HP ThinPro 5.2

Administratorhandbuch

© Copyright 2015 Hewlett-Packard Development Company, L.P.

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

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 zur Verfügung gestellt.

HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument. Ferner übernimmt HP 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.

Erste Ausgabe: Mai 2015

Teilenummer des Dokuments: 824313-041

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 unter ftp: ftp://ftp.hp.com/pub/tcdebian/pool/thinpro52/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 `<pathname>` durch den entsprechenden Pfad, wie z. B. `C:\Windows\System`. Geben Sie bei der Eingabe des eigentlichen Wertes die Klammern nicht mit ein.
`[optional parameters]`	Optionale Parameter sind in eckige Klammern eingeschlossen. Geben Sie bei der Angabe der Parameter die Klammern nicht mit ein.
`"literal value"`	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 2

Dokumentorganisation 2

2 Einführung 4

Auswählen eines Management Service 4

Erstmaliges Einrichten von HP ThinPro 4

3 Navigieren auf der Benutzeroberfläche 6

Verwenden der Taskleiste 6

Verwenden der Connection Manager-Bedienelemente 7

Anzeigen der Systeminformationen 8

Ausblenden der Systeminformations-Bildschirmanzeigen 8

4 Konfigurationen der Systemsteuerung 9

Übersicht Systemsteuerung 9

Clientaggregation 13

Konfigurieren der Clientaggregation 14

Konfigurieren der Aggregation-Clients 14

Konfigurieren des Aggregation-Servers 15

Anzeigeeinstellungen 15

Konfigurieren von Druckern 16

USB-Geräte umleiten 16

Netzwerkeinstellungen 17

Drahtgebundene Netzwerkeinstellungen 17

Wireless-Netzwerkeinstellungen 18

DNS-Einstellungen 19

IPSec-Regeln 19

Konfigurieren von VPN-Einstellungen 20

Konfigurieren von HP Velocity 20

Component Manager (Komponenten-Manager) 20

Entfernen von Komponenten 21

Rückgängigmachen einer Änderung 21

Dauerhaftes Anwenden der Änderungen 21

Anpassungscenter 21

HP ThinState ... 22
Verwalten von HP ThinPro-Images ... 22
Aufzeichnung von HP ThinPro-Images auf einem FTP-Server ... 22
Bereitstellung eines HP ThinPro-Images über FTP oder HTTP ... 23
Aufzeichnen eines HP ThinPro-Images auf einem USB-Flash-Laufwerk ... 23
Bereitstellung eines HP ThinPro-Images mit einem USB-Flash-Laufwerk ... 24
Verwalten eines ThinPro-Profils ... 24
Speichern eines ThinPro-Profils auf einem FTP-Server ... 24
Wiederherstellen eines ThinPro-Profils über FTP oder HTTP ... 25
Speichern eines ThinPro-Profils auf einem USB-Flash-Laufwerk ... 25
Wiederherstellen eines ThinPro-Profils von einem USB-Flash-Laufwerk ... 25
VNC-Shadowing ... 26
Zertifikate ... 26
Certificate Manager ... 26
SCEP Manager ... 27
DHCP-Optionen ... 27

5 Gemeinsame Verbindungskonfigurationen ... 29
Gemeinsame Verbindungseinstellungen ... 29
Kioskmodus ... 30

6 Citrix-Verbindungen ... 32
Citrix Receiver-Funktionen ... 32
HDX MediaStream ... 33
HP True Graphics ... 34
Serverseitige Anforderungen für HP True Graphics ... 34
XenApp/XenDesktop ... 34
HDX 3D Pro ... 34
Überprüfen der Serveroptionen für die Komprimierung ... 34
Clientseitige Konfiguration von HP True Graphics ... 35
Komprimierungseinstellungen ... 35
Fenstereinstellungen ... 35
Monitorlayout- und Hardwarebeschränkungen ... 35
Citrix-Verbindung-Supportmatrix ... 35
Citrix – Allgemeine Einstellungen ... 36
Citrix – Verbindungsspezifische Einstellungen ... 39

7 RDP-Verbindungen ... 41
RPD-Funktionen ... 41
RDP – Allgemeine Einstellungen ... 41

RDP – Verbindungsspezifische Einstellungen 42
Verwenden von RemoteFX mit RDP 46
Verwenden von Multi-Monitor-Sitzungen mit RDP 47
Verwenden der Multimedia-Umleitung mit RDP 47
Verwenden der Geräteumleitung mit RDP 47
Verwenden einer USB-Umleitung mit RDP 48
Verwenden der Massenspeicherumleitung mit RDP 48
Verwenden der Druckerumleitung mit RDP 49
Audioumleitung mit RDP verwenden 49
Smart Card-Umleitung mit RDP verwenden 50

8 VMware Horizon View-Verbindungen 51
VMware Horizon View-Einstellungen 51
Verwenden von Multi-Monitor Sitzungen mit VMware Horizon View 54
Verwenden von Tastaturkürzeln mit VMware Horizon View 55
Verwenden der Multimedia-Umleitung mit VMware Horizon View 55
Geräte-Umleitung mit VMware Horizon View verwenden 55
USB-Umleitung mit VMware Horizon View verwenden 55
Massenspeicher-Umleitung mit VMware Horizon View verwenden 55
Drucker-Umleitung mit VMware Horizon View verwenden 56
Audioumleitung mit VMware Horizon View verwenden 56
Smart Card-Umleitung mit VMware Horizon View verwenden 57
Webcam-Umleitung mit VMware Horizon View verwenden 57
Ändern des VMware Horizon View Protokolltyps 58
Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung 58

9 Web Browser-Verbindungen 60
Web Browser – Allgemeine Einstellungen 60
Web Browser – Verbindungsspezifische Einstellungen 60

10 Zusätzliche Verbindungstypen (gilt nur für ThinPro-Konfiguration) 62
TeemTalk Verbindungseinstellungen 62
XDMCP Verbindungseinstellungen 64
SSH Verbindungseinstellungen 65
Telnet Verbindungseinstellungen 66
Benutzerdefinierte Verbindungseinstellungen 67

11 HP Smart Client Services 68
Unterstützte Betriebssysteme 68
Voraussetzungen für HP Smart Client Services 68

Abrufen von HP Smart Client Services 69
Anzeigen der Automatic Update-Website 69
Ein Automatic Update-Profil erstellen 69
Aktualisieren von Thin Clients 69
Verwenden der Methode zur Aktualisierung per Übertragung 70
Verwenden der Methode zur Aktualisierung per DHCP-Kennung 70
Beispiel für die Durchführung DHCP-Kennung 70
Verwenden der Methode zur Aktualisierung per DNS-Alias 71
Verwenden der Methode zur manuellen Aktualisierung 71
Eine manuelle Aktualisierung durchführen 71

12 Verwenden des Profile Editors 72
Zugriff auf den Profile Editor 72
Laden eines ThinPro-Profils 72
Ändern eines ThinPro-Profils 72
Auswählen der Plattform für ein ThinPro-Profil 73
Konfigurieren einer Standardverbindung für ein ThinPro-Profil 73
Ändern von Registrierungseinstellungen eines ThinPro-Profils 73
Hinzufügen von Dateien zu einem ThinPro-Profil 74
Hinzufügen einer Konfigurationsdatei zu einem ThinPro-Profil 74
Hinzufügen von Zertifikaten zu einem ThinPro-Profil 74
Hinzufügen eines symbolischen Links zu einem ThinPro-Profil 75
Speichern des ThinPro-Profils 75
Konfigurieren eines seriellen oder parallelen Druckers 75
Abrufen der Druckereinstellungen 75
Einrichten von Druckeranschlüssen 76
Drucker auf dem Server installieren 76

13 Fehlerbeseitigung 78
Fehlerbeseitung bei der Netzwerkverbindung 78
Fehlerbeseitigung bei Firmware-Beschädigung 79
Installieren eines neuen Images der Thin Client-Firmware 79
Fehlerbeseitigung bei abgelaufenen Citrix-Kennwörtern 79
Verwenden der Systemdiagnose für die Fehlerbeseitigung 79
Speichern von Systemdiagnosedaten 80
Dekomprimieren der Systemdiagnosedateien 80
Dekomprimieren der Systemdiagnosedateien auf Windows-basierten Systemen 80
Dekomprimieren der Systemdiagnosedateien auf Linux- oder Unix-basierten Systemen 80
Anzeigen der Systemdiagnosedateien 80
Anzeigen von Dateien im Ordner Befehle 80

Anzeigen von Dateien im Ordner /var/log 81
Anzeigen von Dateien im Ordner /etc 81

Anhang A USB Updates 82

Anhang B BIOS-Tools 83
BIOS-Tool für Einstellungen 83
BIOS Flashing-Tool 83

Anhang C Ändern der Größe der Flash-Laufwerk-Partition 84

Anhang D Benutzerdefiniertes Anpassen des Smart Zero-Anmeldebildschirms 85
Anpassen des Bildschirmhintergrunds 85
Gemeinsame Attribute 85
Elemente 88
Image 90
Text 91

Anhang E Registrierungsschlüssel 94
root > Audio 95
root > CertMgr 96
root > ComponentMgr 96
root > ConnectionManager 96
root > ConnectionType 97
root > ConnectionType > custom 97
root > ConnectionType > firefox 100
root > ConnectionType > freerdp 105
root > ConnectionType > ssh 114
root > ConnectionType > teemtalk 120
root > ConnectionType > telnet 123
root > ConnectionType > view 127
root > ConnectionType > xdmcp 136
root > ConnectionType > xen 140
root > CpuMgr 154
root > DHCP 154
root > Dashboard 154
root > Display 155
root > Network 157
root > SCIM 163
root > ScepMgr 163

root > Search 164
root > Serial 165
root > SystemInfo 166
root > TaskMgr 166
root > USB 166
root > auto-update 167
root > background 169
root > config-wizard 170
root > desktop 170
root > entries 171
root > keyboard 171
root > logging 172
root > mouse 172
root > restore-points 173
root > screensaver 173
root > security 174
root > sshd 174
root > time 174
root > touchscreen 175
root > translation 177
root > usb-update 177
root > users 178
root > vncserver 180

Index 183

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 Standard-Verbindungstypen **HINWEIS:** Sie können ändern, welche Verbindungstypen verfügbar sind, indem Sie den Registrierungsschlüssel `PriorityInConnectionLists` für jeden Verbindungstyp verwenden. Weitere Informationen finden Sie unter root > ConnectionType auf Seite 97.	• Citrix • RDP • VMware Horizon View • Web Browser (Firefox) • TeemTalk • XDMCP • SSH • Telnet • Custom	• Citrix • RDP • VMware Horizon View • Web Browser (Firefox)
Anzahl der Verbindungen, die gleichzeitig unterstützt werden	Mehrere	Eine
Standardmäßig für den Kioskmodus konfiguriert	Nein	Ja

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 6 – Bietet eine Übersicht der verschiedenen Komponenten der Benutzeroberfläche.
- „Konfigurationen der Systemsteuerung“ auf Seite 9 – Beschreibt die verbindungsabhängigen Einstellungen und Konfigurationen in der Systemsteuerung und Details zu einigen der erweiterten Konfigurationen.
- „Gemeinsame Verbindungskonfigurationen“ auf Seite 29 – Beschreibt die Einstellungen, die für alle Verbindungstypen gleich sind, und die Konfiguration eines Thin Client für den Kioskmodus.
- „Citrix-Verbindungen“ auf Seite 32 – Beschreibt die Einstellungen und Konfigurationen für den Verbindungstyp Citrix.
- „RDP-Verbindungen“ auf Seite 41 – Beschreibt die Einstellungen und Konfigurationen für den Verbindungstyp RDP.
- „VMware Horizon View-Verbindungen“ auf Seite 51 – Beschreibt die Einstellungen und Konfigurationen für den Verbindungstyp VMware Horizon View.
- „Web Browser-Verbindungen“ auf Seite 60 – Beschreibt die Einstellungen für den Verbindungstyp Web Browser.
- „Zusätzliche Verbindungstypen (gilt nur für ThinPro-Konfiguration)“ auf Seite 62 – Beschreibt die Einstellungen für die Verbindungstypen TeemTalk, XDMCP, SSH, Telnet und Benutzerdefiniert.

- „HP Smart Client Services“ auf Seite 68 – 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 72 – Beschreibt die Verwendung von Profile Editor zum Einrichten und Bearbeiten von ThinPro-Profilen, die Verbindungsinformationen, Einstellungen und Dateien enthalten, die beim Selbstkonfigurationsvorgang verwendet werden.
- „Fehlerbeseitigung“ auf Seite 78 – Beschreibt häufige Probleme und Lösungen bei der Fehlerbehebung.
- „USB Updates“ auf Seite 82 – Beschreibt die Installation von Add-ons und Profil-Updates von einem USB-Flash-Laufwerk.
- „BIOS-Tools“ auf Seite 83 – Beschreibt die Anzeige und Aktualisierung von BIOS-Einstellungen und das Flashen einer neuen BIOS-Version.
- „Ändern der Größe der Flash-Laufwerk-Partition“ auf Seite 84 – Beschreibt, wie man die Größe der Partition Flash-Laufwerk erhöhen kann.
- „Benutzerdefiniertes Anpassen des Smart Zero-Anmeldebildschirms“ auf Seite 85 – Beschreibt die gängigen Attribute und Elemente, die zur Anpassung des Smart Zero-Anmeldebildschirms verwendet werden.
- „Registrierungsschlüssel“ auf Seite 94 – Liste der Pfade, Funktionen und Optionen für die HP ThinPro-Registrierungsschlüssel.

2 Einführung

Auswählen eines Management Service

Thin Clients mit HP ThinPro können entweder vom HP Smart Client-Dienste oder HP Device Manager (HPDM) verwaltet werden. Sie können auch einen andere festgelegten Management Service wählen, je nach dem, was am besten für Ihre Bereitstellung geeignet ist.

HP Smart Client-Dienste sind für die Verwendung mit Smart Zero optimiert. Diese Option ermöglicht die NULL-Verwaltung.

HPDM ist ideal für große Umgebungen, die Thin Clients mit einer Vielzahl von unterschiedlichen Betriebssystemen enthalten. Diese Option bietet bessere Sichtbarkeit auf Thin Clients und eine größere Vielzahl von Optionen für die Verwaltung.

Erstmaliges Einrichten von HP ThinPro

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 17 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 68. 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** (Softwareupdate), 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** (Einfaches 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 Ihre Thin Client-Konfiguration bei der Aktualisierung Ihrer Image-Version beibehalten möchten, aktivieren Sie die Option **Preserve thin client configuration** (Thin Client-Konfiguration beibehalten).

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 22), verwenden Sie die Systemsteuerung, um alle gewünschten Konfigurationen vorzunehmen. Weitere Informationen finden Sie unter „Navigieren auf der Benutzeroberfläche“ auf Seite 6 und „Konfigurationen der Systemsteuerung“ auf Seite 9.

