType/xen/gui/XenManager/widgets/domain	
root/ConnectionType/xen/gui/XenManager/widgets/enablePNADesktopIcons	
root/ConnectionType/xen/gui/XenManager/widgets/enablePNASStartMenuItems	
root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection	
root/ConnectionType/xen/gui/XenManager/widgets/folder	
root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon	
root/ConnectionType/xen/gui/XenManager/widgets/isInMenu	
root/ConnectionType/xen/gui/XenManager/widgets/label	
root/ConnectionType/xen/gui/XenManager/widgets/password	
root/ConnectionType/xen/gui/XenManager/widgets/storeFrontConn	
root/ConnectionType/xen/gui/XenManager/widgets/username	
root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork	
root/ConnectionType/xen/gui/fbpanel/autohide	Festlegen, ob die Taskleiste automatisch ausgeblendet werden soll. Mit der Einstellung "true" wird die Taskleiste automatisch ausgeblendet .
root/ConnectionType/xen/gui/fbpanel/edge	Die Standard-Position der Taskleiste, wenn mehr als ein veröffentlichter Desktop oder mehr als eine veröffentlichte Anwendung verfügbar ist.
root/ConnectionType/xen/gui/fbpanel/hidden	Bei Einstellung des Werts auf 1 wird die Taskleiste vollständig ausgeblendet. Kann nur ausgeblendet werden, wenn AutoStartResource (Ressource automatisch starten) oder AutoStartDesktop (Desktop automatisch starten) aktiviert ist.

root > 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.

root > Dashboard

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > Dashboard**.



HINWEIS: Das Dashboard entspricht der Taskleiste. Die Terminologie in der Registrierung wird in einer zukünftigen Version von HP ThinPro überarbeitet.

Tabelle E-12 root > Dashboard

Registrierungsschlüssel	Beschreibung
root/Dashboard/GUI/Clock	Bei Einstellung auf den Standardwert 1 wird die Uhr in der Taskleiste angezeigt.
root/Dashboard/GUI/ConnectionManager	Bei Einstellung auf den Standardwert 1 wird der HP Connection Manager in der Taskleiste angezeigt.
root/Dashboard/GUI/ControlPanel	Bei Einstellung auf den Standardwert 1 wird die Systemsteuerung in der Taskleiste angezeigt.
root/Dashboard/GUI/PowerButton	Bei Einstellung auf den Standardwert 1 wird die Schaltfläche "Ein/Aus" in der Taskleiste angezeigt.
root/Dashboard/GUI/SystemInformation	Bei Einstellung auf den Standardwert 1 wird die Schaltfläche "System Information" in der Taskleiste angezeigt.
root/Dashboard/GUI/SystemTray	Bei Einstellung auf den Standardwert 1 wird der Infobereich in der Taskleiste angezeigt.
root/Dashboard/GUI/TaskBar	Bei Einstellung auf den Standardwert 1 wird die Taskleiste angezeigt.
root/Dashboard/General/AlwaysOnTop	Bei Einstellung auf den Standardwert 1 wird die Taskleiste immer über den anderen Fenstern auf dem Bildschirm angezeigt.
root/Dashboard/General/AutoHide	Dieser Schlüssel regelt die Automatisch-Ausblenden-Funktionen der Taskleiste. Bei Einstellung des Werts auf 1 wird die Taskleiste automatisch ausgeblendet, nachdem der Mauszeiger sie verlassen hat. Bei Einstellung auf den Standardwert 0 ist die Taskleiste immer sichtbar.
root/Dashboard/General/EnterLeaveTimeout	Das Zeitlimit (in Millisekunden), das erforderlich ist, um das Ein- oder Ausblenden der Taskleiste auf dem Bildschirm auszulösen. Diese Option wird nur verwendet, wenn "Automatisch ausblenden" aktiviert ist.
root/Dashboard/General/IconSize	Regelt die Größe der Symbole in der Taskleiste.
root/Dashboard/General/Length	Die Länge des Hauptbereichs der Taskleiste.
root/Dashboard/General/LengthToScreenSide	Bei Einstellung auf den Standardwert 1 ist die Länge der Taskleiste fest und entspricht der Länge der Bildschirmseite, an der sie angeheftet ist. Bei Einstellung des Werts auf 0 wird die Länge automatisch festgelegt.
root/Dashboard/General/PanelDockSide	Die Andockseite des Hauptbereichs der Taskleiste auf dem Bildschirm.

Tabelle E-12 root > Dashboard (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Dashboard/General/RemainPixel	Die sichtbaren Pixel, wenn die Taskleiste in den Bildschirm gleitet.
root/Dashboard/General/SlidingTimeout	Die Zeit (in Millisekunden), die vergeht, wenn die Taskleiste in und aus dem Bildschirm gleitet. Diese Option wird nur verwendet, wenn "Automatisch ausblenden" aktiviert ist.
root/Dashboard/General/Width	Die Breite des Hauptbereichs der Taskleiste.

root > Display

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > Display**.

Tabelle E-13 root > Display

Registrierungsschlüssel	Beschreibung
root/Display/Configuration/displaymode	Gibt den Anzeigemodus der Einheit an. Ein Wert von 0 bezeichnet den Standardmodus (1-4 Monitore), während der Wert 1 einen Modus mit 6 Monitoren bezeichnet. Der HP t610 mit der entsprechenden Add-on-Karte ist die einzige unterstützte Hardware.
root/Display/Configuration/hexlayout	Gibt das Layout in Sechs-Monitor-Modus an. Siehe Displaymodus-Schlüssel.
root/Display/Configuration/hexprofile	Gibt das im Sechs-Monitor-Modus verwendete Profil an. Siehe Displaymodus-Schlüssel.
root/Display/Configuration/primaryprofile	Dies muss immer auf Default (Standard) eingestellt werden.
root/Display/Configuration/quaternarymode	Wenn unterstützt, gibt dies die Position des vierten Monitors in Bezug auf den primären Monitor an. 0 – Selbe wie 1 – Über 2 – Rechts von 3 – Links von 4 – Unten 5 – Keine HINWEIS: Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Der HP t5335z unterstützt keine zwei Monitore.
root/Display/Configuration/quaternaryprofile	Gibt den für den vierten Monitor verwendeten Profilnamen an.
root/Display/Configuration/quaternaryrelative	Zeigt an, welcher Monitor referenziert wird, um die Position des vierten Monitors einzustellen. Siehe Tertiärmodus-Schlüssel.
root/Display/Configuration/secondaryConnector	Gibt den sekundären Anschluss an.
root/Display/Configuration/secondarymode	Wenn unterstützt, gibt dies die Position des sekundären Monitors in Bezug auf den primären Monitor an.

Tabelle E-13 root > Display (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	<p>0 – Selbe wie</p> <p>1 – Über</p> <p>2 – Rechts von</p> <p>3 – Links von</p> <p>4 – Unten</p> <p>5 – Keine</p> <p>HINWEIS: Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Der HP t5335z unterstützt keine zwei Monitore.</p>
root/Display/Configuration/secondaryorientation	
root/Display/Configuration/secondaryprofile	Gibt den Profilnamen an, der für den zweiten Monitor verwendet wird.
root/Display/Configuration/swapstate	Gibt an, welcher Anschluss den Hauptmonitor verbindet. Dies ist Hardware-abhängig und möglicherweise nicht bei allen Modellen implementiert. In der Regel bedeutet 0 , dass der primäre Monitor am VGA-Anschluss ist, und 1 bedeutet, dass er am "anderen" Anschluss ist. Für den HP t5565z bedeutet 0 , dass der primäre Monitor am DVI-I-Anschluss ist, und 1 bedeutet, dass der primäre Monitor am DVI-D-Anschluss ist. Der HP t5335z unterstützt keine zwei Monitore.
root/Display/Configuration/tertiarymode	<p>Wenn unterstützt, gibt dies die Position des dritten Monitors in Bezug auf den primären Monitor an.</p> <p>0 – Selbe wie</p> <p>1 – Über</p> <p>2 – Rechts von</p> <p>3 – Links von</p> <p>4 – Unten</p> <p>5 – Keine</p> <p>HINWEIS: Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Der HP t5335z unterstützt keine zwei Monitore.</p>
root/Display/Configuration/tertiaryprofile	Gibt den Profilnamen für den dritten Monitor an.
root/Display/Configuration/tertiaryrelative	Zeigt an, welcher Monitor referenziert wird, um die Position des dritten Monitors einzustellen. Siehe Tertiärmodus-Schlüssel.
root/Display/Profiles/{UUID}/colorScaling	Die Farbtemperatur oder direkte RGB-Skalierung für ThinClients mit integrierten Monitoren. Der Eintrag ist ein sechsstelliger Hex-Wert RRGGBB, wobei ffffff eine vollständige (100 %) Skalierung auf allen drei Farbkanälen bedeuten würde.
root/Display/Profiles/{UUID}/depth	Die Display-Bittiefe pro Pixel. Eine höhere Bittiefe bedeutet bessere Qualität, aber mehr Daten und somit geringere Leistung.