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

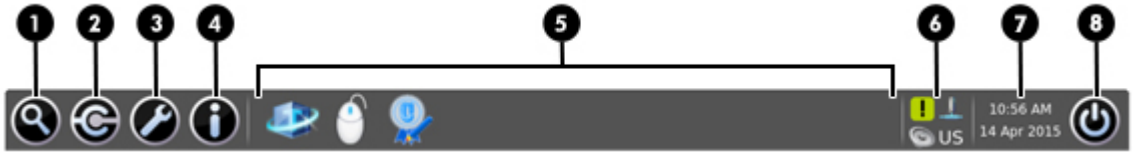


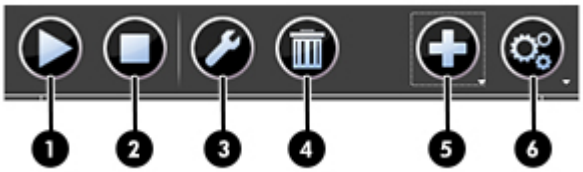
Tabelle 3-1 Komponenten der Taskleiste

1	**Suchen** – Zum Suchen und Ausführen von konfigurierten Verbindungen, Verbindungs-Managern, Dienstprogrammen der Systemsteuerung und Energiesparfunktionen.
2	**Verbindungs-Manager** – Zum Starten, Stoppen, Hinzufügen, Bearbeiten und Löschen von Verbindungen. Weitere Informationen finden Sie unter Verwenden der Connection Manager-Bedienelemente auf Seite 7.
3	**Systemsteuerung** – Zum Konfigurieren des Thin Client, Wechseln zwischen Administratormodus und Benutzermodus und Suchen nach Softwareupdates. Weitere Informationen finden Sie unter Übersicht Systemsteuerung auf Seite 9.
4	**Systeminformationen** – Zum Anzeigen von System-, Netzwerk- und Softwareinformationen zum Thin Client. Weitere Informationen finden Sie unter Anzeigen der Systeminformationen auf Seite 8.
5	**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.
6	**Taskleiste**– bietet schnellen Zugriff auf oder Informationen über bestimmte Dienstprogramme, Anwendungen und Funktionen. Elemente in der Taskleiste können unter anderem folgende sein; einige Elemente werden jedoch möglicherweise abhängig von der Systemkonfiguration nicht angezeigt: • Audiomixer • Virtuelle Tastatur • Netzwerkstatus • Automatischer Update-Status – ein grünes Symbol mit einem Häkchen zeigt an, dass die automatische Aktualisierung erfolgreich abgeschlossen. Ein gelbes Symbol mit einem Ausrufezeichen weist darauf hin, dass der automatische Update-Server nicht gefunden wurde oder dass einige Probleme mit den serverseitigen Einstellungen bestehen. Ein rotes Symbol mit einem X weist darauf hin, dass der automatische Update (Automatic Update) fehlgeschlagen ist, wie beispielsweise bei einem ungültigem Paket oder Profil. Ein blaues Symbol mit einem rotierenden Pfeil zeigt an, dass Automatic Update derzeit nach Updates sucht. • Zum Einstellen der Smart Common Input Method (SCIM) • Citrix-Anwendungen

Tabelle 3-1 Komponenten der Taskleiste (Fortsetzung)

7	**Datum und Uhrzeit** – Zeigt das aktuelle Datum und die Uhrzeit an. Klicken Sie hier, um auf die Datum- und Uhrzeiteinstellungen zuzugreifen.
8	**Ein/Aus-Taste** – Zum Abmelden, Neustarten oder Herunterfahren des Thin Client.

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 Verbindungsmanager) 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 2 für eine Liste der verfügbaren Verbindungstypen.
6	**Einstellungen** – Zum Bearbeiten der allgemeinen Einstellungen für Citrix-, RDP- oder Web Browser-Verbindungen. Diese Einstellungen sind für alle Verbindungen dieses Typs wirksam.

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

- „Gemeinsame Verbindungskonfigurationen“ auf Seite 29
- „Citrix-Verbindungen“ auf Seite 32
- „RDP-Verbindungen“ auf Seite 41
- „VMware Horizon View-Verbindungen“ auf Seite 51
- „Web Browser-Verbindungen“ auf Seite 60
- „Zusätzliche Verbindungstypen (gilt nur für ThinPro-Konfiguration)“ auf Seite 62

Anzeigen der Systeminformationen

Klicken Sie in der Taskleiste auf die Schaltfläche **Systeminformationen**, um System-, Netzwerk- und Softwareinformationen zum Thin 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 Problembehebung: • **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 eine Liste der installierten Add-ons auf der Registerkarte **Service Packs** (Service-Pakete) an, sowie Informationen zur Software-Version auf der Registerkarte **Software Installed** (Installierte Software). **TIPP:** Sie können auch das Administrator-Handbuch (dieses Dokument) über diesen Bildschirm aufrufen.
System Logs (Systemprotokolle)	Zeigt folgende Protokolle an: • Network Manager • Smart Client Services • DHCP Wired Leases • DHCP Wireless Leases • Kernel • X Server • Connection Manager Die Debugstufe kann geändert werden, um weitere Informationen anzuzeigen, die möglicherweise vom HP Support bei der Problembehebung angefragt werden. Klicken Sie auf **Diagnostic** (Diagnose), um eine Diagnosedatei zu speichern. Weitere Informationen finden Sie unter Verwenden der Systemdiagnose für die Fehlerbeseitigung auf Seite 79.

Ausblenden der Systeminformations-Bildschirmanzeigen

Siehe root > SystemInfo auf Seite 166 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
- Component Manager (Komponenten-Manager)
- Anpassungscenter
- HP ThinState
- VNC-Shadowing
- Zertifikate
- DHCP-Optionen

Übersicht Systemsteuerung

Die Systemsteuerung bietet Zugriff auf Dienstprogramme für die Konfiguration des Thin Client. 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 Kombinieren von Thin Clients, um einen zusätzlichen Anzeigebereich zu erstellen. Weitere Informationen finden Sie unter Clientaggregation auf Seite 13.
Display Preferences (Anzeigeeinstellungen)	Ermöglicht das Konfigurieren und Testen von Optionen für eine primäre und sekundäre Anzeige. Weitere Informationen finden Sie unter Anzeigeeinstellungen auf Seite 15.
Keyboard Layout (Tastaturlayout)	Damit können Sie das Tastaturlayout ändern, um es der Sprache der Tastatur anzupassen.
Sound (Audio)	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 16.
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 16.
SCIM Input Method Setup (Einstellung der Eingabemethode)	Zum Konfigurieren der Smart Common Input Method (SCIM) für die Eingabe von Chinesisch, Japanisch und Koreanisch. Weitere Informationen zu diesem Open-Source-Programm finden Sie unter 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)	Zum Anzeigen der HP ThinPro-Oberfläche in einer anderen Sprache.
Network (Netzwerk)	Zum Konfigurieren der Netzwerkeinstellungen. Weitere Informationen finden Sie unter Netzwerkeinstellungen auf Seite 17.
Screensaver (Bildschirmschoner)	Zum Konfigurieren eines Bildschirmschoners.
Security (Sicherheit)	Zum Festlegen und Ändern von Systemkennwörtern für den Thin Client-Administrator und -Benutzer.
Customization Center (Anpassungscenter)	Es stehen folgende Aktionen zur Verfügung:

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

Menüoption	Beschreibung
	• 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 Weitere Informationen finden Sie unter Anpassungscenter auf Seite 21.

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

Menüoption	Beschreibung
AD/DDNS Manager	Zum Hinzufügen des Thin Client zu einer Organisationseinheit des Active Directory-Servers und zur Aktivierung automatischer Dynamic DNS-Updates der Zuordnung von Namen und IP-Adresse des Thin Client. **HINWEIS:** Dieses Dienstprogramm aktiviert nicht die Authentifizierung gegenüber der Active Directory-Datenbank.
HPDM Agent	Zum Konfigurieren des HP Device Manager (HPDM) Agent. Weitere Informationen zu HP Device Manager finden Sie im *HP Device Manager Administratorhandbuch*.
Automatic Update (Automatische Updates)	Damit können Sie den Automatic Update-Server manuell zurücksetzen. Weitere Informationen finden Sie unter „HP Smart Client Services“ auf Seite 68.
Component Manager (Komponenten-Manager)	Zum Entfernen von Systemkomponenten. Weitere Informationen finden Sie unter Component Manager (Komponenten-Manager) auf Seite 20.
Easy Update (einfache Udpates)	Öffnet den Easy Update-Assistenten. Easy Update ist eine Komponente von HP Easy Tools, mit der Sie die neuesten Softwareupdates für den Thin Client installieren können. **TIPP:** Wenn Sie bei der Durchführung eines Image-Updates **Thin Client-Konfiguration beibehalten** auswählen, werden alle zuvor konfigurierten Einstellungen beibehalten. Weitere Informationen über HP Easy Tools finden Sie im *HP Easy Tools Administratorhandbuch*.
Factory Reset (Auslieferungszustand)	Zum Wiederherstellen der Standard-Werkseinstellungen des Thin Client.
Snapshots (Momentaufnahmen)	Zum Wiederherstellen eines früheren Zustands oder der Standard-Werkseinstellungen des Thin Client.
SSHD Manager	Ermöglicht den Zugriff über ein Secure Shell.
ThinState	Mit HP ThinState kann entweder das gesamte Betriebssystem-Image oder nur seine Konfigurationseinstellungen kopiert oder wiederhergestellt werden.

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

Menüoption	Beschreibung
	Weitere Informationen finden Sie unter HP ThinState auf Seite 22.
VNC-Shadow	Zum Konfigurieren von VNC-Shadowing-Optionen. Weitere Informationen finden Sie unter VNC-Shadowing auf Seite 26.
Wireless-Statistiken	Zum Anzeigen von Informationen zu WLAN-Access Points.

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 26.
CPU Manager (Prozessormanager)	Zur Auswahl der Prozessorleistung zwischen **Balanced** (Ausgeglichen) und **High Performance**.
DHCP Options (DHCP-Optionen)	Zum Konfigurieren der DHCP-Optionen. Weitere Informationen finden Sie unter DHCP-Optionen auf Seite 27.
SCEP Manager	Ermöglicht die netzwerkbasierte Zertifikatsverwaltung.
Serial Manager	Zur Konfiguration serieller Geräte.
Keyboard Shortcuts (Tastenkombinationen)	Zum Erstellen, Ändern und Löschen von Tastenkombinationen.
Task Manager	Zum Überwachen der CPU-Auslastung und des Verlaufs der CPU-Auslastung für den Thin Client.
Text Editor	Öffnet einen einfachen Texteditor zum Anzeigen und Bearbeiten von Textdateien.
X Terminal	Zum Ausführen von Linux-Befehlen.

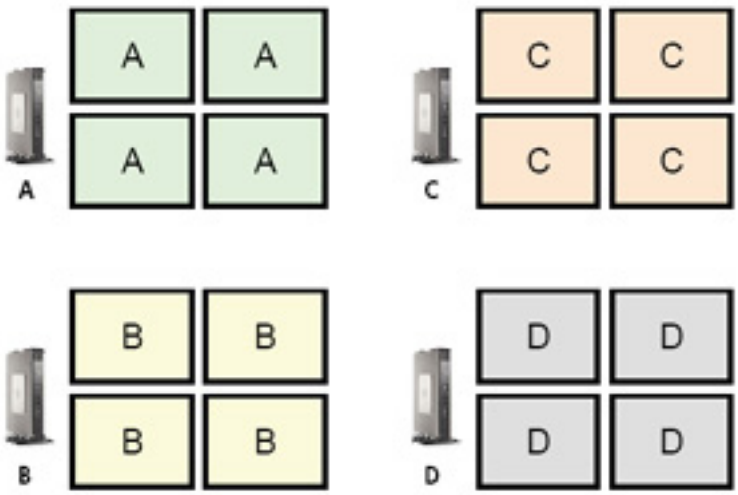
Tabelle 4-5 Control Panel > Miscellaneous (Systemsteuerung > Sonstiges)

Menüoption	Beschreibung
Snipping Tool	Zum Aufnehmen eines Schnappschusses einer rechteckigen Auswahl des Bildschirms, eines bestimmten Fensters oder des gesamten Bildschirms.

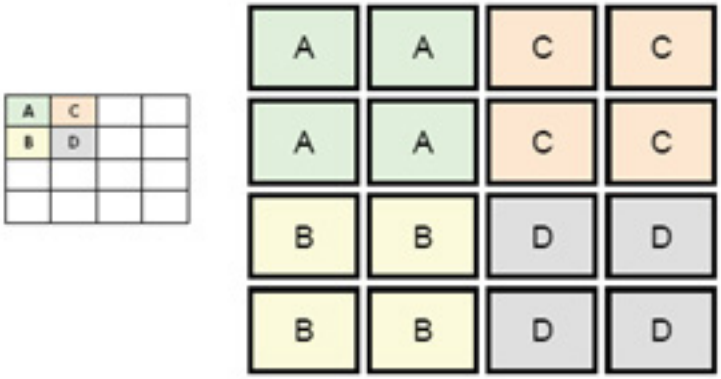
Clientaggregation

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

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

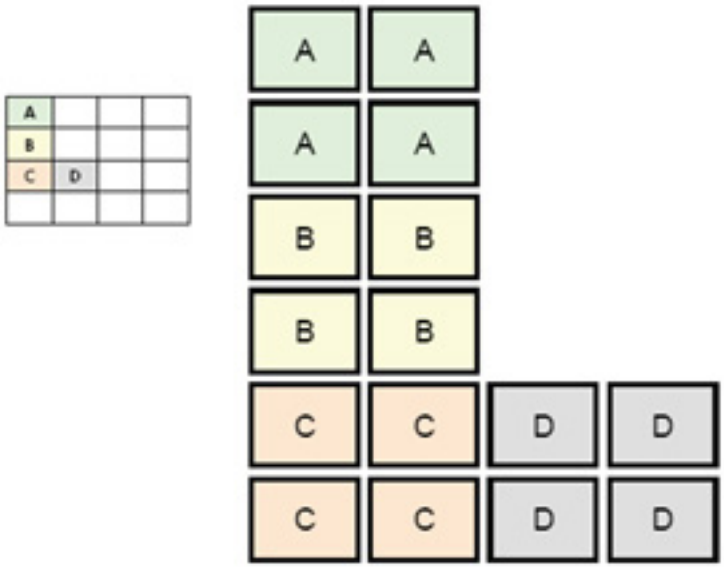


Mithilfe der Clientaggregation können Sie die vier Thin Clients in einem 4 x 4-Raster anordnen. Die folgende Abbildung zeigt eine der möglichen Anordnungen.



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

Die folgende Abbildung zeigt eine weitere mögliche Anordnung.



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

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

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

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

Konfigurieren der Clientaggregation

Die Konfiguration der Clientaggregation erfolgt in zwei Arbeitsschritten:

1. Konfigurieren der Aggregation-Clients auf Seite 14
2. Konfigurieren des Aggregation-Servers auf Seite 15

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 4 x 4-Raster kann jederzeit geändert werden, indem Sie auf das entsprechende Kästchen klicken und es 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 verschiedenen Monitore. Ein Profil beinhaltet Auflösung, Bildwiederholungsrate, Bittiefe und Ausrichtung.

So konfigurieren Sie Anzeigeprofile:

1. Wählen Sie in der Systemsteuerung **Peripherals > Display Preferences** (Peripehriegeräte > 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 Anzeigeprofile nützlich sein kann:

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

Konfigurieren von Druckern

So konfigurieren Sie einen Drucker:

1. Wählen Sie in der Systemsteuerung **Peripherals > Printers** (Peripheriegeräte > Drucker).
2. 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 aktivieren oder deaktivieren.

4. Auf der Seite **Classes** (Klassen) können Sie bestimmte Geräteklassen auswählen, die an Remotesitzungen umgeleitet werden sollen.
5. Wenn Sie fertig sind, 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 Netzwerkumgebung 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 dementsprechend 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: • None (Keine) • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS Beachten Sie Folgendes über TTLS und PEAP: • Die Einstellung der Option **Inner Authentication** (Innere Authentifizierung) sollte auf das eingestellt werden, was Ihr Server unterstützt.

Option	Beschreibung
	• Die Einstellung **CA Certificate** (CA-Zertifikat) sollte auf das Zertifikat des Servers auf dem lokalen Thin Client verweisen. • **Username** (Benutzername) und **Password** (Kennwort) sind die Anmeldeinformationen des Benutzers. Beachten Sie Folgendes über TLS: • Die Einstellung **CA Certificate** (CA-Zertifikat) sollte auf das Zertifikat des Servers auf dem lokalen Thin 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** (Drahtlos) verfügbaren Optionen.