Tabelle E-13 root > Display (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Display/Profiles/{UUID}/height	Die gewünschte Monitor-Auflösungshöhe. Der Wert 0 bedeutet eine automatische Erkennung der Auflösung.
root/Display/Profiles/{UUID}/label	Display-Profilname. Dies sollte auf default (Standard) eingestellt sein.
root/Display/Profiles/{UUID}/orientation	Gibt die Monitorausrichtung an: 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. Die vom Client unterstützten Werte hängen vom Monitor ab. Der Wert 0 bedeutet eine automatische Erkennung der Bildwiederholungsrate. WICHTIG: Die Auswahl einer Bildwiederholungsrate, die von dem am Client angeschlossenen Monitor nicht unterstützt wird, führt dazu, dass der Bildschirm schwarz bleibt. HP empfiehlt, diese Einstellung auf 0 zu lassen.
root/Display/Profiles/{UUID}/width	Die gewünschte Monitor-Auflösungsbreite. Der Wert 0 bedeutet eine automatische Erkennung der Auflösung.
root/Display/userLock	Wenn der Wert auf 1 eingestellt wird und die Display-Einstellungen vom Benutzer geändert wurden, werden die Display-Einstellungen beibehalten und die Profil-Einstellungen werden verworfen.
root/Display/userLockEngaged	Einstellung des Flags auf 1 nach einer Benutzeränderung. Wenn der Wert auf 1 eingestellt und ein UserLock gesetzt ist, werden die Display-Einstellungen beibehalten und die Profil-Einstellungen werden verworfen. Dieser Schlüssel sollte keine Änderung erfordern.

root > Network

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > Network**.

Tabelle E-14 root > Network

Registrierungsschlüssel	Beschreibung
root/Network/ActiveDirectory/Domain	Active Directory-Domäne.
root/Network/ActiveDirectory/DynamicDNS	Ermöglicht dynamische DNS
root/Network/ActiveDirectory/Enabled	Aktiviert Active Directory.
root/Network/ActiveDirectory/Method	Die Methode, die zur Bereitstellung von Anmeldeinformationen verwendet wird.
root/Network/ActiveDirectory/Password	Benutzerpasswort für Active Directory-Domäne, gilt nur in statischer Methode.

Tabelle E-14 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/ActiveDirectory/Username	Benutzername für Active Directory-Domäne, gilt nur in statischer Methode.
root/Network/DNSServers	Hier kann ein zusätzlicher DNS-Server für die Auflösung des Domänennamens angegeben werden. Die angegebenen Server werden zusätzlich zu jeglichen über DHCP abgerufenen Servern verwendet. Es können bis zu drei IPv4- oder IPv6-Adressen, durch Kommas getrennt, angegeben werden.
root/Network/DefaultHostnamePattern	Gibt das Standard-Hostnamensmuster an, das ein Thin Client verwendet, um einen neuen Hostnamen zu generieren, wenn der Registrierungsschlüssel für den Hostnamen und der Hostname in /etc/hostname beide leer sind. Verwenden Sie im Muster % als Trennzeichen. Zum Beispiel bedeutet das Format HPTC%MAC:1-6%, dass HPTC das Präfix ist und der Thin Client MAC für die Zeichen 1-6 verwendet wird. Somit generiert die Thin Client MAC-Adresse 11:22:33:44:55:66 den Hostnamen HPTC112233.
root/Network/FtpProxy	FTP-Proxy-Adresse.
root/Network/Hostname	Host-Name des Clients.
root/Network/HttpProxy	HTTP-Proxy-Adresse.
root/Network/HttpsProxy	HTTPS-Proxy-Adresse.
root/Network/IPSec/IPSecRules/{UUID}/DstAddr	Zieladresse für die IPsec-Regel.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethod	Authentifizierungsmethode für die IPsec-Regel. Geben Sie PSK ein, um einen Pre-Shared-Schlüssel zu verwenden und geben Sie Certificate (Zertifikat) ein, um Zertifikat-Dateien zu verwenden.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethodCACert	Wenn die Authentifizierungsmethode "Certificate" lautet, wird der Dateipfad für das CA-Zertifikat in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethodClientCert	Wenn die Authentifizierungsmethode "Certificate" lautet, wird der Dateipfad für das Zertifikat in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID} / MMAuthMethodPresharedKey	Wenn die Authentifizierungsmethode "PSK" lautet, wird der Wert für den Pre-Shared-Key in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID}/MMAuthMethodPrivateKey	Wenn die Authentifizierungsmethode "Certificate" lautet, wird der Pfad der Client-Zertifikatsdatei, der zu der entsprechenden privaten Schlüsseldatei in diesem Schlüssel gespeichert.
root/Network/IPSec/IPSecRules/{UUID}/MMDHGroup	Phase 1 Diffie-Hellman-Gruppe
root/Network/IPSec/IPSecRules/{UUID}/MMEncryptionAlg	Phase 1 Verschlüsselungsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/MMIntegrityAlg	Phase 1 Integritätsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/MMLifetimeMinutes	Phase 1 Lebensdauer
root/Network/IPSec/IPSecRules/{UUID}/QMAHEnable	Ermöglicht Phase 2 AH.
root/Network/IPSec/IPSecRules/{UUID}/QMAHIntegrityAlg	Phase 2 AH Integritätsalgorithmus.

Tabelle E-14 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/IPSec/IPSecRules/{UUID}/QMESPEnable	Ermöglicht Phase 2 ESP.
root/Network/IPSec/IPSecRules/{UUID}/QMESPEncryptionAlg	Phase 2 ESP Verschlüsselungsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/QMESPIntegrityAlg	Phase 2 ESP Integritätsalgorithmus.
root/Network/IPSec/IPSecRules/{UUID}/QMLifetimeSeconds	Phase 2 Lebensdauer
root/Network/IPSec/IPSecRules/{UUID}/RuleDescription	Beschreibung für die IPsec Regel ein, wie z. B. den Zweck zum Erstellen der Regel.
root/Network/IPSec/IPSecRules/{UUID}/RuleEnable	Kennzeichen für Regel aktivieren oder deaktivieren. Wenn dies auf 1 eingerichtet ist, wird die Regel aktiviert. Richten Sie auf 0 ein, um die Regel zu deaktivieren.
root/Network/IPSec/IPSecRules/{UUID}/RuleName	Name der IPsec-Regel.
root/Network/IPSec/IPSecRules/{UUID}/SrcAddr	Quell-Adresse für die IPsec Regel.
root/Network/IPSec/IPSecRules/{UUID}/TunnelDstAddr	Tunnel-Zieladresse für die IPsec-Regel.
root/Network/IPSec/IPSecRules/{UUID}/TunnelEnable	Ermöglicht Tunnel-Einstellung für die IPsec-Regel. Wenn diese Option aktiviert ist, lautet die Regel "Anwenden auf Tunnelmodus".
root/Network/IPSec/IPSecRules/{UUID}/TunnelSrcAddr	Tunnel-Quell-Adresse für die IPsec Regel.
root/Network/SearchDomains	Zusätzliche Suchdomänen für die FQDN-Auflösung können hier angegeben werden. Die angegebenen Domänen werden an alle unvollständigen Serverdefinitionen angehängt, um zu versuchen, einen FQDN zu erzeugen, der über DNS aufgelöst werden kann. Ein Beispiel: eine Suchdomäne von "mydomain.com" erlaubt der Serverdefinition "myserver" die korrekte Auflösung für "myserver.mydomain.com", auch wenn der DSN-Server "myserver" nicht in seinen Namensauflösungstabellen hat. Es können bis zu fünf zusätzliche Suchdomänen angegeben werden.
root/Network/VPN/AutoStart	Startet VPN beim Systemstart automatisch.
root/Network/VPN/Domain	VPN-Domäne.
root/Network/VPN/Gateway	VPN-Gateway.
root/Network/VPN/Group	VPN-Gruppe.
root/Network/VPN/GroupPassword	VPN-Gruppenkennwort
root/Network/VPN/Password	VPN-Benutzerkennwort
root/Network/VPN/Type	VPN-Type.
root/Network/VPN/Username	VPN-Benutzername.
root/Network/VPN/vpncSecurity	VPNC-Sicherheitsstufe.
root/Network/Wired/DefaultGateway	Das Standard-Gateway, das vom Gerät für die Kommunikation mit dem Internet verwendet wird. In der Regel ist dies die Routeradresse. HINWEIS: Diese Einstellung wird nur wirksam, wenn "Method" (Methode) auf "Static" (Statisch) eingestellt ist.

Tabelle E-14 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/Wired/EnambeDefGatewayasDNS	Bei Einstellung des Werts auf 1 ist das Standard-Gateway der Nameserver.
root/Network/Wired/EthernetSpeed	Die Verbindungsgeschwindigkeit der primären Ethernet-Netzwerkschnittstelle. Automatische Auswahl der schnellsten verfügbaren Verbindungsgeschwindigkeit (in der Regel 1 Gbit/s oder 100 Mbit/s, je nach Switch). 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	Die IPv4-Adresse des Geräts. Diese Einstellung wird nur dann wirksam, wenn "Method" (Methode) auf "Static" (Statisch) eingerichtet ist.
root/Network/Wired/IPv6Enable	Richten Sie diesen Schlüssel auf 1 ein, wenn Sie in einer IPv6-Umgebung arbeiten.
root/Network/Wired/Interface	Die Standard-Ethernet-Schnittstelle oder NIC.
root/Network/Wired/MTU	Richten Sie für eine MTU bei einer kabelgebundenen Verbindung ein, ob sie eine statische Adresse oder eine über DHCP erworbene IP-Adresse verwendet.
root/Network/Wired/Method	Bei der Einstellung Automatic wird das Gerät DHCP verwenden und versuchen, die Netzwerkeinstellungen abzurufen. Bei der Einstellung Static können "IPAddress", "SubnetMask" und "DefaultGateway" mithilfe der verfügbaren Schlüssel manuell eingerichtet werden. HP rät von der Verwendung von "Static" in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients die gleiche IP-Adresse erhalten.
root/Network/Wired/Security/CACert	Pfad zu der CA-Zertifizierungsdatei.
root/Network/Wired/Security/Identity	Identität oder anonyme Identität.
root/Network/Wired/Security/InnerAuth	PEAP innere Authentifizierungsprotokolle.
root/Network/Wired/Security/InnerAuthTTLS	TTLS innere Authentifizierungsprotokolle.
root/Network/Wired/Security/PEAPVersion	PEAP-Version.
root/Network/Wired/Security/Password	Kenntwort.
root/Network/Wired/Security/PrivateKey	Pfad zu der privaten Schlüsseldatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wired/Security/Type	Kabelgebundene 802.1x-Authentifizierungstypen.
root/Network/Wired/Security/UserCert	Pfad zu der Benutzerzertifizierungsdatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wired/Security/Username	Benutzername.
root/Network/Wired/SubnetMask	Die Subnetzmaske des Geräts. Zum Beispiel 255.255.255.0 für ein Standard-Subnetz der Klasse C. Diese Einstellung wird nur dann wirksam, wenn "Method" (Methode) auf "Static" (Statisch) eingerichtet ist.
root/Network/Wireless/DefaultGateway	Das Standard-Gateway, das das Gerät für die Kommunikation mit dem Internet verwendet. In der Regel ist