HINWEIS: Diese Registerkarte ist nur verfügbar, wenn der Thin 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 dementsprechend eingeben, ob Sie IPv4 oder IPv6 verwenden.
Security Settings (Sicherheitseinstellungen)	Zum Festlegen der Authentifizierungseinstellung auf eine der folgenden Optionen: • None (Keine) • WEP • WPA/WPA2-PSK • 802.1X-TTLS • 802.1X-PEAP

Option	Beschreibung
	• 802.1X-TLS • EAP FAST Für WEP und WPA/WPA2-PSK müssen Sie nur den Netzwerkschlüssel eingeben und auf **OK** klicken. 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. Weitere Informationen über TTLS, PEAP und TLS finden Sie unter Drahtgebundene Netzwerkeinstellungen auf Seite 17.

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	Verwenden Sie diese Felder, um Proxy-Server-Informationen im folgenden Format einzugeben: `http://<ProxyServer>:<Port>` HP empfiehlt das Präfix `http://` für alle drei Proxy-Einstellungen zu verwenden, da es besser unterstützt wird. **HINWEIS:** Die Proxy-Einstellungen sind auf die Umgebungsvariablen **http_proxy**, **ftp_proxy** und **https_proxy** für das System eingestellt.

IPSec-Regeln

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

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

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

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

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

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

Konfigurieren von VPN-Einstellungen

HP ThinPro unterstützt zwei Arten von VPN:

- Cisco
- PPTP

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

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

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

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.

Component Manager (Komponenten-Manager)

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

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

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

So öffnen Sie den Komponenten-Manager:

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

Entfernen von Komponenten

So entfernen Sie Komponenten:

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

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

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

Rückgängigmachen einer Änderung

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

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

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

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

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

Dauerhaftes Anwenden der Änderungen

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

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

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

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 2 für weitere Informationen zu den Unterschieden zwischen den beiden Konfigurationen.

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

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

Option	Beschreibung
Launch the Connection Manager at start up (Beim Systemstart den Connection Manager starten)	Wenn aktiviert, wird HP Connection Manager beim Systemstart automatisch gestartet.
Enable right-click menu (Kontextmenü aktivieren)	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-Zugriffskontrollsicherheit 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 82.
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-Images oder der Konfiguration (Profil) auf einem anderen Thin Client eines kompatiblen Modells mit kompatibler Hardware.

Verwalten von HP ThinPro-Images

Aufzeichnung von HP ThinPro-Images auf einem FTP-Server

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

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

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie das **HP ThinPro Image** 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 Thin Client benannt.

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

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

6. 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 Thin Client-Flash-Laufwerks wird beschädigt.

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

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie das **HP ThinPro Image** 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. Wählen Sie **Retain HP ThinPro Configuration** (HP ThinPro-Konfiguration beibehalten), wenn Sie alle zuvor konfigurierten Einstellungen beibehalten möchten.
6. 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. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie das **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 **create a bootable USB flash drive** (Bootfähiges USB-Flash-Laufwerk erstellen) und klicken Sie dann auf **Next** (Weiter).

   Der Thin Client wird neu gestartet und Sie werden dann aufgefordert, ein USB-Flash-Laufwerk anzuschließen.
5. Schließen Sie ein USB-Flash-Laufwerk an einen USB-Anschluss am Thin Client an.
6. Wählen Sie das USB-Flash-Laufwerk und klicken Sie dann auf **Finish** (Beenden).

   Ein neues Fenster zeigt den Fortschritt an. 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 Thin Client-Flash-Laufwerks wird beschädigt. In diesem Zustand muss für den Thin Client über ein USB-Flash-Laufwerk ein neues Image erstellt werden.

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

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

Verwalten eines ThinPro-Profils

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

HINWEIS: Ein Profil kann unter Verwendung des Profil-Editors und Automatic Update auch vorkonfiguriert und bereitgestellt werden (siehe „Verwenden des Profile Editors“ auf Seite 72 und „HP Smart Client Services“ auf Seite 68 für weitere Informationen).

Speichern eines ThinPro-Profils auf einem FTP-Server

So speichern Sie ein ThinPro-Profil auf einem FTP-Server:

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

1. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
2. Wählen Sie **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 eines ThinPro-Profils über FTP oder HTTP

So stellen Sie ein ThinPro-Profil 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 eines ThinPro-Profils auf einem USB-Flash-Laufwerk

So speichern Sie ein ThinPro-Profil auf einem USB-Flash-Laufwerk:

1. Schließen Sie ein USB-Flash-Laufwerk an einen USB-Anschluss am Thin Client an.
2. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
3. Wählen Sie **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 eines ThinPro-Profils von einem USB-Flash-Laufwerk

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

1. Schließen Sie das USB-Flash-Laufwerk, das die Konfigurationsdatei enthält, an einen USB-Anschluss am Ziel-Thin Client an.
2. Wählen Sie in der Systemsteuerung **Management > ThinState** (Verwaltung > ThinState).
3. Wählen Sie **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 Thin 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 beim Zugriff auf den Thin 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 der Anzeige des Benachrichtigungs-Dialogfelds in Sekunden 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 anwendet 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 Hinzufügen von Zertifikaten zu einem ThinPro-Profil auf Seite 74.

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

SCEP Manager

So öffnen Sie den SCEP Manager:

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

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

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

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

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

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

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

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

DHCP-Optionen

So öffnen Sie den DHCP Option Manager:

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

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

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

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

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

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

So ändern Sie einen DHCP-Code:

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

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

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

- 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 verbindungsspezifisch 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, wird 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.
Anmeldedialogoptionen	Aktivieren Sie oder deaktivieren Sie diese Optionen im Anmeldedialog, um die Verbindung zu konfigurieren. **HINWEIS:** Diese Option ist nur für die Verbindungstypen Citrix, RDP und VMware Horizon View verfügbar. Die folgenden Optionen sind verfügbar: • **Feld „Benutzername“ anzeigen**

Tabelle 5-1 Gemeinsame Verbindungseinstellungen (Fortsetzung)

Option	Beschreibung
	• **Feld „Kennwort“ anzeigen** • **Feld „Domäne“ anzeigen** • **Kontrollkästchen „SmartCard“ anzeigen** • **Kontrollkästchen „Merken“ anzeigen** **HINWEIS:** Diese Option speichert den Benutzername und die Domäne, das Kennwort muss jedoch jedes Mal erneut eingegeben werden. • **Schaltfläche „Kennwort einblenden“ anzeigen**

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, ihn auf die Smart Zero-Konfiguration umzuschalten (siehe Anpassungscenter auf Seite 21) 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 auf den lokalen Desktop zurückzukehren, drücken Sie Strg+Alt+Ende.

6 Citrix-Verbindungen

- Citrix Receiver-Funktionen
- Citrix-Verbindung-Supportmatrix
- Citrix – Allgemeine Einstellungen
- Citrix – Verbindungsspezifische Einstellungen

Citrix Receiver-Funktionen

Die Citrix Receiver-Funktionen umfassen Folgendes:

- Einstellungen für die Fenstergröße und -tiefe
- Nahtloser Fenstersupport
- Einstellungen für die Audioqualität
- 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 auf Seite 33.

- 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.

- HP True Graphics (siehe HP True Graphics auf Seite 34)

HDX MediaStream

Wenn möglich, aktiviert HDX MediaStream die Verarbeitungsleistung des Thin Client, um den multimedialen Inhalt wiederzugeben. Auf der Seite Datacenter wird die komprimierte multimediale Information direkt an den Thin Client in ihrem ursprünglichen Format gesendet. Die Erfahrung variiert je nach Verarbeitungsleistung und der multimedialen Kapazität des Thin Client.

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	• 24 FPS
Auflösung	• 1080p • 720p
Video-Container	• WMV • AVI • MPG • MPEG • MOV • MP4
Video-Codecs	• WMV2 • WMV3/VC-1 • H.264/AVC/MPEG-4 Teil 10 • MPEG-4 Teil 2 • H.263 • DivX • Xvid • MPEG1
Audio-Codecs	• MP3 • WMA • AAC • PCM • MPEG-Audio

Tabelle 6-1 HDX MediaStream-Supportmatrix (Fortsetzung)

Funktion	Support
	• MLAW/ULAW

HP True Graphics

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

HP True Graphics erfordert eine der folgenden Citrix-Umgebungen:

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

Serverseitige Anforderungen für HP True Graphics

XenApp/XenDesktop

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

Nur vollständige Desktops oder nicht nahtlos arbeitende Anwendungen werden derzeit beschleunigt, wenn HP True Graphics verwendet wird. Remoteanwendungen, die in einem nahtlosen Fenster ausgeführt werden, profitieren von HP True Graphics nicht. Informationen, wie Sie erzwingen, dass Anwendungen nicht nahtlos ausgeführt werden, indem Sie die Einstellung **TWI Mode** (TWI-Modus) auf dem Thin Client konfigurieren, finden Sie unter Clientseitige Konfiguration von HP True Graphics auf Seite 35.

HDX 3D Pro

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

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

Überprüfen der Serveroptionen für die Komprimierung

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

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

Clientseitige Konfiguration von HP True Graphics

Komprimierungseinstellungen

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

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

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

Fenstereinstellungen

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

Monitorlayout- und Hardwarebeschränkungen

Beachten Sie die folgenden Beschränkungen für das Monitorlayout:

- Derzeit wird HP True Graphics nur für Konfigurationen mit maximal zwei Monitoren mit einer Auflösung von jeweils 1920 x 1200 unterstützt.
- Gedrehte Monitore werden möglicherweise nicht korrekt angezeigt.
- Durch die Standard-BIOS-Konfiguration verwendet der HP t420 Thin Client HP True Graphics nur für einen Monitor. Weitere Informationen finden Sie unter Aktivieren von HP True Graphics für mehrere Monitore auf dem HP t420 auf Seite 35.

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

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

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

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

TIPP: Diese Einstellungen können auch über HPDM oder über die BIOS-Tools konfiguriert werden, die in HP ThinPro enthalten sind (weitere Informationen finden Sie unter BIOS-Tool für Einstellungen auf Seite 83).

Citrix-Verbindung-Supportmatrix

Die folgende Tabelle beschreibt die unterstützten Citrix-Backends.

Tabelle 6-2 Citrix-Verbindung-Supportmatrix

	Backend

Tabelle 6-2 Citrix-Verbindung-Supportmatrix (Fortsetzung)

		XenApp	XenDesktop	VDI-in-a-Box
Zugriffstyp	Direkt (Betriebssystem-unabhängig)	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 7.

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

Option	Beschreibung
Enable HDX MediaStream (HDX MediaStream aktivieren)	Aktiviert HDX MediaStream. **WICHTIG:** Damit der HDX MediaStream aktiviert ist, müssen diese Einstellung und die Einstellung **Enable MultiMedia** (Aktivieren von MultiMedia) aktiviert sein. Beide Einstellungen finden Sie auf derselben Seite in Xen Connection General Settings Manager.
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)	Das Informationsfeld 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 Login for Direct and Web Connections (Smart Card-Anmeldung für direkte und Webverbindungen aktivieren)	Ermöglicht die Verwendung einer mit dem Thin Client verbundenen Smart Card für die Anmeldeauthentifizierung.
Enable Auto Reconnect (Automatische Neuverbindung aktivieren)	Ermöglicht eine automatische Verbindungswiederholung für Verbindungen, die getrennt wurden.
Enable Session Reliability (Sitzungszuverlässigkeit aktivieren)	Aktiviert die Funktion für die Citrix-Sitzungszuverlässigkeit. Weitere Informationen finden Sie in der Citrix-Dokumentation.
MultiMedia aktivieren	Aktiviert HDX MediaStream. **WICHTIG:** Damit der HDX MediaStream aktiviert ist, müssen diese Einstellung und die Einstellung **Enable HDX MediaStream** (Aktivieren des HDX MediaStreams) aktiviert sein. Beide Einstellungen finden Sie auf derselben Seite in Xen Connection General Settings Manager. **HINWEIS:** Diese Option muss möglicherweise deaktiviert werden, um Lync RTME unterstützen.

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

Option	Beschreibung
Enable Clipboard Redirection (Zwischenablageumleitung aktivieren)	Ermöglicht die Zwischenablageumleitung.
Use Data Compression (Datenkomprimierung verwenden)	Aktiviert die Datenkomprimierung für diese Verbindung.
Enable H264 Compression (H264-Komprimierung aktivieren)	Aktiviert die H.264-Komprimierung. Schauen Sie in der Citrix-Dokumentation nach, um festzustellen, ob diese Methode der Datenkomprimierung am besten für Ihren Anwendungsfall geeignet ist.
Enable Middle Button Paste (Einfügen mit mittlerer Taste aktivieren)	Aktiviert das Einfügen mit mittlerer Taste
User Agent String (Benutzer-Agent-Zeichenfolge)	Geben Sie eine Benutzer-Agent-Zeichenfolge ein, die für das Senden von Anforderungen an den Citrix-Server verwendet wird. Diese Option ist für NetScaler-Konfigurationen nützlich.
HDX Flash 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.
Sound (Audio)	Legt die Audioqualität fest oder deaktiviert den Sound vollständig.
SpeedScreen	Steuert die SpeedScreen-Latenzreduktion. Die empfohlene Einstellung ist **Auto** (Automatisch).
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.

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

Option	Beschreibung
Printer (Drucker)	Steuert, wie die lokale Druckerumleitung behandelt wird.
Webcam/Audio-Input (Webcam/Audio-Eingang)	Steuert, wie die Umleitung der lokalen Webcam und des Audioeingangs behandelt wird.
USB Drive Mapping and Redirection (USB-Laufwerkszuordnung und -Umleitung)	Steuert, ob die folgenden Optionen aktiviert sind: **HINWEIS:** Die unten aufgeführten Optionen können einzeln aktiviert und deaktiviert werden, wenn **USB Drive Mapping and Redirection** (USB-Laufwerkszuordnung und -Umleitung) aktiviert ist. • **USB Redirection** (USB-Umleitung) – Aktiviert die USB-Umleitung. • **Dynamic Drive Mapping** (Dynamische Laufwerkszuordnung) – Aktiviert die dynamische Laufwerkszuordnung. • **Static Drive Mapping (Legacy)** (Statische Laufwerkszuordnung (Vorgängerversion)) – Aktiviert die statische Laufwerkszuordnung, über die Sie Laufwerkszuordnungen für lokale Pfade angeben können.

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

Option	Beschreibung
TWI Mode (TWI-Modus)	Ermöglicht die Anzeige eines einzigen nahtlosen Fensters auf dem lokalen ThinPro-Desktop, als ob es eine systemeigene Anwendung wäre.
Default Window Size (Standard-Fenstergröße)	Wenn **TWI Mode** (TWI-Modus) auf **Force Seamless Off** (Nahtlos erzwingen - Aus) eingestellt ist, wird damit die Standard-Fenstergröße gesteuert.
Default Window Colors (Standard-Fensterfarben)	Legt die Standard-Farbtiefe fest.
Default 256 Color Mapping (Standardzuordnung 256 Farben)	Legt die Methode für die Farbzuordnung fest, wenn **Default Window Colors** (Standard-Fensterfarben) auf **256** eingestellt ist.
Show the Virtual Desktop on all monitors (Virtuellen Desktop auf allen Monitoren anzeigen)	Wenn die Option aktiviert ist, wird der virtuelle Desktop auf allen Monitoren angezeigt.
Left Monitor (Linker Monitor) Right Monitor (Rechter Monitor) Top Monitor (Oberer Monitor) Bottom Monitor (Unterer Monitor)	Wenn **Show the Virtual Desktop on all monitors** (Virtuellen Desktop auf allen Monitoren anzeigen) deaktiviert ist, können Sie mit diesen Feldern angeben, wie der virtuelle Desktop auf bestimmten Monitoren angezeigt wird.