Tabelle E-14 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	dies die Adresse des Routers. Diese Einstellung wird nur dann wirksam, wenn "Method" (Methode) auf "Static" (Statisch) eingerichtet ist.
root/Network/Wireless/EnableDefGatewayAsDNS	Bei Einstellung des Werts auf 1 ist das Standard-Gateway der Nameserver.
root/Network/Wireless/IPAddress	Die IPv4-Adresse des Geräts. Diese Einstellung wird nur wirksam, wenn "Method" (Methode) auf "Static" (Statisch) eingestellt ist.
root/Network/Wireless/IPv6Enable	Richten Sie diesen Schlüssel auf 1 ein, wenn Sie in einer IPv6-Umgebung arbeiten.
root/Network/Wireless/Interface	Die drahtlose Standardschnittstelle oder der Wireless-Netzwerkadapter.
root/Network/Wireless/Method	Bei der Einstellung Automatic wird das Gerät DHCP verwenden und versuchen, die Netzwerkeinstellungen abzurufen. Bei der Einstellung auf "Static" können "IPAddress", "SubnetMask" und "DefaultGateway" mithilfe der verfügbaren Schlüssel manuell eingerichtet werden. HP rät von der Verwendung von "Static" in einem generischen Client-Profil ab, da dies dazu führt, dass alle Clients die gleiche IP-Adresse erhalten.
root/Network/Wireless/PowerEnable	Richten Sie diesen Schlüssel auf 0 ein, um das Energiemanagement der Wireless-Netzwerkkarte zu deaktivieren.
root/Network/Wireless/SSID	Die ausgewählte WLAN-Access Point-SSID.
root/Network/Wireless/SSIDHidden	Der ausgeblendete Status der ausgewählten WLAN-Access Point-SSID.
root/Network/Wireless/Security/CACert	Pfad zu der CA-Zertifizierungsdatei.
root/Network/Wireless/Security/EAPFASTPAC	Pfad zur PAC-Datei der EAP-FAST-Authentifizierung.
root/Network/Wireless/Security/EAPFASTProvision	EAP-FAST-Authentifizierung – Option zur schnellen Bereitstellung.
root/Network/Wireless/Security/Identity	Identität oder anonyme Identität.
root/Network/Wireless/Security/InnerAuth	PEAP innere Authentifizierungsprotokolle.
root/Network/Wireless/Security/InnerAuthTTLS	TTLS innere Authentifizierungsprotokolle.
root/Network/Wireless/Security/PEAPVersion	PEAP-Version.
Root/Netzwerk/Wireless/Security/Password	Kennwort.
root/Network/Wireless/Security/PrivateKey	Pfad zu der privaten Schlüsseldatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wireless/Security/Type	Drahtlos-Authentifizierungstypen.
root/Network/Wireless/Security/UserCert	Pfad zu der Benutzerzertifizierungsdatei, nur zur Verwendung bei der TLS-Authentifizierung.
root/Network/Wireless/Security/Username	Benutzername.
root/Network/Wireless/Security/WEPAuth	WEP-Authentifizierungstyp.
root/Network/Wireless/Security/WEPIndex	WEP-Kennwortindex, nur für WEP.

Tabelle E-14 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/Wireless/SubnetMask	Die Subnetzmaske des Geräts. Zum Beispiel 255.255.255.0 (für ein Standard-Subnetz der Klasse C). Diese Einstellung wird nur dann wirksam, wenn "Method" (Methode) auf "Static" (Statisch) eingerichtet ist.
root/Network/disableLeftClickMenu	Deaktiviert das beim Klicken auf das Netzwerksymbol in der Taskleiste angezeigte Menü, welches das Starten, Stoppen und Deaktivieren der Netzwerkverbindung ermöglicht.
root/Network/disableRightClickMenu	Deaktiviert das Rechtsklick-Kontextmenü auf dem Netzwerk-Infobereich-Symbol, mit dem Sie die Netzwerkverbindung starten, stoppen und neustarten können.
root/Network/iPeak/ShowStatus	Bei Einstellung des Werts auf 1 zeigt der Network Manager den HP Velocity-Status im Infobereich-Symbol an.
root/Network/iPeak/Status	Bei Einstellung des Werts auf 1 ist HP Velocity aktiviert. Wenn es aktiviert ist, hat dies keine Auswirkungen auf die Netzwerk-Paketübertragung, wenn die serverseitige Komponente nicht erkannt wird. Bei Einstellung des Werts auf 2 befindet sich HP Velocity im Überwachungsmodus und überwacht nur den Netzwerkstatus.
root/Network/userLock	Bei Einstellung des Werts auf 1 und die Anzeigeeinstellungen vom Benutzer geändert wurden, werden die Anzeigeeinstellungen beibehalten und die Einstellungen des Profils werden verworfen.
root/Network/userLockEngaged	Das Kennzeichen wird nach einer Änderung durch den Benutzer auf 1 eingestellt. Bei Einstellung des Werts auf 1 und userLock gesetzt ist, werden die Anzeigeeinstellungen beibehalten und die Einstellungen der Profile werden verworfen. Dieser Schlüssel sollte keine Änderung erfordern.

root > SCIM

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > SCIM**.

Tabelle E-15 root > SCIM

Registrierungsschlüssel	Beschreibung
root/SCIM/ScimEnabled	Bei Einstellung des Werts auf 1 ist SCIM für CJK-Eingabe aktiviert. HINWEIS: Dieser Schlüssel ist nur vorhanden, wenn das Client-Kit für ostasiatische Sprachen installiert ist.

root > Serial

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > Serial**.

Tabelle E-16 root > Serial

Registrierungsschlüssel	Beschreibung
root/Serial/{UUID}/baud	Die Geschwindigkeit des seriellen Geräts.
root/Serial/{UUID}/dataBits	Zeigt an, wie viele Bits in den einzelnen Zeichen der Datenbits des seriellen Geräts enthalten sind.
root/Serial/{UUID}/device	Das serielle Gerät, das am System angeschlossen ist.
root/Serial/{UUID}/flow	Die Flusssteuerung des seriellen Geräts, die das Starten und Anhalten der seriellen Kommunikation kommuniziert.
root/Serial/{UUID}/name	Der Windows-Geräte-Port, der für die Kommunikation mit dem seriellen Gerät verwendet wird.
root/Serial/{UUID}/parity	Das Paritätsbit des seriellen Geräts, das zur Fehlererkennung verwendet wird. Die Einstellung none bedeutet, es gibt keine Paritätserkennung.

root > SystemInfo

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > SystemInfo**.

Tabelle E-17 root > SystemInfo

Registrierungsschlüssel	Beschreibung
root/SystemInfo/Pages/General	Aktiviert oder deaktiviert die Registerkarte "General" (Allgemeines). Bei Einstellung des Werts auf 0 können Benutzer diese Registerkarte im Bereich Systeminformation nicht sehen.
root/SystemInfo/Pages/NetTools	Aktiviert oder deaktiviert die Registerkarte Netzwerktools. Bei Einstellung des Werts auf 0 können die Benutzer diese Registerkarte im Bereich Systeminformationen nicht sehen.
root/SystemInfo/Pages/Network	Aktiviert oder deaktiviert die Registerkarte Netzwerk. Bei Einstellung des Werts auf 0 können die Benutzer diese Registerkarte im Bereich Systeminformationen nicht sehen.
root/SystemInfo/Pages/SoftwareInformation	Aktiviert oder deaktiviert die Registerkarte Systeminformationen. Bei Einstellung des Werts auf 0 können die Benutzer diese Registerkarte im Bereich Systeminformationen nicht sehen.
root/SystemInfo/Pages/SystemLogs	Aktiviert oder deaktiviert die Registerkarte System-Logs. Bei Einstellung des Werts auf 0 können die Benutzer diese Registerkarte im Bereich Systeminformationen nicht sehen.
root/SystemInfo/authorized	Aktiviert die Systeminformationen-Schaltfläche im ThinPro-Kontrollzentrum.

root > TaskMgr

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > TaskMgr**.

Tabelle E-18 root > TaskMgr

Registrierungsschlüssel	Beschreibung
root/TaskMgr/General/AlwaysOnTop	Legt fest, dass das Task-Manager-Fenster immer oben angezeigt wird.

root > USB

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > USB**.

Tabelle E-19 root > USB

Registrierungsschlüssel	Beschreibung
root/USB/Classes/<Defined at Interface level>/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/<Defined at Interface level>/DisplayName	Name der USB-Klasse.
root/USB/Classes/<Defined at Interface level>/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/<Defined at Interface level>/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Application Specific Interface/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Application Specific Interface/DisplayName	Name der USB-Klasse.
root/USB/Classes/Application Specific Interface/Status	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Application Specific Interface/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Audio/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Audio/DisplayName	Name der USB-Klasse.
root/USB/Classes/Audio/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Audio/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Audio and Video Devices/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Audio and Video Devices/DisplayName	Name der USB-Klasse.
root/USB/Classes/Audio and Video Devices/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Audio and Video Devices/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/CDC Data/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/CDC Data/DisplayName	Name der USB-Klasse.
root/USB/Classes/CDC Data/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.

Tabelle E-19 root > USB (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/USB/Classes/CDC Data/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Communications/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Communications/DisplayName	Name der USB-Klasse.
root/USB/Classes/Communications/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Communications/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Content Security/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Content Security/DisplayName	Name der USB-Klasse.
root/USB/Classes/Content Security/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Content Security/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Diagnostic Device/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Diagnostic Device/DisplayName	Name der USB-Klasse.
root/USB/Classes/Diagnostic Device/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Diagnostic Device/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Hub/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Hub/DisplayName	Name der USB-Klasse.
root/USB/Classes/Hub/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Hub/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Human Interface Device/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Human Interface Device/DisplayName	Name der USB-Klasse.
root/USB/Classes/Human Interface Device/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Human Interface Device/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Imaging/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Imaging/DisplayName	Name der USB-Klasse.
root/USB/Classes/Imaging/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Imaging/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Mass Storage/ClassID	ID-Nummer der USB-Klasse.

Tabelle E-19 root > USB (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/USB/Classes/Mass Storage/DisplayName	Name der USB-Klasse.
root/USB/Classes/Mass Storage/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Mass Storage/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Miscellaneous Device/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Miscellaneous Device/DisplayName	Name der USB-Klasse.
root/USB/Classes/Miscellaneous Device/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Miscellaneous Device/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Personal Healthcare/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Personal Healthcare/DisplayName	Name der USB-Klasse.
root/USB/Classes/Personal Healthcare/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Personal Healthcare/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Physical Interface Device/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Physical Interface Device/DisplayName	Name der USB-Klasse.
root/USB/Classes/Physical Interface Device/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Physical Interface Device/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Printer/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Printer/DisplayName	Name der USB-Klasse.
root/USB/Classes/Printer/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Printer/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/ShowTab	Bei der Einstellung auf 1 wird die Registerkarte Klassen in der Benutzeroberfläche des USB-Manager angezeigt.
root/USB/Classes/Smart Card/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Smart Card/DisplayName	Name der USB-Klasse.
root/USB/Classes/Smart Card/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Smart Card/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Vendor Specific Class/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Vendor Specific Class/DisplayName	Name der USB-Klasse.

Tabelle E-19 root > USB (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/USB/Classes/Vendor Specific Class/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Vendor Specific Class/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Video/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Video/DisplayName	Name der USB-Klasse.
root/USB/Classes/Video/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Video/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Classes/Wireless/ClassID	ID-Nummer der USB-Klasse.
root/USB/Classes/Wireless/DisplayName	Name der USB-Klasse.
root/USB/Classes/Wireless/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist.
root/USB/Classes/Wireless/Visible	Gibt an, ob die Klasse auf der Benutzeroberfläche angezeigt, nicht angezeigt oder deaktiviert wird.
root/USB/Devices/{UUID}/DisplayName	Der Name, der in der Benutzeroberfläche im USB-Manager angezeigt wird. Falls keine Angabe gemacht wird, versucht der USB-Manager, anhand der Geräteinformationen einen entsprechenden zu generieren.
root/USB/Devices/{UUID}/ProductID	Produkt-ID des Geräts.
root/USB/Devices/{UUID}/State	Gibt an, ob diese Klasse dem Remotecomputer zugeordnet ist. Bei Einstellung 0 erfolgt keine Umleitung. Bei Einstellung 1 werden Standardwerte verwendet. Bei Einstellung 2 wird umgeleitet.
root/USB/Devices/{UUID}/VendorID	Lieferanten-ID des Geräts.
root/USB/root/holdProtocolStatic	Bei Einstellung des Werts auf 1 wird das remote USB-Protokoll nicht auf der Grundlage des ausgewählten Wertes gewechselt. Belassen Sie diese Einstellung immer auf dem Wert in root/protocol.
root/USB/root/mass-storage/allowed	Bei Einstellung des Werts auf 1 werden Massenspeichergeräte automatisch bereitgestellt, wenn das Protokoll "local" lautet.
root/USB/root/mass-storage/read-only	Bei Einstellung des Werts auf 1 werden Massenspeichergeräte schreibgeschützt, wenn sie automatisch lokal bereitgestellt werden.
root/USB/root/opendebug	Bei Einstellung des Werts auf 1 wird eine Debug-Meldung in /tmp/USB-mgr-log geschrieben.
root/USB/root/protocol	Nachverfolgung der aktuellen Eigentümer des Remote-USB. Wird nur intern verwendet.

root > auto-update

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner `root > auto-update`.

Tabelle E-20 root > auto-update

Registrierungsschlüssel	Beschreibung
root/auto-update/DNSAliasDir	Gibt das voreingestellte Stammverzeichnis auf dem SCS-Server für den DNS-Alias-Modus an.
root/auto-update/ManualUpdate	Einrichten auf 1 , um die Überprüfung der DHCP-Kennung und des DNS-Alias, das Senden für Automatic Update-Server-URLs und das manuelle Einrichten des Automatic Update-Servers zu deaktivieren. Wenn dies eingestellt ist, müssen Kennwort, Pfad, Protokoll, Benutzer und ServerURL festgelegt sein, um sicherzustellen, dass der Update-Server bekannt ist.
root/auto-update/ScheduledScan/Enabled	Einrichten auf 1 , damit die Clients in regelmäßigen Abständen Scans des Automatic Update-Servers durchführen und nach Aktualisierungen suchen. Bei Einstellung des Werts auf 0 suchen die Clients nur beim Systemstart nach Aktualisierungen.
root/auto-update/ScheduledScan/Interval	Die Zeit, die zwischen geplanten Update-Scans gewartet werden soll. Geben Sie den Zeitraum im Format HH:MM an. Intervalle können mit mehr als 24 Stunden angegeben werden. Um beispielsweise Aktualisierungen für alle 48 Stunden zu planen, stellen Sie das Intervalls auf 48:00 ein.
root/auto-update/ScheduledScan/Period	Während des definierten Zeitraums aktivieren die Clients den geplanten Scan nach dem Zufallsprinzip. Mit einem langen Zeitraum verhindern Sie Situationen, in denen alle Clients gleichzeitig aktualisieren, wodurch eine Netzwerküberlastung verursacht werden kann. Geben Sie den Zeitraum im Format HH:MM an. Um beispielsweise die Client-Aktualisierungen über einen Zeitraum von 2,5 Stunden zu verteilen, stellen Sie den Zeitraum auf 02:30 ein.
root/auto-update/ScheduledScan/StartTime	Der Start des ersten geplanten Scans im Format HH:MM mit 24-Stunden-Zeitformat. So wird z. B. 4:35 pm als 16:35 eingegeben.
root/auto-update/ServerURL	Die IP oder der Domänenname des Update-Servers, die bzw. der verwendet wird, wenn ManualUpdate aktiviert ist.
root/auto-update/enableOnBootup	Einrichten auf 0 , um die automatische Aktualisierung beim Systemstart zu deaktivieren. Der Standardwert ist 1 , wodurch Automatic Update nach System-Updates suchen darf.
root/auto-update/gui/auto-update/ManualUpdate	Zum Einstellen des Status für das Widget Enable manual configuration (Manuelle Konfiguration aktivieren) in der Automatic Update-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/gui/auto-update/ServerURL	Zum Einstellen des Status für das Widget Server in der Automatic Update-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der

Tabelle E-20 root > auto-update (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/gui/auto-update/enableOnBootup	Zum Einstellen des Status für das Widget Enable manual configuration (Manuelle Konfiguration aktivieren) in der Automatic Update-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/gui/auto-update/password	Zum Einstellen des Status für das Widget Password (Kennwort) in der Automatic Update-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/gui/auto-update/protocol	Zum Einstellen des Status für das Widget Protocol (Protokoll) in der Automatic Update-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/gui/auto-update/tag	Dieser Schlüssel hat keine Funktion.
root/auto-update/gui/auto-update/user	Zum Einstellen des Status für das Widget User name (Benutzername) in der Automatic Update-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/auto-update/password	Das gewünschte Kennwort, wenn ManualUpdate aktiviert ist. Dies wird nur dann verwendet, wenn das Protokoll auf ftp eingestellt ist. Dieses Feld wird verschlüsselt im Profil gespeichert.
root/auto-update/path	Der gewünschte relative Pfad von der Standard-Server-URL, wenn ManualUpdate aktiviert ist. Dies ist normalerweise leer oder auf auto-update eingestellt.
root/auto-update/protocol	Einrichten auf ftp , http oder https , um das gewünschte Aktualisierungsserver-Protokoll zu definieren, wenn Manualupdate aktiviert ist.
root/auto-update/tag	Hiermit wurde früher die Kennungsnummer für DHCP 137 angegeben. Dies ist mittlerweile veraltet und wird nicht erkannt.
root/auto-update/user	Der gewünschte Benutzer, wenn ManualUpdate aktiviert ist. Dies wird nur dann verwendet, wenn das Protokoll auf ftp eingestellt ist.

root > background

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > background**.