Tabelle 6-6 Xen Connection General Settings Manager > Firewall

Option	Beschreibung
Proxy Type (Proxytyp)	Gibt den Proxytyp an.
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
Enable UseLocalIM (UseLocalIM aktivieren)	Verwendet die lokale Eingabemethode, um die Tastatureingabe zu interpretieren. Dies wird nur für europäische Sprachen unterstützt.
Use EUKS Number (EUKS-Nummer verwenden)	Regelt die Verwendung von Extended Unicode Keyboard Support (EUKS, Erweiterte Unicode-Tastaturunterstützung) auf Windows-Servern. Gültige Optionen werden nachfolgend beschrieben: • 0 – EUKS wird nicht verwendet. • 1 – EUKS wird als Ausweichoption verwendet. • 2 – EUKS wird möglichst immer verwendet.
Handling of keyboard shortcuts (Verwendung von Tastenkombinationen)	Gibt an, wie Tastenkombinationen verarbeitet werden sollen. Die folgenden Einstellungen sind verfügbar:

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

Option	Beschreibung
	• **Translated (Übersetzt)** – Tastenkombinationen gelten für den lokalen Desktop (Client) • **Direct in full screen desktops only (Direkt nur für Vollbilddesktops)** – Tastenkombinationen gelten für den Remotedesktop (Server), aber nur für eine nicht nahtlose ICA-Sitzung im Vollbildmodus • **Direct (Direkt)** – Tastenkombinationen gelten für den Remotedesktop (Server) für nahtlose und nicht nahtlose ICA-Sitzungen, wenn ihre Fenster den Tastaturfokus haben.
Stop Direct key handling (Verwendung von Direkttasten stoppen)	Gibt die Tastenkombination an, die die direkte Verarbeitung der Tastenkombinationen deaktiviert.
<List of keyboard shortcuts> (Liste der Tastenkombinationen)	Zum Hinzufügen von zu verarbeitenden Tastenkombinationen.

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.
Server Check Timeout (Server-Test-Timeout)	Zur Durchführung einer grundlegenden Konnektivitätsprüfung am ausgewählten Server und Port, legen Sie diese Option auf einen Wert fest, der nicht dem Standardwert **-1** entspricht.
TIPP: Durch Einstellen eines dieser Werte auf weniger als 0 wird die automatische Abmeldung deaktiviert. **HINWEIS:** Verzögerungen bei Citrix-Verarbeitungsprozessen können die Zeit bis zur automatischen Abmeldung verlängern.	

Citrix – Verbindungsspezifische Einstellungen

Die folgende Tabelle beschreibt die Einstellungen, die im Citrix Verbindungsmanager verfügbar sind. Diese Einstellungen sind verbindungsspezifisch 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 7.

Tabelle 6-9 Citrix Verbindungsmanager > Konfiguration

Option	Beschreibung
Name	Der Verbindungsname.

Tabelle 6-9 Citrix Verbindungsmanager > Konfiguration (Fortsetzung)

Option	Beschreibung
Service-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.
Connection Mode (Verbindungsmodus)	Legt den Verbindungsmodus auf eine der folgenden Optionen fest: • **PNAgent** • **StoreFront** • **StoreFront-SmartCard** • **Direct** Wenn Sie **PNAgent**, **StoreFront** oder **Direct** eingerichtet haben, können Sie den Benutzernamen, das Kennwort und die Domäne einstellen. Wenn Sie **StoreFront-SmartCard** eingerichtet haben, können Sie den Sicherheitsmodultyp und die durchzuführende Aktion festlegen, wenn die Smart Card entfernt wird.
Auto Start Resource (Autostart-Ressource)	Gibt den Namen einer Ressource an, die automatisch beim Herstellen einer Verbindung gestartet werden soll.
Auto Start Desktop (Autostart-Desktop)	Wenn diese Option ausgewählt ist, wird eine Desktopressource automatisch beim Herstellen einer Verbindung gestartet, falls verfügbar.
Auto Start Single Application (Auto-Start einzelner Anwendung)	Wenn diese Option ausgewählt ist und nur eine veröffentlichte Ressource vorhanden ist, startet diese Ressource beim Herstellen einer Verbindung automatisch.
Show applications on desktop (Anwendungen auf Desktop anzeigen)	Wenn diese Option ausgewählt ist, werden Remoteressourcen der Verbindung auf dem lokalen ThinPro-Desktop angezeigt.
Show applications on taskbar(Anwendungen in Taskleiste anzeigen)	Wenn diese Option ausgewählt ist, werden Remoteressourcen der Verbindung auf der lokalen ThinPro-Taskleiste angezeigt.
Auto Reconnect Applications on Login (Automatisches Neuverbinden von Anwendungen bei der Anmeldung)	Wenn diese Option ausgewählt ist, werden Ressourcen, die geöffnet waren, als sich der Benutzer zuletzt abgemeldet hat, wieder geöffnet, wenn er sich erneut anmeldet. **TIPP:** Wenn Sie die Citrix SmoothRoaming-Funktion nicht verwenden, deaktivieren Sie diese Option, um Ihre Verbindungsgeschwindigkeit zu erhöhen.

Tabelle 6-10 Citrix Verbindungsmanager > Sicherheit

Ignore Certificate Check (Zertifikat-Test ignorieren)	Wenn aktiviert, werden Zertifikate nicht überprüft und die Verbindung ist unsicher.
Force HTTPS Connection (HTTPS-Verbindung erzwingen)	Wenn aktiviert, wird die Verbindung gezwungen, das HTTPS-Protokoll zu verwenden, um dabei zu helfen, eine sichere Verbindung sicherzustellen.

HINWEIS: Siehe Gemeinsame Verbindungseinstellungen auf Seite 29 für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des Citrix Verbindungsmanager.

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
- Gateway und vermittelte Verbindungsunterstützung

RDP – Allgemeine Einstellungen

Die folgende Tabelle beschreibt die Einstellungen, die im RDP Connection General Settings Manager (Manager für allgemeine Verbindungseinstellungen) 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 7.

Tabelle 7-1 RDP Verbindungsmanager Allgemeine Einstellungen

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

RDP – Verbindungsspezifische Einstellungen

Die folgenden Tabellen beschreiben die Einstellungen, die im RDP Verbindungsmanager verfügbar sind. Diese Einstellungen sind verbindungsspezifisch 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 7.

Tabelle 7-2 RDP Verbindungsmanager-Einstellungen > Netzwerk

Option	Beschreibung
Name	Ein benutzerdefinierter Name für diese Verbindung.
Address (Adresse)	Die IP-Adresse oder der Servername für diese Verbindung oder die URL des RD Web Access-Feeds. Falls erforderlich, kann der Port nach einem Doppelpunkt an den Server angehängt werden (standardmäßig ist der Port für eine direkte RDP-Verbindung 3389). **HINWEIS:** Die URL des RD Web Access-Feeds muss mit `https://` beginnen. Standardmäßig wird dies automatisch hinzugefügt, gemäß den Angaben im Registrierungsschlüssel `rdWebFeedUrlPattern`, der das Muster der URL definiert.
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).
Server Probe (Servertest)	Startet den Servertest, der verwendet werden kann, um festzustellen, welche RDP-Funktionen von Ihrem RDP-Server unterstützt werden.

Tabelle 7-3 RDP Verbindungsmanager > Dienst

Option	Beschreibung
Service (Dienst)	Legt den RDP-Dienst auf eine der folgenden Optionen fest: • **Remote Computer** (Remotecomputer) – Wenn dieser Dienst verwendet wird, wird eine direkte RDP-Verbindung mit einem Remotecomputer erstellt. Eine Remoteanwendung oder eine andere Shell kann optional beim Herstellen einer Verbindung gestartet werden. Die folgenden zusätzlichen Optionen stehen für einen Remotecomputerdienst zur Verfügung: ◦ Wenn **Mode** (Modus) auf **Remote Application** (Remoteanwendung) festgelegt ist, ist im Feld **Application** (Anwendung) der Pfad der auszuführenden Anwendung angegeben. **TIPP:** Wenn Sie den Modus RDP Seamless Windows (RPD Nahtlose Fenster) verwenden, geben Sie den Pfad der `seamlessrdpshell.exe` auf Ihrem Server ein, gefolgt von einem Leerzeichen und anschließend den Pfad, auf dem die Anwendung ausgeführt wird. Siehe folgendes Beispiel: `c:\seamless\seamlessrdpshell.exe c:\Program Files \Microsoft\Word.exe` ◦ Wenn **Mode** (Modus) auf **Alternate Shell** (Andere Shell) festgelegt ist, ist im Feld **Command** (Befehl) der Befehl angegeben, der die Anwendung ausführt,

Tabelle 7-3 RDP Verbindungsmanager > Dienst

Option	Beschreibung
	die in der anderen Shell ausgeführt werden soll. Um Microsoft Word auszuführen, geben Sie z. B. `Word.exe` ein. Wenn **Mode** (Modus) auf **Alternate Shell** (Andere Shell) festgelegt ist, gibt das Feld **Directory** (Verzeichnis) den Pfad des Arbeitsverzeichnisses des Servers für Programmdateien der Anwendung an. Beispiel: Das Arbeitsverzeichnis für Microsoft Word ist `C:\Program Files\Microsoft`. • **RD Web Access** – Wenn dieser Dienst verwendet wird, wird eine Liste von RemoteApp-Ressourcen vom Server abgerufen und für den Benutzer angezeigt. Die eigentliche RDP-Verbindung wird gestartet, wenn eine Ressource ausgewählt wurde. Die folgenden zusätzlichen Optionen sind für RD Web Access verfügbar: ◦ **Keep resource selection window open** (Fenster für die Ressourcenauswahl nicht schließen) – Wenn diese Option ausgewählt ist, können Benutzer mehrere Ressourcen gleichzeitig im Ressourcenauswahlfenster öffnen. ◦ **Auto-start single resource** (Eine Ressource automatisch starten) – Wenn diese Option ausgewählt ist und nur eine veröffentlichte Ressource vorhanden ist, startet diese Ressource beim Herstellen einer Verbindung automatisch. ◦ **Resource filter** (Ressourcenfilter) und **Web Feed Browser** (Browser für Web-Feeds) – Diese Optionen können verwendet werden, um die Remoteressourcen zu beschränken, die dem Benutzer im Ressourcenauswahlfenster zur Verfügung gestellt werden. **HINWEIS:** Ein Vorteil der Verwendung von RD Web Access ist, dass damit die Details der vermittelten Verbindungen und die Lastenausgleichs-URL automatisch verarbeitet werden.

Tabelle 7-4 RDP Verbindungsmanager > Fenster

Option	Beschreibung
Hide Window Decoration (Fensterdekoration ausblenden)	Mit dieser Einstellung wird sichergestellt, dass Bildschirmelemente, wie z. B. die Menüleiste, die Minimierungs- und Schließ-Optionen sowie die Ränder von Fensterbereichen nicht angezeigt werden.
Window Size (Fenstergröße)	Legt die Fenstergröße auf **full** (voll), **fixed** (fest) oder **percent** (prozentual) fest.
Percentage Size (Prozentuale Größe)	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 resultierenden Größen können gerundet werden. **HINWEIS:** RemoteFX unterstützt nur eine feste Liste von Auflösungen.
Fixed Size (Feste Größe)	Wenn **Window Size** (Fenstergröße) auf **fixed** (fest) eingestellt ist, legt diese Option die Breite und Höhe, die das Desktopfenster einnimmt, in Pixeln fest.

Tabelle 7-5 RDP Verbindungsmanager > Optionen

Option	Beschreibung
Enable motion events (Bewegungsereignisse aktivieren)	Wenn aktiviert, werden die Mausbewegungen beständig an den RDP-Server übermittelt.
Enable data compression (Datenkomprimierung aktivieren)	Ermöglicht die Massenkomprimierung von Daten zwischen dem RDP-Server und dem RDP-Client.

Tabelle 7-5 RDP Verbindungsmanager > Optionen (Fortsetzung)

Option	Beschreibung
Enable deprecated RDP encryption (Veraltete RPD-Verschlüsselung aktivieren)	Aktiviert die RDP-Verschlüsselung der letzten Generation, wenn NLA nicht verfügbar ist.
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.
Enable buffering of RDP6 primitives (Pufferung von RDP6-Grundtypen aktivieren)	Wenn diese Option aktiviert ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
Certificate Verification Policy (Richtlinie zur Zertifikatverwendung)	Führen Sie eine der folgenden Aktionen aus: • **Akzeptieren Sie alle RDP-Server-Zertifikate** • **Verwenden beibehaltener Hosts; Bei unbekannten oder ungültigen Zertifikaten warnen** • **Überspringen beibehaltener Hosts; Bei unbekannten oder ungültigen Zertifikaten warnen** • **Nur mit vorab genehmigten RDP-Servern verbinden**
Hostname to send (Hostname für Sendevorgang)	Normalerweise wird der Thin Client-Hostname für Client-Zugriffslizenzen verwendet. Dieses Feld erlaubt das Senden eines anderen Werts. **TIPP:** Klicken Sie auf das Symbol **?** neben dieser Option, um weitere Informationen zu erhalten.
Load Balance Info (Lasteninformationen laden)	Verwenden Sie diese Option mit einer vermittelten RDP-Verbindung. **TIPP:** Klicken Sie auf das Symbol **?** neben dieser Option, um weitere Informationen zu erhalten.

Tabelle 7-6 RDP Verbindungsmanager > Lokale Ressourcen

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.
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.

Tabelle 7-6 RDP Verbindungsmanager > Lokale Ressourcen (Fortsetzung)

Option	Beschreibung
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 7-7 RDP Verbindungsmanager > Erfahrung

Option	Beschreibung
Choose your connection speed to optimize performance (Auswahl der Verbindungsgeschwindigkeit zur Optimierung der Leistung)	Das Auswählen einer Verbindungsgeschwindigkeit (**LAN**, **Broadband** (Breitband) oder **Modem**) wird die folgenden Optionen aktivieren oder deaktivieren, um die Leistung zu optimieren: • **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) Die Auswahl von **Client Preferred Settings** (Vom Client bevorzugte Einstellungen) ermöglicht dem RDP-Client die Auswahl der Optionen, die zur besten RPD-Erfahrung führen. Sie können auch Ihren eigene benutzerdefinierte Kombination von Optionen auswählen.
End-to-End Connection Health Monitoring (Ende-zu-Ende Verbindungs-Health-Überwachung)	Dient zum Aktivieren der Timeout-Options.
Warning Timeout (Warnungs-Zeitlimit)	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. Wenn die Option **Show Warning Dialog** (Dialogfeld mit Warnung anzeigen) ausgewählt ist, wird ein Warnungsdialogfeld angezeigt, wenn dieses Zeitlimit erreicht ist. Andernfalls wird die Warnung nur in das Verbindungsprotokoll geschrieben. **TIPP:** HP empfiehlt, den Wert des Zeitlimits für Netzwerke, die regelmäßig hoch belastet oder zeitweise überlastet sind bzw. ausfallen, zu erhöhen.
Recovery Timeout (Zeitlimit für Wiederherstellung)	Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client auf die Wiederherstellung der Verbindung wartet, bevor eine bestimmte Maßnahme eingeleitet wird. Am Ende dieser Frist versucht der RDP-Client kurz, erneut eine Verbindung mit der Sitzung aufzubauen.
Error Timeout (Fehler-Zeitlimit)	Gibt die Dauer in Millisekunden nach dem Erhalt des letzten Netzwerkverkehrs vom Server an, die der RDP-Client wartet, bevor er aufhört zu versuchen, die Verbindung mit diesem Server wiederherzustellen. **TIPP:** Klicken Sie auf das Symbol **?** neben diesem Feld, um weitere Informationen zu erhalten.