Tabelle E-21 root > background

Registrierungsschlüssel	Beschreibung
root/background/desktop/color	Durch die Einstellung none für das Design, ist dieser Schlüssel die Standardfarbe, die das benutzerdefinierte Design verwendet. Wenn die Design-Einstellung nicht "none" ist, hat diese Einstellung keine Funktion.
root/background/desktop/imagePath	Durch die Einstellung none für das Design, ist dieser Schlüssel der vom benutzerdefinierten Design verwendete Desktop-Hintergrundbild-Pfad. Wenn die Design-Einstellung nicht "none" ist, hat diese Einstellung keine Funktion.
root/background/desktop/lastBrowseDir	Durch die Einstellung none für das Design, ist dieser Schlüssel das zuletzt verwendete Verzeichnis. Wenn die Design-Einstellung nicht "none" ist, hat diese Einstellung keine Funktion.
root/background/desktop/style	Durch die Einstellung none für das Design, definiert dieser Schlüssel, wie das Bild auf dem Desktop erscheint. Wenn die Design-Einstellung nicht "none" ist, hat diese Einstellung keine Funktion.
root/background/desktop/theme	Die System-Design-Einstellung. Dieser Wert wird über die GUI eingerichtet. Gültigen Einstellungen werden bei den Designs aufgeführt, die auf dem System vorhanden sind. Setzen Sie die Einstellung auf none , damit der Benutzer das Design definieren kann.

root > config-wizard

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > config-wizard**.

Tabelle E-22 root > config-wizard

Registrierungsschlüssel	Beschreibung
root/config-wizard/FirmwareUpdate/firmwareUpdateTimeout	Die Zeitlimit-Dauer (in Sekunden), die der Thin Client nach Updates sucht. Stellen Sie den Wert -1 für kein Zeitlimit ein.
root/config-wizard/FirmwareUpdate/firmwareUpdateURL	Die FTP-URL für Image-Aktualisierungen.
root/config-wizard/enableConnectionCheck	Bei Einstellung des Werts auf 0 ist die Prüfung der Verbindungssitzung deaktiviert. Bei Einstellung auf den Standardwert 1 ist die Prüfung der Verbindungssitzung beim Systemstart aktiviert.
root/config-wizard/enableNetworkCheck	Bei Einstellung des Werts auf 0 ist die Netzwerk-Prüfung deaktiviert. Bei Einstellung auf den Standardwert 1 ist die Netzwerk-Prüfung beim Systemstart aktiviert.
root/config-wizard/updateCheck	Bei Einstellung des Werts auf 1 ist die Update-Prüfung aktiviert. Der Standardwert 0 deaktiviert die Update-Prüfung beim Systemstart.

root > desktop

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > desktop**.

Tabelle E-23 root > desktop

Registrierungsschlüssel	Beschreibung
root/desktop/shortcuts/default-Close/command	Gibt den Befehl an.
root/desktop/shortcuts/default-Close/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/default-Lock/command	Gibt den Befehl an.
root/desktop/shortcuts/default-Lock/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/default-MaximizeWindow/command	Gibt den Befehl an.
root/desktop/shortcuts/default-MaximizeWindow/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/default-MinimizeAll/command	Gibt den Befehl an.
root/desktop/shortcuts/default-MinimizeAll/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/default-MinimizeWindow/command	Gibt den Befehl an.
root/desktop/shortcuts/default-MinimizeWindow/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/default-NextWindow/command	Gibt den Befehl an.
root/desktop/shortcuts/default-NextWindow/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/default-Shutdown/command	Gibt den Befehl an.
root/desktop/shortcuts/default-Shutdown/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/default-ToggleFullscreen/command	Gibt den Befehl an.
root/desktop/shortcuts/default-ToggleFullscreen/shortcut	Gibt den Verknüpfungsnamen an.
root/desktop/shortcuts/reset-display-prefs/command	Gibt den Befehl an.
root/desktop/shortcuts/reset-display-prefs/shortcut	Gibt den Verknüpfungsnamen an.

root > entries

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > entries**.

Tabelle E-24 root > entries

Registrierungsschlüssel	Beschreibung
root/entries/{UUID}/command	
root/entries/{UUID}/folder	
root/entries/{UUID}/icon	
root/entries/{UUID}/label	
root/entries/{UUID}/metaInfo	

Table E-24 root > entries (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/entries/{UUID}/onDesktop	
root/entries/{UUID}/onMenu	

root > keyboard

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > keyboard**.

Table E-25 root > keyboard

Registrierungsschlüssel	Beschreibung
root/keyboard/SystrayMenu/keyboardLayout	Bei Einstellung auf den Standardwert 1 bietet das Rechtsklick-Kontextmenü im Tastatur-Systeminfo-Symbol eine Option zum Öffnen des Tastaturlayout-Dienstprogramms.
root/keyboard/SystrayMenu/languages	Bei Einstellung auf den Standardwert 1 bietet das Rechtsklick-Kontextmenü im Tastatur-Systeminfo-Symbol eine Option zum Öffnen des Sprachauswahl-Dienstprogramms.
root/keyboard/SystrayMenu/virtualKeyboard	Bei Einstellung auf den Standardwert 1 bietet das Rechtsklick-Kontextmenü im Tastatur-Systeminfo-Symbol eine Option zum Öffnen der virtuellen Tastatur.
root/keyboard/VisibleInSystray	Bei Einstellung auf den Standardwert 1 wird in der Systeminformation das aktuelle Tastaturlayout angezeigt.
root/keyboard/XkbLayout	Ein interner Schlüssel, der verwendet wird, um das Modell/Layout einem XKB-Tastaturlayout zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbModel	Ein interner Schlüssel, der dazu verwendet wird, das Modell/Layout einem XKB-Tastaturmodell zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbOptions	Ein interner Schlüssel, der dazu verwendet wird, das Modell/Layout zu XKB-Tastaturoptionen zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbVariant	Ein interner Schlüssel, der dazu verwendet wird, das Modell/Layout einer XKB-Tastaturvariante zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/enable2	Bei Einstellung des Werts auf 1 kann die sekundäre Tastatur "layout2" umgestellt werden durch die Tastenkombination, die durch "switch" definiert wurde.
root/keyboard/layout	Das Tastaturlayout definiert, welche Symbole die Tasten generieren. Dies hängt häufig von der jeweiligen Sprache ab. Englisch (en), Spanisch (es), Französisch (fr), Deutsch (de), und Japanisch (jp) sind die häufigsten Layouts.
root/keyboard/layout2	Das sekundäre Tastaturlayout.
root/keyboard/model	Das Tastaturmodell definiert, welche Tasten sich wo auf der Tastatur befinden. Am häufigsten ist der Standard "pc104"

Tabelle E-25 root > keyboard (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	oder "pc105" für International. Andere Modelle werden ebenfalls unterstützt.
root/keyboard/model2	Das sekundäre Tastaturmodell.
root/keyboard/numlock	Wenn dies auf die Standardeinstellung 1 gesetzt wird, wird die NUM-Funktion beim Systemstart eingeschaltet. Andernfalls wird die NUM-Led ausgeschaltet.
root/keyboard/rdp_kb	Ein interner Schlüssel, der dazu verwendet wird, das Modell/ Layout einer RDP-Tastaturkarte zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/switch	Wird dazu verwendet, die Tastenkombination zum Umschalten zwischen dem ersten und zweiten Layout, zu verwenden, wenn "enable2" gesetzt ist. Gültige Werte sind grp:ctrl_shift_toggle , grp:ctrl_alt_toggle und grp:alt_shift_toggle .
root/keyboard/variant	Die Tastaturvariante definiert leichte Abweichungen im Layout. In der Regel wird die Abweichung wcompat verwendet, da sie am nächsten mit den Windows Tastaturlayouts übereinstimmt.
root/keyboard/variant2	Die sekundäre Tastaturvariante.

root > logging

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > logging**.

Tabelle E-26 root > logging

Registrierungsschlüssel	Beschreibung
root/logging/general/debug	Bei Einstellung des Werts auf 1 ist Debugging auf allen unterstützten Debug-Subsystemen aktiviert. Dies wird gewöhnlich in Verbindung mit "generateDiagnostic.sh" oder mit dem Diagnosetool "Systeminformationen" verwendet, um ein Diagnosepaket mit Systemdebugging-Protokollen zu erzeugen.

root > mouse

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > mouse**.

Tabelle E-27 root > mouse

Registrierungsschlüssel	Beschreibung
root/mouse/MouseHandedness	Ob die Maus rechts- oder linkshändig ist. 0 für Rechtshänder, 1 für Linkshänder.
root/mouse/MouseSpeed	Die Beschleunigung des Mauszeigers. In der Regel ist eine Zahl von 0-25 der nutzbare Bereich. 0 wird die

Tabelle E-27 root > mouse (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Beschleunigung vollständig deaktivieren. Dadurch bewegt sich der Mauszeiger ständig langsam, aber messbar.
root/mouse/MouseThreshold	Die Anzahl der Pixel vor Beginn der Beschleunigung ist aktiviert. 0 richtet die Beschleunigung auf eine natürliche Kurve ein, die allmählich die Beschleunigung skaliert und damit präzise und zugleich schnelle Bewegungen erlaubt.

root > screensaver

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > screensaver**.