Tabelle 7-8 RDP Verbindungsmanager > Diagnose

Option	Beschreibung
Show Connection Health Graph (Diagramm zum Verbindungszustand anzeigen)	Wenn diese Option aktiviert ist, wird ein zweidimensionales Diagramm der Antwortzeit vom RDP-Server angezeigt, wenn die Verbindung gestartet wird. **TIPP:** Klicken Sie auf das Symbol **?** neben dieser Option, um weitere Informationen zu erhalten.
USB Redirection Analysis (Analyse der USB-Umleitungen)	Diese Funktion bestimmt und zeigt die aktuelle Umleitungsmethode für jedes umgeleitete USB-Gerät. **TIPP:** Klicken Sie auf das Symbol **?** neben dieser Option, um weitere Informationen zu erhalten.

HINWEIS: Siehe Gemeinsame Verbindungseinstellungen auf Seite 29 für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des RDP Verbindungsmanager.

Verwenden von RemoteFX mit RDP

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

RFX ist standardmäßig aktiviert. Der Administrator oder Benutzer muss keine Änderungen an den Einstellungen vornehmen, um es zu aktivieren. Der RDP-Client verhandelt mit jedem RDP-Server, den er kontaktiert, und wenn 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 ohne eine Änderung der Gruppenrichtlinien keine RemoteFX-Inhalte an Thin Clients, die für RDP 7.1 aktiviert sind. Überprüfen Sie die Einstellung für die folgende Richtlinie:

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

Darüber hinaus benötigt Windows Server 2012 und Windows Server 2012 R2 die folgenden Einstellungen, um auf **32-Bit** eingestellt werden zu können:

Lokale Computer Richtlinie > Computer-Konfiguration >-Administratorvorlagen > Windows-Komponenten > Remote Desktop Services > Remote Desktop-Sitzung Host > Remote-Sitzung Umgebung > Beschränken der maximalen Farbtiefe

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 Bildschirmeinstellungen 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 Thin Client.

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

HINWEIS: Remote Desktop Virtualization Host (RDVH)-Sitzungen mit Grafikkarten-Unterstützung unterstützen möglicherweise nur bestimmte Auflösungen und eine bestimmte Anzahl an Monitoren. Die Grenzwerte werden angegeben, wenn das RemoteFX virtuelle Grafikgerät 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 RDP-Client streamt, anstatt sie auf dem Remote-Host abzuspielen und über RDP neu zu codieren. Diese Technologie reduziert die Serverlast und den Netzwerk-Datenverkehr und verbessert die Multimedia-Erfahrung erheblich, da sie eine 24 fps-Wiedergabe von 1080p-Videos mit automatischer Audio-Synchronisierung unterstützt. MMR ist standardmäßig aktiviert. Der RDP-Client verhandelt mit jedem RDP-Server, den er kontaktiert, und wenn MMR verfügbar ist, wird es verwendet.

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

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

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

Da RemoteFX bereits akzeptable Multimedia-Leistung bietet, können Sie MMR mit 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 ein Gerät automatisch erkannt wird und in der Remotesitzung verfügbar ist, wenn ein Benutzer ein Gerät mit dem Thin Client verbindet. RDP unterstützt die Umleitung von vielen verschiedenen Arten von Geräten.

Verwenden einer USB-Umleitung mit RDP

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

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

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

- Der Server muss die USB-Umleitung unterstützen, um für den Thin Client verfügbar zu sein. Die USB-Umleitung für allgemeine Zwecke wird bei RDVH-Servern mit RemoteFX, Windows 8 und Windows Server 2012 unterstützt.
- Das Protokoll im USB-Manager in der Systemsteuerung muss auf RDP 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 über eine High-Level-Laufwerksumleitung an den Remote-Host um. Wenn ein Gerät wie ein USB-Flash-Laufwerk, ein USB-DVD-ROM-Laufwerk oder ein externes USB-Festplattenlaufwerk an den Thin Client angeschlossen ist, erkennt der Thin Client dies und stellt es im lokalen Dateisystem bereit. RDP erkennt dann ein bereitgestelltes Laufwerk und leitet es zum Remote-Host um. Auf dem Remote-Host erscheint es als neue Festplatte in Windows Explorer, mit dem Namen `<device label> on <client hostname>`; Beispiel: `Bill_USB on HP04ab598100ff`.

Es gibt drei Einschränkungen für diese Art von Umleitung.

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

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

Tabelle 7-9 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 um die Umleitung von USB-Massenspeichergeräten zu deaktivieren, jedoch anderen Geräten die Umleitung weiterhin zu ermöglichen, löschen Sie im Thin Client-Dateisystem die udev-Regel `/etc/udev/rules.d/010_usbdrive.rules`.

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-Umleitung** – Wenn die USB-Umleitung auf dem Remote-Host nicht verfügbar ist oder wenn der Drucker ein paralleler oder serieller Drucker ist, verwenden Sie die High-Level-Umleitung. Konfigurieren Sie den Drucker für die Verwendung eines lokalen Druckerspoolers und der RDP-Client richtet automatisch einen Remotedrucker ein, der Befehle für Druckspoolvorgänge über einen virtuellen Kanal vom Remote-Host an den Thin Client sendet.

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

HINWEIS: Weitere Informationen finden Sie unter Konfigurieren eines seriellen oder parallelen Druckers auf Seite 75.

Audioumleitung mit RDP verwenden

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

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

- RDP liefert die höchste Audioqualität, die die Netzwerkbandbreite zulässt. RDP reduziert die Audioqualität für die Wiedergabe bei Verbindungen mit geringer Bandbreite.
- Bei Standard-RDP stehen keine nativen Audio- oder Videosynchronisationsmechanismen zur Verfügung. Längere Videos können möglicherweise nicht mit Audio synchronisiert werden. MMR oder RemoteFX können dieses Problem beheben.

- HP empfiehlt eine High-Level Audio-Umleitung; eine USB-Umleitung der Audiogeräte ist jedoch nur möglich, wenn zusätzliche Funktionen, wie z. B. eine digitale Lautstärkeregelung, vorhanden sind. Für analoge Geräte ist nur eine High-Level-Umleitung verfügbar.
- Die Mikrofon-Umleitung ist standardmäßig aktiviert. Die Standard-Mikrofonlautstärke muss möglicherweise auf dem Thin Client angepasst werden. Die Einstellungen älterer Windows RDP-Server müssen geändert werden, um einen Audioeingang zu aktivieren.
- Sowohl die lokalen wie die Remote-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 RDP Verbindungsmanager **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 den Treiber des Smart Card-Lesegeräts auf dem Thin Client installiert werden. Standardmäßig werden die CCID- und Gemalto-Treiber installiert, die Unterstützung für die meisten der verfügbaren Smart Card-Lesegeräte bieten. Zusätzliche Treiber können installiert werden, indem Sie sie `/usr/lib/pkcs11/` hinzufügen.

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

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-Einstellungen

Die folgenden Tabellen beschreiben die Einstellungen, die im VMware Horizon View Connection Manager verfügbar sind. Diese Einstellungen sind verbindungsspezifisch 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 7.

Tabelle 8-1 VMware Horizon View Connection Manager > Netzwerk

Option	Beschreibung
Name	Eingabe des Namens für diese Verbindung.
Server	Den Hostnamen oder die IP-Adresse des VMware Horizon View-Servers eingeben.
Username (Benutzername)	Den für die Verbindung zu verwendenen 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 > Allgemein

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 57.
Don't start application maximized (Starten Sie keine Anwendung maximiert)	Wenn aktiviert, starten Anwendungen nicht maximiert in Windows.

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

Option	Beschreibung
Application Size (Anwendungsgröße)	Legt die Fenstergröße der Anwendung fest. Sie können **All Monitors** (alle Monitore), **Full Screen** (Vollbild), **Large Window** (großes Fenster) oder **Small Window** (kleines Fenster) auswählen.
Desktop Size (Desktop-Größe)	Legt die Fenstergröße des Desktops fest. Sie können **All Monitors** (alle Monitore), **Full Screen** (Vollbild), **Large Window** (großes Fenster) oder **Small Window** (kleines Fenster) auswählen.
Command Line Arguments (Befehlszeilenargumente)	Geben Sie alle gewünschten Befehlszeilenargumente ein, die für die Verbindung verwendet werden sollen. Führen Sie eine der folgenden Optionen aus, um weitere Hilfe zur Verwendung von erweiterten Befehlszeilenargumenten zu erhalten: • Geben Sie in der Befehlszeile `vmware-view--help` ein. • Weitere Informationen finden Sie in der Dokumentation für den VMware Horizon View-Client für Linux, die von VMware unter http://www.vmware.com bereitgestellt wird.

Tabelle 8-3 VMware Horizon View Connection Manager > Sicherheit

Option	Beschreibung
Close After Disconnect (Nach Verbindungsunterbrechung schließen)	Sorgt dafür, dass sich der VMware Horizon View-Client automatisch schließt, nachdem sich Benutzer an ihren Desktops abgemeldet haben oder die Sitzung aufgrund eines Fehlers beendet wurde. Diese Option ist eine Sicherheitsfunktion und so konzipiert, dass ein Benutzer keinen weiteren Schritt durchführen muss, um sich vollständig abzumelden nachdem er mit seiner Desktop-Sitzung fertig ist. Diese Option ist standardmäßig aus Sicherheitsgründen aktiviert, kann aber deaktiviert werden, wenn Benutzer nach dem Abmelden von einer Sitzung häufig zu einem neuen Desktop-Pool wechseln und sich nicht wieder komplett neu anmelden möchten.
Hide top Menu bar (Obere Menüleiste ausblenden)	Macht die obere Menüleiste für Benutzer unsichtbar. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie diese Option, wenn der Benutzer während einer VMware Horizon View-Sitzung Zugriff auf Optionen für die Fenstergröße oder Desktop-Pool-Auswahl haben möchte.
Prevent users from changing server address (Verhindert, dass B	Wenn aktiviert, können Standardbenutzer, die Serveradresse nicht ändern.
Connection Security Levels (Verbindungs-Sicherheitsstufen)	Verwenden Sie die **Connection Security Level** (Sicherheitsstufe der Verbindung) zum Einstellen der Sicherheitsstufe, die der VMware Horizon View-Client bei der Verbindung zum Server verwendet. **HINWEIS:** Nähere Informationen über das Verhalten von Verbindungs-Sicherheitsstufen finden Sie unter Anforderungen für die VMware Horizon View HTTPS- und Zertifikatverwaltung auf Seite 58.

Tabelle 8-4 VMware Horizon View Connection Manager > RDP-Optionen

Option	Beschreibung
Enable motion events (Bewegungsereignisse aktivieren)	Aktiviert das Senden von Bewegungen für diese Verbindung.

Tabelle 8-4 VMware Horizon View Connection Manager > RDP-Optionen (Fortsetzung)

Option	Beschreibung
Enable data compression (Datenkomprimierung aktivieren)	Aktiviert die Datenkomprimierung für diese Verbindung.
Enable deprecated RDP encryption (Veraltete RPD-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.
Enable buffering of RDP6 primitives (Pufferung von RDP6-Grundtypen aktivieren)	Wenn diese Option aktiviert ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
Certificate Verification Policy (Richtlinie zur Zertifikatverwendung)	Führen Sie eine der folgenden Aktionen aus: • **Akzeptieren Sie alle RDP-Server-Zertifikate** • **Verwenden beibehaltener Hosts; Bei unbekannten oder ungültigen Zertifikaten warnen** • **Überspringen beibehaltener Hosts; Bei unbekannten oder ungültigen Zertifikaten warnen** • **Nur mit vorab genehmigten RDP-Servern verbinden**
Hostname to send (Hostname für Sendevorgang)	Normalerweise wird der Thin Client-Hostname für Client-Zugriffslizenzen verwendet. Dieses Feld erlaubt das Senden eines anderen Werts. **TIPP:** Klicken Sie auf das Symbol **?** neben dieser Option, um weitere Informationen zu erhalten.
Load Balance Info (Lasteninformationen laden)	Verwenden Sie diese Option mit einer vermittelten RDP-Verbindung. **TIPP:** Klicken Sie auf das Symbol **?** neben dieser Option, um weitere Informationen zu erhalten.
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 die seriellen und parallelen Anschlüsse des Thin Client der Remotesitzung zu.
Enable printer mapping (Druckerzuweisung aktivieren)	Ordnet die lokale Druckwarteschlange der Remotesitzung zu. Verwenden Sie diese Option, wenn die USB-Umleitung auf dem Remote-Host nicht verfügbar ist oder wenn der Drucker ein paralleler oder serieller Drucker ist. Konfigurieren Sie den Drucker für die Verwendung eines lokalen Druckerspoolers und der VMware Horizon View-Client richtet automatisch einen Remotedrucker ein, der Befehle für Druckspoolvorgänge über einen virtuellen Kanal vom Remote-Host an den Thin Client sendet. Diese Methode erfordert, dass der Drucker auf dem Thin Client konfiguriert ist und ein Windows-Treiber auf dem Thin Client angegeben wurde, da der VMware Horizon View-Client für den Remote-Host angeben muss, welcher Treiber für den Remotedrucker verwendet werden soll. Dieser Windows-Treiber muss mit dem Treiber übereinstimmen, den der Drucker verwenden würde, wenn er an ein Windows-Betriebssystem lokal angeschlossen wäre. Diese Informationen finden Sie normalerweise unter **Modell** in den Druckereigenschaften.
Shared folders (Freigegebene Ordner)	**Add** (Hinzufügen), **Remove** (Entfernen) oder **Edit** (Bearbeiten) freigegebener Ordner.

Tabelle 8-5 VMware Horizon View Connection Manager > RDP-Erfahrung

Option	Beschreibung
Enable MMR (MMR aktivieren)	Aktiviert die Multimedia-Umleitung.
Choose your connection speed to optimize performance (Auswahl der Verbindungsgeschwindigkeit zur Optimierung der Leistung)	Das Auswählen einer Verbindungsgeschwindigkeit (**LAN**, **Broadband** (Breitband) oder **Modem**) wird die folgenden Optionen aktivieren oder deaktivieren, um die Leistung zu optimieren: • **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) Die Auswahl von **Client Preferred Settings** (Vom Client bevorzugte Einstellungen) ermöglicht dem VMware Horizon View-Client die Auswahl der zu verwendenden Optionen. Sie können auch Ihren eigene benutzerdefinierte Kombination von Optionen auswählen.

HINWEIS: Siehe Gemeinsame Verbindungseinstellungen auf Seite 29 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 eines 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 47.

Geräte-Umleitung mit VMware Horizon View verwenden

USB-Umleitung mit VMware Horizon View verwenden

Um USBR 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 48

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 48.

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 49 für weitere Informationen.

Audioumleitung 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\fDisableAudioCapture` 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 VMware Horizon View-Client verwendet eine High-Level-Audioumleitung. Um das USB-Headset umzuleiten, verwenden Sie den USB-Manager des Thin Client und wählen Sie das USB-Headset aus, das umgeleitet werden soll. Stellen Sie sicher, dass die **VMware Horizon View** als 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: Für eine Anmeldung am VMware Horizon View Manager-Administratorserver mit einer Smart Card muss der lokale Smart Card-Treiber auf dem Thin Client installiert sein. Unter Smart Card-Umleitung mit RDP verwenden auf Seite 50 finden Sie weitere Informationen zur Smart Card-Treiberinstallation. Nach der Anmeldung am Remote-Host wird die Smart Card über einen virtuellen Kanal und nicht USBR an den Remote-Host übergeben. Diese Umleitung über einen virtuellen Kanal stellt sicher, dass die Smart Card für Aufgaben wie E-Mail-Signaturen, Bildschirmsperren usw. verwendet werden kann, führt aber möglicherweise dazu, dass die Smart Card nicht als Smart Card-Gerät im Geräte-Manager von Windows angezeigt wird.

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

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 48.

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 einen Pool aus, der eines der folgenden Protokolle unterstützt:
   - PCoIP
   - RDP
2. Wählen Sie unter dem Menü **Connection** (Verbindung) **Settings** (Einstellungen) aus.
3. Ändern Sie das Protokoll mithilfe des Dropdown-Feldes neben **Connect Via** (verbinden über).