Tabelle E-28 root > screensaver

Registrierungsschlüssel	Beschreibung
root/screensaver/ctrlbindkey	Stellen Sie den Wert 1 ein, um die Display-Sperre zu starten.
root/screensaver/enableCustomLogo	Stellen Sie den Wert 1 ein, um ein benutzerdefiniertes Bild für die Display-Sperre zu verwenden.
root/screensaver/enableDPMS	Stellen Sie den Wert 0 ein, um die Monitor-Energieverwaltung zu deaktivieren. Dies bewirkt, dass den Monitor eingeschaltet bleibt, bis er manuell ausgeschaltet wird.
root/screensaver/enableScreensaver	Stellen Sie den Wert 1 ein, um den Bildschirmschoner zu aktivieren.
root/screensaver/enableSleep	Stellen Sie den Wert 0 ein, um den Energiesparmodus zu deaktivieren.
root/screensaver/lockScreen	Stellen Sie den Wert 1 ein, um ein Kennwort anzufordern, wenn der Benutzer aus dem gesperrten Bildschirmstatus in den normalen Arbeitsstatus wechselt.
root/screensaver/mode	Legt den Wiedergabe-Modus für das Bild des Bildschirmschoners fest. Mit der Einstellung Center (Mitte) wird das Bild in die Mitte des Bildschirms gesetzt, mit Stretch (Strecken) wird das Bild dem Bildschirm angepasst, mit Tile (Kachel) wird das Bild im gekachelten Modus angezeigt und mit Default (Standard) wird das Bild ohne weitere Anpassungen angezeigt.
root/screensaver/off	Verzögerung des Zeitlimits zum Ausschalten des Monitors (in Minuten).
root/screensaver/standby	Verzögerung des Zeitlimits, um den Monitor in den Energiesparmodus zu bringen (in Minuten).
root/screensaver/suspend	Verzögerung des Zeitlimits, um den Monitor in den Bereitschaftsstatus zu bringen (in Minuten).
root/screensaver/timeoutScreensaver	Verzögerung des Zeitlimits bis zum Starten des Bildschirmschoners (in Minuten).
root/screensaver/timeoutSleep	Verzögerung des Zeitlimits bis der Thin Client in den Energiesparmodus versetzt wird (in Minuten).

root > security

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > security**.

Tabelle E-29 root > security

Registrierungsschlüssel	Beschreibung
root/security/mustLogin	Stellen Sie den Wert 1 ein, um eine Anmeldung aller Benutzer vor dem Zugriff auf den Desktop zu erzwingen.

root > sshd

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > sshd**.

Tabelle E-30 root > sshd

Registrierungsschlüssel	Beschreibung
root/sshd/enabled	Stellen Sie den Wert 1 ein, um den SSH-Daemon zu aktivieren, sodass der Benutzer über SSH auf den Thin Client zugreifen kann.
root/sshd/userAccess	Stellen Sie den Wert 1 ein, um nicht-Administratoren die Verbindung mit dem Thin Client über SSH zu ermöglichen.

root > time

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > time**.

Tabelle E-31 root > time

Registrierungsschlüssel	Beschreibung
root/time/NTPServers	Eine durch Komma getrennte Liste der zu verwendenden NTP-Server. Private NTP-Server oder große virtuelle NTP-Cluster wie "pool.ntp.org" 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.
root/time/TimeServerIPAddress	Dies ist der Zeitserver, der vom Linux-Netzbehl verwendet wird. Diese Server sind in der Regel die DC-Server im Unternehmensnetzwerk. Verwenden Sie diese, wenn die NTP-Server entweder nicht konfiguriert sind oder nicht reagieren. Der Linux-Netzbehl identifiziert diese Server selbstständig; es kann hier jedoch eine spezifische Server-IP-Adresse bereitgestellt werden, falls gewünscht.
root/time/WebServerURL	Gibt die Webserver-URL an. Dieser Server wird abgefragt bei der Verwendung des http-Protokolls zur Abfrage der Zeit. Diese URL kann sich innerhalb des Intranets oder im Internet befinden.
root/time/timezone	Zur manuellen Angabe der Zeitzone. Zeitzonen sollten im folgenden Format angegeben werden: '[region]/[subregion]'

Tabelle E-31 root > time (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	gemäß Definition 'Linux timezone:' im Datum- und Uhrzeit-Menüelement der Client-Systemsteuerung.
root/time/use24HourFormat	Wählen Sie gemäß des Gebietsschemas: 0 – Uhrzeitformat AM/PM 1 – 24-Stundenformat
root/time/useDHCPTimezone	Bei Einstellung des Werts auf 1 werden Clients versuchen, die Zeitzone über DHCP einzurichten. So richten Sie die Zeitzone mithilfe dieses Schlüssels korrekt ein: stellen sie sicher, dass der DHCP-Server für die Clients das DHCP-Tag "tcode" (normalerweise Tag 101, aber 100 und 2 funktionieren möglicherweise auch) weiterleitet.
root/time/useNTPServers	Richten Sie 1 ein, um die Verwendung von NTP-Zeitservern zum Synchronisieren der Client-Uhr aktivieren. Wenn dies aktiviert ist, vergewissern Sie sich, dass ein NTP-Server über DHCP angegeben ist oder der Schlüssel "NTP-Servers".

root > touchscreen

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > touchscreen**.

Tabelle E-32 root > touchscreen

Registrierungsschlüssel	Beschreibung
root/touchscreen/calibrated	Dieser Schlüssel ist zur Verwendung reserviert.
root/touchscreen/enabled	Stellen Sie den Wert 1 ein, um das Touchscreen-Modul im System zu aktivieren.
root/touchscreen/maxx	Dieser Schlüssel ist zur Verwendung reserviert.
root/touchscreen/maxy	Dieser Schlüssel ist zur Verwendung reserviert.
root/touchscreen/minx	Dieser Schlüssel ist zur Verwendung reserviert.
root/touchscreen/miny	Dieser Schlüssel ist zur Verwendung reserviert.
root/touchscreen/port	Der Geräteport zur Verbindung zum Touchscreen.
root/touchscreen/swapx	Dieser Schlüssel ist zur Verwendung reserviert.
root/touchscreen/swapy	Dieser Schlüssel ist zur Verwendung reserviert.
root/touchscreen/type	Der Controller-Typ für den Touchscreen.

root > translation

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > translation**.

Tabelle E-33 root > translation

Registrierungsschlüssel	Beschreibung
root/translation/coreSettings/localeMapping/{language}	Ein interner Schlüssel, der dazu verwendet wird, die Textzeichenfolge neben der entsprechenden Sprache in der Sprachauswahl zur Verfügung zu stellen. Dieser Schlüssel sollte keine Änderung erfordern.
root/translation/coreSettings/localeSettings	Ändert das Gebietsschema für den Client. Dieses Gebietsschema wird außerdem an die Remote-Verbindung weitergeleitet. Gültige Gebietsschemen: en_US (Englisch), de_DE (Deutsch), es_ES (Spanisch) und fr_FR (Französisch). Andere Gebietsschemen, wie z. B. ja_JP (Japanisch) und zh_CN (Chinesisch) können unter Umständen als Client-Aktualisierungen bereitgestellt werden.
root/translation/gui/LocaleManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/translation/gui/LocaleManager/status	Der aktive Status der Einstellungseditor für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/translation/gui/LocaleManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/translation/gui/LocaleManager/widgets/localeSettings	Zum Einstellen des Widget "Locale Setting" (Gebietsschema-Einstellung) in den USA. Dieses Feld sollte ausgeblendet werden und der Wert des Schlüssels sollte inactive sein. Dieser Schlüssel sollte keine Änderung erfordern.

root > usb-update

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > usb-update**.

Tabelle E-34 root > usb-update

Registrierungsschlüssel	Beschreibung
root/usb-update/authentication	Legt fest, ob für USB-Updates ein Administratorkennwort erforderlich ist oder nicht.
root/usb-update/enable	Aktiviert oder deaktiviert die USB-Auto-Update-Erkennung.
root/usb-update/height	Die Höhe der Benutzeroberfläche in Pixel.
root/usb-update/searchMaxDepth	Die Tiefe der Unterverzeichnisse zum Durchsuchen nach Updates. Einrichten einer hohen Suchtiefe führt möglicherweise zu Verzögerungen auf USB-Sticks, die Tausende von Verzeichnissen haben.
root/usb-update/width	Die Breite der Benutzeroberfläche in Pixel.

root > users

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > users**.