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 erfüllt wird:

- 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 8-6 VMware Horizon View Sicherheitsstufen von Zertifikaten

	Sicherheitsstufen		
	Unsichere Verbindungen verweigern	**Warnen**	**Alle Verbindungen erlauben**

Tabelle 8-6 VMware Horizon View Sicherheitsstufen von Zertifikaten (Fortsetzung)

		Sicherheitsstufen		
Vertrauens-würdigkeit des Zertifikats	**Vertrauenswürdig**	Vertrauenswürdig	Vertrauenswürdig	Vertrauenswürdig
	Selbstsigniert	Fehler	Warnung	Nicht vertrauenswürdig
	Abgelaufen	Fehler	Warnung	Nicht vertrauenswürdig
	Nicht vertrauenswürdig	Fehler	Fehler	Nicht vertrauenswürdig

Tabelle 8-7 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 entsperrtes Schlosssymbol an.
Warnung	Stellt mit dem Dialog für eine Zertifikatswarnung eine Verbindung her und zeigt ein rotes entsperrtes Schlosssymbol an.
Fehler	Erlaubt die Verbindung nicht

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 (Web Browser Verwaltung der allgemeinen Verbindungseinstellungen) 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 7.

Tabelle 9-1 Web Browser Connection General Settings Manager (Web Browser Verwaltung der allgemeinen Verbindungseinstellungen)

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 7.

Tabelle 9-2 Web Browser Connection Manager > Konfiguration

Option	Beschreibung
Name	Der Verbindungsname.
URL	Die URL für die Verbindung.
Intended Use (Beabsichtigte Verwendung)	Festlegen der beabsichtigten Verwendung der Verbindung auf **Citrix**, **RDP** oder **Internet**.
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 29 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 Thin Client auf die ThinPro-Konfiguration eingestellt ist. Weitere Informationen finden Sie unter Vergleich von ThinPro und Smart Zero auf Seite 2.

- 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 verbindungsspezifisch 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 7.

Tabelle 10-1 TeemTalk Connection Manager > Konfiguration

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 29 für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des TeemTalk Connection Manager.

Die folgenden Tabellen beschreiben die Einstellungen, die im TeemTalk-Sitzungsassistenten (Komponente des TeemTalk Connection Manager) verfügbar sind. Diese Einstellungen sind verbindungsspezifisch 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 > Konfiguration“, auf Seite 62.

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 63 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** (Einstellungen speichern), 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)	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. **HINWEIS:** Diese Option wird erst beim nächsten Systemstart aktiviert und überschreibt die Optionen **Show Configuration Bar** (Konfigurationsleiste anzeigen) und **Save Current Window Position** (aktuelle Fensterposition speichern).
Browser Command (Browserbefehl)	Geben Sie den Befehl in das Feld ein, mit dem Ihr Internetbrowser ausgeführt wird, wie z. B. : `/ display html links Firefox`
Command Line Start Up Options (Startoptionen für Befehlszeile)	Wird verwendet, um einen alternativen Speicherort für die Startoptionen anzugeben. **HINWEIS:** Für spezifische Informationen über die HP TeemTalk Befehlszeilen-Startoptionen siehe *HP TeemTalk Terminal Emulator Benutzerhandbuch*.

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 verbindungsspezifisch 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 7.

Tabelle 10-7 XDMCP Connection Manager > Konfiguration

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 XDMCP Connection Manager > Konfiguration (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 Anzeigekonfiguration für die Verbindung einzurichten. Wenn Sie keine Konfiguration festlegen, wird die Standardkonfiguration verwendet.

HINWEIS: Siehe Gemeinsame Verbindungseinstellungen auf Seite 29 für Informationen zu den verfügbaren Einstellungen auf der letzten Seite des XDMCP Connection Manager.

SSH Verbindungseinstellungen

Secure Shell (SSH) ist die am häufigsten verwendete Möglichkeit, Remotezugriff für Befehlszeilen auf UNIX-ähnlichen Betriebssystemen, z. B. Linux, BSD und HP-UX zu erhalten. SSH ist außerdem verschlüsselt.

Die folgende Tabelle beschreibt die Einstellungen, die im TeemTalk Connection Manager verfügbar sind. Diese Einstellungen sind verbindungsspezifisch 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 7.

Tabelle 10-8 Secure Shell Connection Manager > Konfiguration

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 Sitzung zu starten, die den Befehl ausführt. Sobald der Befehl ausgeführt wird, geht die Sitzung zu Ende. Wenn kein Befehl angegeben wird, wird die Sitzung normal ausgeführt, als wäre die Option nicht ausgewählt worden.
Foreground color (Vordergrundfarbe)	Die Standardfarbe für den Text in der SSH-Sitzung.
Background color (Hintergrundfarbe)	Die Standardfarbe für den Hintergrund in der SSH-Sitzung.
Font (Schriftart)	Gültige Optionen sind: **7X14**, **5X7**, **5X8**, **6X9**, **6X12**, **7X13**, **8X13**, **8X16**, **9X15**, **10X20** und **12X24**.

HINWEIS: Siehe Gemeinsame Verbindungseinstellungen auf Seite 29 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 verbindungsspezifisch 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 7.

Tabelle 10-9 Telnet Connection Manager > Konfiguration

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 29 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 Verbindungsmanager verfügbar sind. Diese Einstellungen sind verbindungsspezifisch 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 7.

Tabelle 10-10 Custom Connection Manager > Konfiguration

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 29 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 ThinPro-Profile konfigurieren können, die auf eine große Anzahl Thin Clients verteilt werden können. Diese Funktion wird als Automatic Update (Automatische Updates) bezeichnet.

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

- Unterstützte Betriebssysteme
- Voraussetzungen für HP Smart Client Services
- Abrufen von HP Smart Client Services
- Anzeigen der Automatic Update-Website
- Ein Automatic Update-Profil erstellen
- Aktualisieren von Thin Clients

Unterstützte Betriebssysteme

HP Smart Client Services unterstützt die folgenden Betriebssysteme:

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

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

Voraussetzungen für HP Smart Client Services

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

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

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

Abrufen von HP Smart Client Services

So rufen Sie die HP Smart Client Services ab:

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

Anzeigen der Automatic Update-Website

1. 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. Ermitteln Sie die MAC-Adresse des Thin Client über die Systeminformationen. In den folgenden Schritten wird z. B. die MAC-Adresse `00fcab8522ac` verwendet.
2. Verwenden Sie den Profile Editor zum Erstellen oder Ändern eines ThinPro-Profils (siehe „Verwenden des Profile Editors“ auf Seite 72), bevor Sie das ThinPro-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 ThinPro-Profil wie folgt 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 Thin Client neu, der die angegebene MAC-Adresse verwendet, um die automatische Aktualisierung einzuleiten.

Aktualisieren von Thin Clients

- Verwenden der Methode zur Aktualisierung per Übertragung
- Verwenden der Methode zur Aktualisierung per DHCP-Kennung
- Verwenden der Methode zur Aktualisierung per DNS-Alias
- Verwenden der Methode zur manuellen Aktualisierung

Verwenden der Methode zur Aktualisierung per Übertragung

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

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

TIPP: Um zu überprüfen, ob die Aktualisierung per Übertragung funktioniert, führen Sie 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 78.

Verwenden der Methode zur Aktualisierung per DHCP-Kennung

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

Beispiel für die Durchführung DHCP-Kennung

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

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

1. Auf dem Server-Desktop wählen Sie **Start > Administrative Tools > DHCP** (Start > Verwaltungstools > DHCP).
2. Klicken Sie in der linken Seite des Bildschirms **DHCP** auf die Domäne, mit der die Thin 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** (Vordefinierte Optionen und Werte) auf **Add** (Hinzufügen).
5. Im Feld **Option Type** (Optionstyp) konfigurieren Sie die Optionen wie in der folgenden Tabelle beschrieben.

Tabelle 11-1 Beispieloptionen für DHCP-Kennung

Feld	Eintrag
Name	Geben Sie `auto-update` ein.
Datentyp	Wählen Sie **Einstellungen** aus.
Code	Typ `137`.
Beschreibung	Typ `HP Automatic Update`.

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

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

8. Um das Setup abzuschließen, klicken Sie auf **OK**. Die DHCP-Kennung kann jetzt für die Aktualisierung bestimmter Thin Clients verwendet werden.

Verwenden der Methode zur Aktualisierung per DNS-Alias

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

So konfigurieren Sie die Aktualisierungsmethode mit DNS Alias:

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

Verwenden der Methode zur manuellen Aktualisierung

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

HINWEIS: 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 Thin Clients bestimmte Aktualisierungen 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 im 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. Wählen Sie **Preserve thin client configuration** (Thin Client-Konfiguration beibehalten) aus, wenn Sie alle zuvor konfigurierten Einstellungen beibehalten möchten.
7. Klicken Sie auf **OK** und der Thin Client ruft die Aktualisierungen ab.

12 Verwenden des Profile Editors

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

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

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

Dieser Abschnitt enthält die folgenden Themen:

- Zugriff auf den Profile Editor
- Laden eines ThinPro-Profils
- Ändern eines ThinPro-Profils
- Konfigurieren eines seriellen oder parallelen Druckers

HINWEIS: Siehe „Registrierungsschlüssel“ auf Seite 94 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 ThinPro-Profils

Der Profile Editor lädt automatisch das ThinPro-Profil, 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 ThinPro-Profil:

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

Ändern eines ThinPro-Profils

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

- Auswählen der Plattform für ein ThinPro-Profil
- Konfigurieren einer Standardverbindung für ein ThinPro-Profil
- Ändern von Registrierungseinstellungen eines ThinPro-Profils

- Hinzufügen von Dateien zu einem ThinPro-Profil
- Speichern des ThinPro-Profils

Auswählen der Plattform für ein ThinPro-Profil

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

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

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

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

So konfigurieren Sie die Plattformeinstellungen eines ThinPro-Profils:

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

WICHTIG: Stellen Sie sicher, dass Sie für jeden Hardwaretyp ein anderes ThinPro-Profil erstellen.

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

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

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

Konfigurieren einer Standardverbindung für ein ThinPro-Profil

So konfigurieren Sie eine Standardverbindung für ein ThinPro-Profil:

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

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

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

Ändern von Registrierungseinstellungen eines ThinPro-Profils

So ändern Sie die Standard-Registrierungseinstellungen für ein ThinPro-Profil:

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

Hinzufügen von Dateien zu einem ThinPro-Profil

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

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

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

Hinzufügen einer Konfigurationsdatei zu einem ThinPro-Profil

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

   HINWEIS: Dateien können auch über die Schaltfläche **Export File** (Datei exportieren) exportiert werden, wenn weitere Einzelheiten über die Datei erforderlich sind.
3. Geben Sie im Feld **Path** (Pfad) den Pfad ein, in dem die Datei auf dem Thin Client installiert werden soll.
4. Legen Sie im Abschnitt **File details** (Dateidetails) die Felder **Owner** (Besitzer), **Group** (Gruppe) und **Permissions** (Berechtigungen) auf die entsprechenden Werte fest.

   HINWEIS: 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. Wählen Sie **Save** (Speichern) aus, um das Hinzufügen der Konfigurationsdatei zum ThinPro-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 Werkseinstellungen wiederhergestellt werden.

Hinzufügen von Zertifikaten zu einem ThinPro-Profil

ThinPro-Profile enthalten automatisch Zertifikate, die in 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 in ein ThinPro-Profil:

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

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

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

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

4. Wählen Sie **Save** (Speichern) aus, um das Hinzufügen des Zertifikats zum ThinPro-Profil abzuschließen.
5. Verwenden Sie nach der Installation des ThinPro-Profils den **Certificate Manager** (Zertifikats-Manager), um sicher zu gehen, dass das Zertifikat ordnungsgemäß importiert wurde.

Hinzufügen eines symbolischen Links zu einem ThinPro-Profil

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

Speichern des ThinPro-Profils

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

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

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

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

TIPP: Zum Beenden des Testdruckmodus müssen Sie den Drucker eventuell wieder ausschalten oder die **Feed** (Papierzufuhr)-Taste nochmals drücken, damit die Diagnoseseite 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** (Verbindungen), wählen Sie **New connection** (Neue Verbindung) aus und klicken Sie auf **OK**. Legen Sie den Registrierungsschlüssel **portMapping** (Port-Zuordnung) 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** (Verbindungen), wählen Sie **New connection** (Neue Verbindung) aus und klicken Sie auf **OK**. Legen Sie unter dem Ordner **xfreerdpOptions** den Registrierungsschlüssel **portMapping** (Port-Zuordnung) 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 75 ein.

   Stellen Sie den Wert **device** (Gerät) auf den Port ein, an dem der Drucker angeschlossen wird. So wäre beispielsweise der erste serielle Port `/dev/ttyS0`, der zweite serielle Port wäre `/dev/ttyS1` usw. Verwenden Sie für serielle USB-Drucker das Format `/dev/ttyUSB#`, wobei `#` die Nummer des Ports ist, beginnend mit 0.

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

13 Fehlerbeseitigung

In diesem Kapitel werden folgende Themen behandelt:

- Fehlerbeseitung bei der Netzwerkverbindung
- Fehlerbeseitigung bei Firmware-Beschädigung
- Fehlerbeseitigung bei abgelaufenen Citrix-Kennwörtern
- Verwenden der Systemdiagnose für die Fehlerbeseitigung

Fehlerbeseitung bei der Netzwerkverbindung

1. Führen Sie den Ping-Befehl für den gewünschten Server mit den folgenden Schritten aus:

   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 ist, ist der Thin Client möglicherweise vom Netzwerk getrennt und es entsteht eine lange Verzögerung ohne Systemausgabe.

2. Wenn der Thin Client nicht auf den Ping-Befehl reagiert, gehen Sie wie folgt vor:

   a. Überprüfen Sie das Netzwerkkabel und überprüfen Sie die Netzwerkeinstellungen in der Systemsteuerung.

   b. Versuchen Sie, den Ping-Befehl für andere Server oder Thin Clients auszuführen.

   c. Wenn Sie andere Thin Clients erreichen können, überprüfen Sie, ob Sie die richtige Serveradresse eingegeben haben.

   d. Führen Sie einen Ping unter Verwendung der IP-Adresse durch anstelle des Domänennamens oder umgekehrt.

3. Überprüfen Sie die Systemprotokolle indem Sie Folgendes durchführen:

   a. 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 der Thin Client zwei Signaltöne ausgibt, nachdem er eingeschaltet wurde, oder nicht zu starten scheint, ist möglicherweise die Gerätefirmware beschädigt. Dieses Problem kann behoben werden, indem das Thin Client-Image von http://www.hp.com heruntergeladen, das Image auf ein austauschbares USB-Flash-Laufwerk kopiert und anschließend der Thin Client mit diesem Flash-Laufwerk gestartet wird.

Installieren eines neuen Images der Thin Client-Firmware

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. Fahren Sie den Thin Client herunter.
6. Schließen Sie das USB-Flash-Laufwerk an den Thin Client an.
7. Schalten Sie den Thin Client ein und er startet mit dem USB-Flash-Laufwerk.
8. Folgen Sie den Anleitungen auf dem Bildschirm, um ein neues Image auf dem Thin Client zu installieren.
9. Wenn der Re-Imaging-Prozess abgeschlossen ist, entfernen Sie das USB-Flash-Laufwerk und drücken Sie die Eingabetaste.

Fehlerbeseitigung bei abgelaufenen Citrix-Kennwörtern

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

Verwenden der Systemdiagnose für die Fehlerbeseitigung

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

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

Speichern von Systemdiagnosedaten

1. Schließen Sie ein USB-Flash-Laufwerk am Thin Client an.
2. 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 diese.

   HINWEIS: Eine kostenlose Kopie von 7-Zip für Windows erhalten Sie unter http://www.7-zip.org/download.html.

2. Stecken Sie das USB-Flash-Laufwerk, das die gespeicherte Systemdiagnosedatei enthält, ein, und kopieren Sie anschließend **Diagnostic.tgz** auf den Desktop.
3. Klicken Sie mit der rechten Maustaste auf **Diagnostic.tgz** und wählen Sie **7-Zip > Extract files** (Dateien entpacken ...).
4. Öffnen Sie den neu erstellten Ordner mit der Bezeichnung **Diagnostic** (Diagnose) und führen Sie Schritt 3 in **Diagnostic.tar** aus.

Dekomprimieren der Systemdiagnosedateien auf Linux- oder Unix-basierten Systemen

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

Anzeigen der Systemdiagnosedateien

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

Anzeigen von Dateien im Ordner Befehle

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

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 die USB-Updates aktiviert sind (siehe Anpassungscenter auf Seite 21), können Sie ein USB-Flash-Laufwerk verwenden, um gleichzeitig mehrere Add-ons und Zertifikate zu installieren oder zum Bereitstellen eines Profils.

So führen Sie USB-Updates durch:

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

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

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

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

3. 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
`hptc-bios-cfg -G [options] [filename]`	Ruft die aktuellen BIOS-Einstellungen ab und speichert sie in der angegebenen Datei, sodass sie angezeigt oder geändert werden können (standardmäßig CPQSETUP.TXT).
`hptc-bios-cfg -S [options] [filename]`	Schreibt die BIOS-Einstellungen aus der angegebenen Datei (standardmäßig CPQSETUP.TXT) ins BIOS.
`hptc-bios-cfg -h`	Zeigt eine Liste der Optionen an.

BIOS Flashing-Tool

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

Syntax	Beschreibung
`hptc-bios-flash [options] <ImageName>`	Flasht das BIOS mit dem spezifizierten BIOS-Image.
`hptc-bios-flash -h`	Zeigt eine Liste der Optionen an.

C Ändern der Größe der Flash-Laufwerk-Partition

WICHTIG: HP Thin Clients, die mit HP ThinPro 5.2 oder höher ausgeliefert werden, verwenden das gesamte Flash-Laufwerk. Die Image-Aufzeichnungsmethoden wurden aktualisiert, um ein möglichst kleines Image aufzuzeichnen. Dadurch können Images von größeren Flash-Laufwerken auf kleineren Flash-Laufwerken bereitgestellt werden, die über ausreichend Speicherplatz für das aufgezeichnete Image verfügen. Eine Änderung der Größe der Partition des Flash-Laufwerks sollte für HP Thin Clients nicht mehr erforderlich sein, die mit HP ThinPro 5.2 oder höher ausgeliefert werden. Beachten Sie für Thin Clients mit HP ThinPro, die aus einem bestimmten Grund nicht das gesamte Flash-Laufwerk verwenden, die folgenden Informationen.

Um den gesamten Speicherplatz des Flash-Laufwerks zu verwenden, müssen Sie die Größe der Partition anpassen und das Dateisystem erweitern, sodass es diesen zusätzlichen Platz aufnimmt. Dies kann erreicht werden, indem man das Skript `resize-image` verwendet.

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

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

Syntax	Beschreibung
`resize-image`	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.
`resize-image --size <SizeInMB>` Beispiel: `resize-image --size 1024`	Mit dieser Syntax können Sie die Ziel-Partitionsgröße in Megabyte (MB) als Parameter angeben und die Änderung anschließend bestätigen.

`resize-image --no-prompt`
– oder –
`resize-image --no-prompt --size <SizeInMB>`
Beispiel: `resize-image --no-prompt --size 1024`
	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 zum Anpassen des Smart Zero-Anmeldebildschirms 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 (Auffüllen)

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 (Farbe)

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 (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 (Größe)

Typ	Beschreibung
Parameter	WWxHH, wobei WW der Breite in absoluten Pixeln oder einem Prozentsatz der Bildschirmbreite und HH der Höhe in absoluten Pixeln oder einem Prozentsatz der Bildschirmhöhe entspricht.
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 (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 (Ausrichtung)

Typ	Beschreibung
Parameter	[left I hcenter I right] [top I vcenterIbottom]
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 (Kontext)

Typ	Beschreibung
Parameter	[login I desktop I all]
Beispiel	context: login;
Standard	all
Verwendung	Legt fest, ob das Element nur auf dem Anmeldebildschirm für das Protokoll bzw. auf dem Desktopbildschirm für das Protokoll (wenn

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

Typ	Beschreibung
	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** • **color** (Farbverlauf) – legt die Volltonfarbe für den Hintergrund des Bildschirms fest, wenn keine Farbverläufe spezifiziert sind • **padding** (Auffüllen) – legt den Standardabstand für alle nachfolgenden Elemente fest

Tabelle D-10 Anmeldebildschirm > Elemente > Benutzerdefiniert > Gradient (Farbverlauf)

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

Tabelle D-11 Anmeldebildschirm > Elemente > Benutzerdefiniert > Type (Typ)

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 (Achse)

Typ	Beschreibung
Parameter	[height I width]
Beispiel	axis: width;

Tabelle D-12 Anmeldebildschirm > Elemente > Benutzerdefiniert > Axis (Achse) (Fortsetzung)

Typ	Beschreibung
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 der halben Bildschirmhöhe oder der halben Bildschirmbreite entspricht.

Tabelle D-13 Anmeldebildschirm > Elemente > Benutzerdefiniert > Metric (Metrisch)

Typ	Beschreibung
Parameter	[linear I squared]
Beispiel	metric: linear;
Standard	squared
Verwendung	Für radiale Farbverläufe legt die Metrik fest, ob die Farbinterpolation zwischen Punkten anhand einer dx2+dy2-Distanzberechnung (quadratisch) oder der Quadratwurzel der Zahl (linear) erfolgt. Die quadratische Interpolation ist zum Zeichnen etwas schneller.

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

Typ	Beschreibung
Parameter	Eine durch Leerzeichen getrennte Liste von [Wert,Farbe]-Paaren, wobei der Wert eine Fließkommabruchzahl 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 in 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 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 (Dithering)

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 (Bild)

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 (Quelle)

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 (wahr) sein Seitenverhältnis beibehalten, um es innerhalb des spezifizierten Rechtecks einzupassen. Bei false (falsch) 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 (Lokalisierung)

Typ	Beschreibung
Parameter	Lokalisierter Text
Beispiel	text-de_DE: Dieser Text ist in Deutsch.;
Standard	Nicht zutreffend
Verwendung	Wenn der Text im übereinstimmenden Gebietsschema ist, wird er für die Zeichenfolge verwendet. Die unterstützten Textzeichenfolgen lauten: • de_DE (Deutsch) • en_US (Englisch) • es_ES (Spanisch) • fr_FR (Französisch) • ja_JP (Japanisch) • zh_CN (Vereinfachtes Chinesisch) **HINWEIS:** Die Dateicodierung ist UTF-8.

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 (gebietsschemaspezifische Schriftart)

Typ	Beschreibung
Parameter	gebietsschemaspezifische Schriftart

Tabelle D-22 Anmeldebildschirm > Text > font-locale (gebietsschemaspezifische Schriftart) (Fortsetzung)

Typ	Beschreibung
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 (Schriftart)

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 (Schriftartgröße)

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

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 (maximale Höhe)

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 verschiedene Weisen geändert werden:

- Verwenden einer **_File and Registry** -Task in HPDM
- Mithilfe der Komponente Registry Editor (Registrierungseditor) des Profile Editors und der anschließenden Bereitstellung des neuen Profils
- Mithilfe des Registry Editors in der HP ThinPro-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 > ComponentMgr
- root > ConnectionManager
- root > ConnectionType
- root > CpuMgr
- root > DHCP
- root > Dashboard
- root > Display
- root > Network
- root > SCIM
- root > ScepMgr
- root > Search
- 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 > restore-points
- root > screensaver
- root > security
- root > sshd
- root > time
- root > touchscreen
- root > translation
- root > usb-update
- root > users
- root > vncserver

root > Audio

Tabelle E-1 root > Audio

Registrierungsschlüssel	Beschreibung
`root/Audio/AdjustSoundPath`	Legt den vollständigen Pfad auf den wiedergegebenen Sound fest, wenn die Wiedergabelautstärke über die Lautstärkeregler geändert wird.
`root/Audio/OutputMute`	Wenn der Wert 1 ist, sind die internen Lautsprechern und die Kopfhörerbuchse stumm geschaltet.
`root/Audio/OutputScale`	Bestimmt die Lautstärke-Skalierung für die internen Lautsprecher und die Kopfhörerbuchse, die zwischen 1 und 400 liegt.
`root/Audio/OutputScaleAuto`	Wenn der Wert 1 ist, wird der `OutputScale` -Wert automatisch basierend auf dem Thin Client-Modell gesetzt.
`root/Audio/OutputVolume`	Legt die Lautstärke für die internen Lautsprechern und die Kopfhörerbuchse fest, die zwischen 1 bis 100 liegt.
`root/Audio/PlaybackDevice`	Legt fest, dass das Gerät für die Wiedergabe verwendet wird.
`root/Audio/RecordDevice`	Legt fest, dass das Gerät für die Aufzeichnung verwendet wird.
`root/Audio/RecordMute`	Wenn auf 1 gesetzt, ist das Mikrofon stumm geschaltet.
`root/Audio/RecordScale`	Legt die Laustärkeskalierung für die Mikrofonbuchse fest, die zwischen 1 und 400 liegt.
`root/Audio/RecordScaleAuto`	Wenn der Wert 1 ist, wird der `RecordScale` -Wert automatisch basierend auf dem Thin Client-Modell gesetzt.

Tabelle E-1 root > Audio (Fortsetzung)

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

root > CertMgr

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

root > ComponentMgr

Tabelle E-2 root > ComponentMgr

Registrierungsschlüssel	Beschreibung
root/ComponentMgr/General/ NotShowDeleteSnapshotWarning	Wenn der Wert 1 ist, wird beim Löschen eines Schnappschusses keine Warnung angezeigt.

root > ConnectionManager

Tabelle E-3 root > ConnectionManager

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

root > ConnectionType

root > ConnectionType > custom

Tabelle E-4 root > ConnectionType > custom

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/authorizations/user/add	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/custom/authorizations/user/general	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/custom/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/custom/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
root/ConnectionType/custom/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/custom/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/custom/connections/<UUID>/autoReconnect	Bei Einstellung auf den Wert 1 wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/custom/connections/<UUID>/autoReconnectDelay	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn `autoReconnect` auf 1 eingestellt ist.
root/ConnectionType/custom/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/custom/connections/<UUID>/autostartDelay	Gibt die Wartezeit in Sekunden an, bevor die Verbindung beim Systemstart gestartet wird. Beim Standardwert 0 wird die Verbindung sofort nach dem Systemstart gestartet. Diese Einstellung wird nur wirksam, wenn `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 Hauptbefehl für die benutzerdefinierte Verbindung an.
root/ConnectionType/custom/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/custom/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/custom/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/custom/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/custom/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf `Default Connection` eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/custom/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/custom/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/custom/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/custom/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/custom/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/custom/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/custom/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/custom/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.
root/ConnectionType/custom/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den

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

Registrierungsschlüssel	Beschreibung
	Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
`root/ConnectionType/custom/coreSettings/serverRequired`	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp ist.
`root/ConnectionType/custom/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/custom/coreSettings/watchPid`	Wenn der Wert 1 ist, wird die unter dem Namen `AppName` angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/custom/coreSettings/wrapperScript`	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/custom/gui/CustomManager/name`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/custom/gui/CustomManager/status`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/custom/gui/CustomManager/title`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect`	Steuert den Status des Widgets **Auto reconnect** (Automatisches Neuverbinden) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Auto start priority** (Automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Enter command to run** (Auszuführenden Befehl eingeben) im Verbindungsmanager für

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

Registrierungsschlüssel	Beschreibung
	diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Fallback Connection** (Ausweichverbindung) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Show icon on desktop** (Symbol auf Desktop zeigen) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. 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/waitForNetwork`	Steuert den Status des Widgets **Wait for network before connecting** (Vor dem Verbinden auf Netzwerk warten) im Verbindungsmanager für diesen Verbindungstyp. 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

Tabelle E-5 root > ConnectionType > firefox

Registrierungsschlüssel	Beschreibung
`root/ConnectionType/firefox/authorizations/user/add`	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
`root/ConnectionType/firefox/authorizations/user/general`	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
`root/ConnectionType/firefox/connections/<UUID>/address`	Legt die URL- oder IP-Adresse für die Verbindung an.
`root/ConnectionType/firefox/connections/<UUID>/afterStartedCommand`	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/firefox/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/firefox/connections/<UUID>/autoReconnect	Bei Einstellung auf den Wert 1 wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/firefox/connections/<UUID>/autoReconnectDelay	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn autoReconnect auf 1 eingestellt ist.
root/ConnectionType/firefox/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/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	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/firefox/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/connections/<UUID>/enablePrintDialog	Wenn der Wert 1 ist, kann der Dialog „Drucken“ des Webbrowsers verwendet werden.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/firefox/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/firefox/connections/<UUID>/forbiddenFiles	Dieser Registrierungsschlüssel funktioniert nur, wenn **Allow connections to manage their own settings** (Verbindungen die Verwaltung der eigenen Einstellungen ermöglichen) im Web Browser Connection General Settings Manager aktiviert ist. Die Dateien, die im Wert dieses Registrierungsschlüssels aufgeführt sind, werden entfernt, sobald eine Web Browser-Verbindung beendet wurde. Die Dateinamen sollte durch Kommas getrennt

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

Registrierungsschlüssel	Beschreibung
	werden und ein Platzhalter wird unterstützt. Beispiel: `*.rdf,cookies.sqlite`
`root/ConnectionType/firefox/connections/<UUID>/fullscreen`	Wenn der Wert 1 ist, startet der Webbrowser im Vollbildmodus. Wenn `KioskMode` deaktiviert ist, ist die Benutzeroberfläche des Browsers im Vollbildmodus zugänglich.
`root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon`	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
`root/ConnectionType/firefox/connections/<UUID>/intendedUse`	Legt die vorgesehene Nutzung dieser Web Browser-Verbindung auf `Citrix`, `RDP` oder `Internet` fest.
`root/ConnectionType/firefox/connections/<UUID>/kioskMode`	Wenn der Wert 1 ist, wird der Internetbrowser im Kioskmodus gestartet, was bedeutet, dass der Internetbrowser im Vollbildmodus gestartet wird, (selbst wenn `fullscreen` auf 0 eingestellt ist) und die Benutzeroberfläche des Browsers nicht zur Verfügung steht.
`root/ConnectionType/firefox/connections/<UUID>/label`	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf `Default Connection` 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/USBrelevant`	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
`root/ConnectionType/firefox/coreSettings/appName`	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/firefox/coreSettings/className`	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/firefox/coreSettings/editor`	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/firefox/coreSettings/generalSettingsEditor`	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/firefox/coreSettings/icon16Path`	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
`root/ConnectionType/firefox/coreSettings/icon32Path`	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/firefox/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.
root/ConnectionType/firefox/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/firefox/coreSettings/restartIdleTime	Legt die Zeit in Minuten fest, bevor der Webbrowser neu gestartet wird, wenn das System keine Benutzereingabe erhält. Wenn der Wert 0 ist, ist Neustart deaktiviert.
root/ConnectionType/firefox/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp 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-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/firefox/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/firefox/general/enableUserChanges	Wenn der Wert 1 ist, werden die Einstellungen, die im Dialog Firefox-Einstellungen konfiguriert sind, nach jeder Sitzung gespeichert.
root/ConnectionType/firefox/gui/FirefoxManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/address	Steuert den Status des Widgets **URL** im Verbindungsmanager für diesen Verbindungstyp. 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-5 root > ConnectionType > firefox (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect	Steuert den Status des Widgets **Auto reconnect** (Automatisches Neuverbinden) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Auto start priority** (Automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Enable print dialog** (Dialogfeld „Drucken“ aktivieren) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Fallback Connection** (Ausweichverbindung) im Verbindungsmanager für diesen Verbindungstyp. 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/hasDesktopIcon	Steuert den Status des Widgets **Show icon on desktop** (Symbol auf Desktop zeigen) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Enable kiosk mode** (Kiosk-Modus aktivieren) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Enable full screen** (Vollbild aktivieren) im Verbindungsmanager für diesen Verbindungstyp. 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