Tabelle E-35 root > users

Registrierungsschlüssel	Beschreibung
root/users/gui/hptc-user-rights/name	Der Name der GUI. Dieser Schlüssel sollte nicht verändert werden.
root/users/gui/hptc-user-rights/status	Der Status der GUI. Dieser Schlüssel sollte nicht verändert werden.
root/users/gui/hptc-user-rights/title	Der Titel der GUI. Dieser Schlüssel sollte nicht verändert werden.
root/users/root/password	Das Kennwort für den Administratormodus. Wenn leer, ist der Administratormodus gesperrt. Der Administratormodus bietet Zugriff auf alle Elemente der Systemsteuerung.
root/users/user/SSO	
root/users/user/WOL	Aktiviert die Wake-on-LAN-Funktion.
root/users/user/XHostCheck	Aktiviert die X-Host-Zugriffskontroll-sicherheit.
root/users/user/apps/hptc-ad-dns-mgr/authorized	Bei Einstellung des Werts auf 1 wird der AD/DDNS Manager für Benutzer aktiviert.
root/users/user/apps/hptc-agent-mgr/authorized	Bei Einstellung des Werts auf 1 wird der HPDM Manager für Benutzer aktiviert.
root/users/user/apps/hptc-auto-update/authorized	Bei Einstellung des Werts auf 0 können Benutzer nicht auf die Server-Einstellungen für das automatische Update zugreifen. Die Standardkonfiguration ist deaktiviert, da Clients ihre Automatische-Update-Server-URL per Broadcast oder DHCP-Kennung erhalten.
root/users/user/apps/hptc-background-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Hintergrund-Manager-Element für Benutzer deaktiviert.
root/users/user/apps/hptc-bluetooth-manager/authorized	Bei Einstellung des Werts auf 0 können Benutzer den Bluetooth Manager nicht mehr verwenden.
root/users/user/apps/hptc-cda/authorized	Bei Einstellung des Werts auf 1 wird das CDA-Modus-Manager-Element für Benutzer deaktiviert.
root/users/user/apps/hptc-cert-mgr/authorized	Bei Einstellung des Werts auf 0 können Benutzer nicht auf die Certificate Manager-Einstellungen zugreifen. Dies kann in einer nur-DHCP-Umgebung hilfreich sein, in der alle Einstellungen des Certificate Manager auf Clients vom DHCP-Server angegeben werden.
root/users/user/apps/hptc-clientaggregation-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Client Aggregation Manager-Element für Benutzer aktiviert.
root/users/user/apps/hptc-date-mgr/authorized	Bei Einstellung des Werts auf 0 sind Benutzer nicht in der Lage, auf die lokalen Datums- und Uhrzeiteinstellungen des Clients zuzugreifen. Dies kann hilfreich sein in einer Umgebung, in der das Datum und die Uhrzeit des Clients von NTP eingerichtet werden.
root/users/user/apps/hptc-dhcp-mgr/authorized	Bei Einstellung des Werts auf 1 wird das DHCP Manager-Element für Benutzer deaktiviert.
root/users/user/apps/hptc-display-prefs/authorized	Bei Einstellung des Werts auf 0 sind Benutzer nicht in der Lage Änderungen der Bildschirmauflösung, Bittiefe oder Bildwiederholungsrate vorzunehmen.
root/users/user/apps/hptc-easy-update/authorized	Bei Einstellung des Werts auf 1 wird das Easy Update Manager-Element für Benutzer aktiviert.

Tabelle E-35 root > users (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/users/user/apps/hptc-i18n-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Gebietschemen-Element in der Systemsteuerung für Benutzer aktiviert.
root/users/user/apps/hptc-keyboard-layout/authorized	Bei Einstellung des Werts auf 1 wird das vollständige Tastaturlayout-Element der Systemsteuerung für Benutzer aktiviert.
root/users/user/apps/hptc-mixer/authorized	Bei Einstellung des Werts auf 0 wird die Mixer-Systemsteuerung in voller Größe für Benutzer deaktiviert. Sie ist normalerweise überflüssig, da die Ministeuerung die gleichen Funktionen abdeckt.
root/users/user/apps/hptc-mouse/authorized	Bei Einstellung des Werts auf 0 sind Benutzer nicht in der Lage, die lokalen Client-Mauseinstellungen zu ändern. Benutzer können jedoch die Mauseinstellungen jederzeit über die Remote-Host-Einstellungen ändern.
root/users/user/apps/hptc-network-mgr/authorized	Bei Einstellung des Werts auf 0 sind Benutzer nicht in der Lage, auf Netzwerkeinstellungen zuzugreifen. Dies kann in einer Nur-DHCP-Umgebung hilfreich sein, in der alle Netzwerkeinstellungen vom DHCP-Server an die Clients übergeben werden.
root/users/user/apps/hptc-printer-mgr/authorized	Bei Einstellung des Werts auf 0 sind Benutzer nicht in der Lage, die Windows Treiber-Werte für lokal angeschlossene Drucker einzurichten. Dies könnte dazu führen, dass manche Drucker nicht korrekt zu Remote-Sitzungen zuordnen können. Diese Einstellung hat keine Auswirkungen auf die USB-Umleitung.
root/users/user/apps/hptc-restore/authorized	Bei Einstellung des Werts auf 1 können Benutzer Wiederherstellungspunkte verwalten.
root/users/user/apps/hptc-screenlock-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Screensaver Manager-Element für Benutzer aktiviert.
root/users/user/apps/hptc-security/authorized	Bei Einstellung des Werts auf 1 wird das Element Sicherheit für Benutzer aktiviert.
root/users/user/apps/hptc-shortcut-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element Verknüpfungsmanager für Benutzer aktiviert.
root/users/user/apps/hptc-sshd-mgr/authorized	Bei Einstellung des Werts auf 1 wird der Secure Shell Daemon Manager für Benutzer aktiviert.
root/users/user/apps/hptc-task-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element Task-Manager für Benutzer aktiviert.
root/users/user/apps/hptc-text-editor/authorized	Bei Einstellung des Werts auf 1 wird das Element Texteditor für Benutzer aktiviert.
root/users/user/apps/hptc-thinstate/authorized	Bei Einstellung des Werts auf 1 wird das ThinState Manager-Element für Benutzer aktiviert.
root/users/user/apps/hptc-touchscreen/authorized	Bei Einstellung des Werts auf 1 wird das Touchscreen Manager-Element für Benutzer aktiviert.
root/users/user/apps/hptc-usb-mgr/authorized	Bei Einstellung des Werts auf 1 wird das USB-Manager-Element für Benutzer aktiviert.
root/users/user/apps/hptc-user-rights/authorized	Bei Einstellung des Werts auf 1 wird das ThinPro Configuration Manager-Element für Benutzer aktiviert.

Tabelle E-35 root > users (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/users/user/apps/hptc-vncshadow/authorized	Bei Einstellung des Werts auf 1 wird das VNC Shadowing-Element in der Systemsteuerung für Benutzer aktiviert.
root/users/user/apps/hptc-xterm/authorized	Bei Einstellung des Werts auf 0 wird ein Stammverzeichnis-X-Terminal-Element in der Systemsteuerung für Benutzer aktiviert. VORSICHT! Das Aktivieren des Zugriffs auf ein Stammverzeichnis-Terminal stellt ein Sicherheitsrisiko dar und wird in einer Produktionsumgebung nicht empfohlen. Das Stammverzeichnis-Terminal sollte nur zur Verwendung in einer fehlerfreien geschützten, nicht produktiven Umgebung aktiviert werden.
root/users/user/apps/scim-setup/authorized	Bei Einstellung des Werts auf 1 wird das SCIM-Element in der Systemsteuerung für Benutzer aktiviert. HINWEIS: SCIM wird zur Eingabe asiatischer Sprachen verwendet und ist unter Umständen ohne die Installation eines Kits für asiatische Sprachen nicht auf dem System vorhanden.
root/users/user/hideDesktopPanel	Bei Einstellung des Werts auf 1 werden Desktop-Bedienfelder, wie z. B. Fbpanel oder Taskleiste, nicht gestartet oder auf dem Desktop angezeigt. Bei Einstellung des Werts auf 1 im Kioskmodus, wird die Ein/Aus-Schaltfläche in der Benutzeroberfläche angezeigt.
root/users/user/kioskMode	
root/users/user/launchConnectionManager	Aktiviert das Starten des HP Connection Manager beim Systemstart.
root/users/user/rightclick	Aktiviert das Rechtsklick-Kontextmenü für den Desktop.
root/users/user/ssconnectiontype	
root/users/user/switchAdmin	Ermöglicht dem Benutzer in den Administratormodus zu wechseln.
root/users/user/xhosts/{UUID}/xhost	Die XHost-Adresse/Name in der XHost-Zugriffskontrollliste.

root > vncserver

Dieser Abschnitt beschreibt die Registrierungsschlüssel, Funktionen, Optionen und Beschreibungen im Ordner **root > vncserver**.

Tabelle E-36 root > vncserver

Registrierungsschlüssel	Beschreibung
root/vncserver/coreSettings/enableVncShadow	Stellen Sie den Wert 1 ein, um den VNC-Shadow-Server für den Thin Client zu aktivieren.
root/vncserver/coreSettings/userNotificationMessage	Die Benachrichtigungsmeldung, die dem Benutzer angezeigt wird.
root/vncserver/coreSettings/vncNotifyShowTimeout	Stellen Sie den Wert 1 ein, um ein Zeitlimit für die Benachrichtigungsmeldung festzulegen.

Tabelle E-36 root > vncserver (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/vncserver/coreSettings/vncNotifyTimeout	Die Benachrichtigungsmeldung, die angezeigt wird, wenn "vncNotifyShowTimeout" aktiviert ist. Nach der Zeitüberschreitung wird die Nachricht ausgeblendet.
root/vncserver/coreSettings/vncNotifyUser	Stellen Sie den Wert 1 ein, um eine entsprechende Benachrichtigungsmeldung zu aktivieren, wenn ein VNC-Client versucht, eine Verbindung zum Thin Client herzustellen.
root/vncserver/coreSettings/vncPassword	Das Kennwort für VNC, wenn "VncUsePassword" aktiviert ist.
root/vncserver/coreSettings/vncReadOnly	Stellen Sie den Wert 1 ein, um VNC auf den schreibgeschützten Modus zu beschränken. Die VNC-Clients sind auf Nur-Ansicht eingeschränkt.
root/vncserver/coreSettings/vncRefuseInDefault	Stellen Sie den Wert 1 ein, um die Verbindung abzulehnen, wenn der Benutzer die Benachrichtigungsmeldung nicht akzeptiert oder verweigert. Stellen Sie den Wert 0 ein, um die Verbindung zu akzeptieren, wenn der Benutzer die Benachrichtigungsmeldung nicht akzeptiert oder verweigert.
root/vncserver/coreSettings/vncTakeEffectRightNow	Stellen Sie den Wert 1 ein, um eine sofortige Wirksamkeit der VNC-Einstellung zu bewirken.
root/vncserver/coreSettings/vncUsePassword	Stellen Sie den Wert 1 ein, um zu bewirken, dass VNC ein Kennwort für die Authentifizierung des Clients-Zugriffs verwendet.
root/vncserver/coreSettings/vncUseSSL	Regelt die Verwendung von SSL für die VNC-Verbindung. Die Standardeinstellung ist 0 .
root/vncserver/gui/VNCShadowManager/name	Der Name des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/vncserver/gui/VNCShadowManager/status	Der aktive Status der Einstellungseditor für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/vncserver/gui/VNCShadowManager/title	Der Fenstertitel des Einstellungseditors für diese Anwendung. Dieser Schlüssel sollte keine Änderung erfordern.
root/vncserver/gui/VNCShadowManager/widgets/enableVncShadow	Zum Einstellen des Status für das Widget Enable VNC (Systemstart von VNC aktivieren) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/userNotificationMessage	Zum Einstellen des Status für das Widget User Notification Message (Benutzerbenachrichtigung) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout	Zum Einstellen des Status für das Widget VNC Show Timeout for Notification (VNC Zeitlimit für Benachrichtigung anzeigen) in der VNC Shadowing-Utility. Durch die

Tabelle E-36 root > vncserver (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout	Zum Einstellen des Status für das numerische Widget, das den Wert für das Zeitlimit der Benachrichtigung in der VNC Shadowing-Utility angibt. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser	Zum Einstellen des Status für das Widget VNC Notify User to Allow Refuse (VNC Benutzer benachrichtigen, um Ablehnung zuzulassen) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncPassword	Zum Einstellen des Status für das Widget Set Password (Kennwort einrichten) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly	Zum Einstellen des Status für das Widget VNC Read Only (VNC Schreibgeschützt) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault	Zum Einstellen des Status für das Widget Refuse connections in default (Verbindungen standardmäßig verweigern) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow	Zum Einstellen des Status für das Widget Re-set VNC server right now (VNC-Server jetzt gleich zurücksetzen) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.
root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword	Zum Einstellen des Status für das Widget VNC Use Password (VNC Kennwort verwenden) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der

Tabelle E-36 root > vncserver (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL	Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt. Zum Einstellen des Status für das Widget VNC Use SSL (VNC SSL verwenden) in der VNC Shadowing-Utility. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung inactive wird das Widget ausgeblendet. Durch die Einstellung read-only wird das Widget im schreibgeschützten Modus angezeigt.

Index

- A**
 - AD/DDNS Manager 10
 - Add-Ons 1
 - Aktualisieren von Clients
 - Aktualisierung mit DHCP-Kennung 63
 - Aktualisierung per Übertragung 63
 - Anzeigeeinstellungen 14
 - Anzeigeprofile 14
 - Audioeinstellungen 9
 - Audioumleitung
 - RDP 43
 - VMware Horizon View 49
- B**
 - Background Manager 9
 - Benutzeroberfläche
 - Navigieren 5
 - Bildschirmschoner-Einstellungen 9
- C**
 - Certificate Manager 25
 - Citrix
 - Einstellungen, allgemeine 31
 - Einstellungen, verbindungsspezifisch 35
 - HDX MediaStream 30
 - Supportmatrix 31
 - Clientaggregation 12
 - Clientkonfiguration 13
 - Serverkonfiguration 14
 - Client-Anmeldebildschirm
 - Anpassen 78
 - Client-Profil
 - bearbeiten 65
 - Dateien hinzufügen 67
 - laden 65
 - Registrierungseinstellungen 66
 - speichern 68
 - Symbolischen Link hinzufügen 68
 - Zertifikate 67
- Clients
 - aktualisieren. *Siehe* Aktualisieren von Clients
 - Clients aktualisieren
 - DNS Alias Update 64
 - manuelle Aktualisierung 64
 - Connection Manager-Bedienelemente 6
 - Custom-Verbindungen 60
- D**
 - Datums- und Uhrzeiteinstellungen 9
 - DHCP-Optionen 25
 - Drucker 15
 - Druckerkonfiguration 68
 - Druckerumleitung
 - RDP 43
 - VMware Horizon View 49
- E**
 - Easy Update 10
 - Einführung 4
- F**
 - Fehlerbeseitigung 71
 - Firmware-Beschädigung 72
 - Netzwerkverbindung 71
 - verwenden der Systemdiagnose 72
- G**
 - Geräteumleitung
 - RDP 41
 - VMware Horizon View 48
- H**
 - HDX MediaStream 30
 - HP Device Manager. *Siehe* HPDM Agent
 - HPDM Agent 10
 - HP Smart Client Services
 - Installation 61
 - Profile Editor. *Siehe* Profile Editor
- Übersicht 61
 - unterstützte Betriebssysteme 61
- HP TeamTalk. *Siehe* TeamTalk
- HP Velocity 19
- I**
 - Image-Aktualisierungen 1
 - Imageerstellung und -verwendung. *Siehe* HP ThinState
- K**
 - Kennwörter, ändern 10
 - Kioskmodus 28
 - Konfiguration eines parallelen Druckers 68
 - Konfiguration eines seriellen Druckers 68
- M**
 - Massenspeicherumleitung
 - RDP 42
 - VMware Horizon View 49
 - Mauseinstellungen 9
 - MMR
 - VMware Horizon View 48
 - Momentaufnahmen 10
 - Multimedia-Umleitung
 - RDP 41
- N**
 - Netzwerkeinstellungen
 - DNS 18
 - drahtgebunden 16
 - HP Velocity 19
 - IPSec 18
 - VPN 19
 - Wireless 17
 - Zugreifen 16
- P**
 - Profile Editor
 - verwenden 65

R

RDP

- Audioumleitung 43
- Druckerumleitung 43
- Einstellungen, allgemeine 36
- Einstellungen,
verbindungsspezifisch 37
- Geräteumleitung 41
- Massenspeicherumleitung 42
- Multimedia-Umleitung 41
- Multi-Monitor-Sitzungen 40
- RemoteFX 40
- Smart Card-Umleitung 44
- USB-Umleitung 41

Registrierungsschlüssel 87

RemoteFX 40

RFX. *Siehe* RemoteFX

S

SCEP Manager 11, 25

SCIM 9

Serial Manager 11

Sicherheitseinstellungen 10

Smart Card-Umleitung

RDP 44

VMware Horizon View 50

So finden Sie weitere

Informationsquellen 1

Spracheinstellungen 9

SSH 58

SSHD Manager 10

Systemdiagnose 72

System information

(Systeminformationen)

Anzeigen 7

Systeminformations-

Bildschirmanzeigen

Ausblenden 7

Systemsteuerung

AD/DDNS Manager 10

Anpassungcenter 10

Bildschirmschoner 9

Client Aggregation

(Clientaggregation) 12

Datum und Uhrzeit 9

DHCP Options Manager 25

Dienstprogramme,

ausblenden 10

Display Preferences

(Anzeigeinstellungen) 14

Easy Update 10

Hintergrundeinstellungen 9

Language (Sprache) 9

Maus 9

Momentaufnahmen 10

Netzwerk 16

SCEP Manager 11

SCIM Input Method Setup

(Einstellung der

Eingabemethode) 9

Security (Sicherheit) 10

Serial Manager 11

Sound 9

SSHD Manager 10

Task Manager 11

Tastenkombinationen 11

Text Editor 11

ThinState. *Siehe* HP ThinState

Touchscreen 9

Übersicht 8

VNC Shadow 24

X Terminal 11

T

Taskleiste

Verwenden 5

Task Manager 11

Tastenkombinationen 11

TeamTalk 55

Telnet 59

Text Editor 11

ThinState. *Siehe* HP ThinState

Touchscreen-Einstellungen 9

U

USB-Umleitung

RDP 41

USB-Manager 15

VMware Horizon View 48

V

Verbindungen

Ausblenden 10

Gemeinsame Einstellungen

27

Typen 1

VMware Horizon View

Audioumleitung 49

Druckerumleitung 49

Einstellungen 45

Geräteumleitung 48

Massenspeicherumleitung 49

MMR 48

Multi-Monitor-Sitzungen 48

Protokolle ändern 51

Sicherheitsstufen von

Zertifikaten 51

Smart Card-Umleitung 50

Tastaturbefehle 48

USB-Umleitung 48

Webcamumleitung 50

Zertifikate 51

VNC-Shadowing 24

W

Web Browser

Einstellungen, allgemeine 54

Einstellungen,

verbindungsspezifisch 54

Webcamumleitung

VMware Horizon View 50

Webseiten

Citrix-Support 1

HP-Support 1

Microsoft-Support 1

VMware-Support 1

X

XDMCP 57

X Terminal 11

Z

Zertifikate

Installation 25

VMware Horizon View 51