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

Registrierungsschlüssel	Beschreibung
	ausgeblendet. Durch die Einstellung `read-only` wird das Widget im schreibgeschützten Modus angezeigt.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/waitForNetwork`	Steuert den Status des Widgets **Wait for network before connecting** (Vor dem Verbinden auf Netzwerk warten) im Verbindungsmanager für diesen Verbindungstyp. 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

Tabelle E-6 root > ConnectionType > freerdp

Registrierungsschlüssel	Beschreibung
`root/ConnectionType/freerdp/authorizations/user/add`	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
`root/ConnectionType/freerdp/authorizations/user/general`	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
`root/ConnectionType/freerdp/connections/<UUID>/ExtraArgs`	Gibt zusätzliche Argumente zum Xfreerdp-Client an. Führen Sie `xfreerdp –help` über ein X-Terminal aus, um alle verfügbaren Argumente zu sehen.
`root/ConnectionType/freerdp/connections/<UUID>/SingleSignOn`	
`root/ConnectionType/freerdp/connections/<UUID>/address`	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll. Die Portnummer kann nach einem Doppelpunkt am Ende angehängt werden. Beispiel: `servername:3389`
`root/ConnectionType/freerdp/connections/<UUID>/afterStoppedCommand`	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
`root/ConnectionType/freerdp/connections/<UUID>/application`	Gibt eine alternative Shell oder Anwendung an, die ausgeführt werden soll.
`root/ConnectionType/freerdp/connections/<UUID>/attachToConsole`	
`root/ConnectionType/freerdp/connections/<UUID>/audioLatency`	Legt den durchschnittlichen Offset in Millisekunden zwischen dem Audiostream und der Anzeige der entsprechenden Videoframes nach dem Entschlüsseln fest.
`root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/edit`	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
`root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/execution`	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Ausführen dieser Verbindung.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/autoReconnect	Bei Einstellung auf den Wert 1 wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnectDelay	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn autoReconnect auf 1 eingestellt ist.
root/ConnectionType/freerdp/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/freerdp/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/freerdp/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/freerdp/connections/<UUID>/clipboardExtension	Bei Einstellung des Werts auf 1, ist die Zwischenablage sowohl zwischen verschiedenen RDP-Sitzungen als auch zwischen RDP-Sitzungen und dem lokalen System aktiviert.
root/ConnectionType/freerdp/connections/<UUID>/compression	Bei Einstellung des Werts auf 1, wird die Komprimierung von RDP-Daten zwischen dem Client und dem Server aktiviert.
root/ConnectionType/freerdp/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/freerdp/connections/<UUID>/directory	Gibt das Systemstart-Verzeichnis an, in dem eine alternative Shell-Anwendung ausgeführt wird.
root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX	Wenn die Einstellung 1 ist, wird die Multimedia-Umleitung deaktiviert, wenn eine gültige RemoteFX-Sitzung aufgebaut wurde.
root/ConnectionType/freerdp/connections/<UUID>/domain	Legt die Standarddomäne fest, die während der Anmeldung für den Remote-Host benötigt wird. Wenn keine Domäne angegeben ist, wird die Standarddomäne für den Remote-Host verwendet.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/freerdp/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount	Legt die Anzahl der Videoframes fest, die der Server pushen kann, ohne auf eine Bestätigung vom Client zu warten. Niedrigere Zahlen führen zu einem schneller reagierenden Desktop, jedoch auch zu einer niedrigeren Bildfrequenz. Bei Einstellung des Werts auf 0 wird die Frame-Bestätigung bei den Client-Server-Interaktionen nicht verwendet.
root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress	Legt den RD-Gateway-Servernamen oder die Adresse fest.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain	Legt die Standarddomäne fest, die während der Anmeldung vom RD-Gateway benötigt wird. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn GatewayUsesSameCredentials auf 1 eingestellt ist, wird dieser Wert deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled	Bei Einstellung des Werts auf 1 wird die Verwendung des RD-Gateway erwartet.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword	Gibt das Standardkennwort an, das vom RD-Gateway während der Anmeldung benötigt wird. Dieser Wert ist normalerweise verschlüsselt. In der Regel, wird diese Einstellung bei Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername zur Anmeldung verwendet wird. Wenn 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 RD-Gateway dieselben Anmeldeinformationen, die auch zur Verbindung mit dem endgültigen Server verwendet werden.
root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf Default Connection eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo	Dieser Wert ist der Lastenausgleich-Cookie, der zu Vermittlungszwecken beim Herstellen einer Verbindung an den Server gesendet wird und entspricht dem Feld Loadbalanceinfo in der Datei .rdp. Der Standardwert ist leer.
root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection	Bei Einstellung des Werts auf 1 werden die lokalen nicht-USB-Speicherpartitionen über die Storage zum Remote-Host umgeleitet. Wenn der Wert 0 ist, ist die Erweiterung für nicht-USB-Speicher Partitionen deaktiviert, die nicht von HP ThinPro verwendet werden.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld **Domain** (Domäne) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/password	Wenn der Wert 1 ist, wird das Feld **Password** (Kennwort) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen **Remember me** (Anmeldedaten merken) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/showpassword	Wenn der Wert 1 ist, wird die Schaltfläche **Show password** (Kennwort anzeigen) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird die Schaltfläche angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird die Schaltfläche ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/smartcard	Wenn der Wert 1 ist, wird das Kontrollkästchen **Smart card login** (Smart Card-Anmeldung) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet. Dieses Kontrollkästchen wird möglicherweise nicht angezeigt, wenn keine Smart Card erkannt wird, auch wenn diese Option aktiviert ist.
root/ConnectionType/freerdp/connections/<UUID>/loginfields/username	Wenn der Wert 1 ist, wird das Feld **User Name** (Benutzername) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/freerdp/connections/<UUID>/mouseMotionEvents	Bei Einstellung des Werts auf 0 werden Mausbewegungsereignisse nicht an den Server gesendet. Dies kann dazu führen, dass einige Benutzerfeedbacks, wie z. B. Quickinfos, nicht richtig funktionieren.
root/ConnectionType/freerdp/connections/<UUID>/offScreenBitmaps	Bei Einstellung des Werts auf 0 werden Off-Screen-Bitmaps deaktiviert. Dies kann die Leistung etwas erhöhen, bewirkt aber, dass die Bildschirmblöcke asynchron aktualisiert werden, wodurch auch Übergänge nicht gleichmäßig aktualisiert werden.
root/ConnectionType/freerdp/connections/<UUID>/password	Legt das Standardkennwort fest, das der Remote-Host während der Anmeldung benötigt. Dieser Wert ist normalerweise verschlüsselt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagDesktopComposition	Die Einstellung des Werts 1 ermöglicht die Desktopgestaltung, wie z. B. durchsichtige Rahmen, wenn dies vom Server unterstützt wird. Das Ausschalten der Desktopgestaltung kann die Leistung für Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagFontSmoothing	Die Einstellung des Werts 1 ermöglicht eine Schriftglättung, wenn dies vom Server unterstützt wird und aktiviert ist. Das Ausschalten dieser Option kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorSettings	Die Einstellung des Werts 1 deaktiviert das Blinken des Cursors, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorShadow	Die Einstellung des Werts 1 schaltet den Mauscursor-Schatten aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger

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

Registrierungsschlüssel	Beschreibung
	Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoMenuAnimations	Die Einstellung des Werts 1 schaltet Menüanimationen aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoTheming	Die Einstellung des Werts 1 schaltet die Designs der Benutzeroberfläche aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWallpaper	Die Einstellung des Werts 1 schaltet die Desktop-Hintergrundbilder aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWindowDrag	Die Einstellung des Werts 1 schaltet die Option zum Ziehen von Fenstern mit vollem Inhalt aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Stattdessen werden die Fensterumrisse verwendet. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/freerdp/connections/<UUID>/portMapping	Wenn der Wert 1 ist, werden alle seriellen und parallelen Anschlüsse über die Erweiterung der `Ports` zum Remote-Host weitergeleitet. Durch die Einstellung 0 wird die Erweiterung deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/printerMapping	Wenn der Wert 1 ist, werden alle lokal über CUPS definierten Drucker über die `Printers` zum Remote-Host weitergeleitet werden. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Durch die Einstellung 2 werden USB-Audiogeräte entsprechend der Angaben im USB-Manager weitergeleitet.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoStartSingleResource	Wenn der Wert 1 ist und wenn nur eine einzige veröffentlichte Ressource (RemoteApp-Programm oder virtueller Desktop) vom Server zurückgegeben wird, wird diese Ressource automatisch gestartet.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/alias	Gibt den Alias einer Ressource für den Ressourcenfilter an. RemoteApp- und Desktopressourcen mit einem passenden Alias sind für Benutzer verfügbar.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/name	Gibt den Namen einer Ressource für den Ressourcenfilter an. RemoteApp- und Desktopressourcen mit einem passenden Namen sind für Benutzer verfügbar.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/keepResourcesWindowOpened	Wenn der Wert 0 ist, wird das Ressourcenauswahlfenster automatisch geschlossen, nachdem eine Ressource gestartet wurde. Wenn der Wert 1 ist, bleibt das Ressourcenauswahlfenster geöffnet, nachdem Ressourcen gestartet wurden. Dies ermöglicht es dem Benutzer, mehrere Ressourcen zu starten, bevor das Ressourcenauswahlfenster geschlossen wird.
root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering	Wenn der Wert 1 ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs	Wenn der Wert 1 ist, werden RDP 8-Codecs verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der

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

Registrierungsschlüssel	Beschreibung
	RDP 8-Codecs deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert 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 Server verwendet.
root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec	Wenn der Wert 1 ist, werden RDP 8 H.264-Codecs verwendet, wenn verfügbar. Für diese Einstellung gibt es bekannte visuelle Fehler, insbesondere bei Konfigurationen mit mehreren Monitoren, daher sollte sie als experimentell und nicht unterstützt betrachtet werden. Durch Aktivieren dieser Einstellung wird einfach der Server darauf hingewiesen, dass der Thin Client H.264 für die Desktopanzeige unterstützt. Der Server muss auch H.264 unterstützen und der Server trifft die endgültige Entscheidung darüber, welche Codecs verwendet werden. Diese Einstellung wirkt sich nur auf die Desktop-Codecs aus. Codecs für die Multimedia-Umleitung sind davon nicht betroffen.
root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec	Wenn der Wert 1 ist, werden progressive RDP 8-Codecs verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der progressiven RDP 8-Codecs deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
root/ConnectionType/freerdp/connections/<UUID>/remoteApp	Gibt den Namen einer verfügbaren Anwendung an, die im RAIL-Modus (Remote Application Integrated Locally) ausgeführt werden soll.
root/ConnectionType/freerdp/connections/<UUID>/remoteDesktopService	Wenn der Wert `Remote Computer` ist, wird eine direkte RDP-Verbindung mit einem Remotecomputer hergestellt. Wenn der Wert `RD Web Access` ist, wird zuerst eine Verbindung mit einem RD Web Access-Dienst hergestellt, um einen Feed der veröffentlichte RemoteApp-Ressourcen abzurufen.
root/ConnectionType/freerdp/connections/<UUID>/remoteFx	Wenn der Wert 1 ist, wird RemoteFX in der Form von RDP 7.1 verwendet, wenn verfügbar. Diese Einstellung ist veraltet und ist möglicherweise in einer zukünftigen Version von HP ThinPro nicht mehr enthalten. Diese Einstellung sollte nur bei einem Fehler des RemoteFX-Protokolls deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
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.
root/ConnectionType/freerdp/connections/<UUID>/securityLevel	Legt die Sicherheitsstufen von Zertifikaten fest. Wenn der Wert 0 ist, sind alle Verbindungen zulässig. Wenn der Wert 1 ist, werden beibehaltene Hosts überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 2 ist, werden beibehaltene Hosts nicht überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 3 ist, werden alle unsichere Verbindungen verweigert.
root/ConnectionType/freerdp/connections/<UUID>/sendHostname	Legt den Thin Client-Hostnamen fest, der an den Remote-Host gesendet wird. Wenn keine Eintragung vorgenommen wird, wird der System-Host-Namen gesendet. Der Registrierungsschlüssel `root/ConnectionType/freerdp/general/sendHostname` muss auf `hostname` eingestellt sein, damit dieser Schlüssel verwendet wird.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/showConnectionGraph	Dies ist eine Diagnosefunktion. Wenn der Wert 1 ist, wird beim Starten der Sitzung ein separates Programm gestartet, um den Verbindungszustand grafisch darzustellen.
root/ConnectionType/freerdp/connections/<UUID>/smartcard	Wenn der Wert 1 ist, ist die lokale Smart Card-Authentifizierung zum Remote-Host zulässig. Zurzeit wird dadurch Network Level Authentication (NLA) deaktiviert.
root/ConnectionType/freerdp/connections/<UUID>/sound	Durch die Einstellung 1 werden die Wiedergabe- und Aufnahmegeräte über die Erweiterung von `Audio` zum Remote-Host umgeleitet. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Durch die Einstellung 2 werden USB-Audiogeräte entsprechend der Angaben im USB-Manager weitergeleitet. In der Regel, empfiehlt HP, dass dieser Wert auf 1 gesetzt wird, sodass High-Level-Audio-Umleitung verwendet wird. Dadurch wird die Audioqualität verbessert und sichergestellt, dass Client-Audio, das mittels anderer Methoden umgeleitet wird (wie zum Beispiel `Multimedia Redirection`), den lokalen Audioeinstellungen entspricht.
root/ConnectionType/freerdp/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/freerdp/connections/<UUID>/timeoutError	Legt die Anzahl von Millisekunden fest, die nach dem Verlust einer Verbindung gewartet werden, bevor der Versuch, eine Verbindung mit dem Server herzustellen, aufgegeben wird. Wenn der Wert 0 ist, dann wird immer wieder versucht, die Verbindung wieder herzustellen.
root/ConnectionType/freerdp/connections/<UUID>/timeoutRecovery	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung für die Wiederherstellung des Netzwerkbetriebs vergehen, bevor versucht wird eine erneute Verbindung zu erzwingen.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarning	Legt die Anzahl von Millisekunden fest, die nach dem Ausfall einer Verbindung mit dem Server vergehen, bevor der Benutzer gewarnt wird, dass die Verbindung getrennt wurde.
root/ConnectionType/freerdp/connections/<UUID>/timeoutWarningDialog	Wenn der Wert 1 ist, dann wird ein Dialogfeld angezeigt, wenn ein Abfallen einer Ende-zu-Ende-Verbindung erkannt wird, und das Display wird grau. Andernfalls werden Nachrichten in das Verbindungsprotokoll geschrieben und die Sitzung fährt sich fest.
root/ConnectionType/freerdp/connections/<UUID>/timeoutsEnabled	Wenn der Wert 1 ist, dann sind die Health-Tests der Ende-zu-Ende-Verbindung abgeschlossen.
root/ConnectionType/freerdp/connections/<UUID>/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. Wenn der Wert 2 ist, dann werden alle anderen USB-Geräte zum Remote-Host umgeleitet, wie im USB-Manager konfiguriert.
root/ConnectionType/freerdp/connections/<UUID>/usbStorageRedirection	Wenn der Wert 1 ist, werden alle USB-Speichergeräte über die `Storage`-Erweiterung zum Remote-Host weitergeleitet werden. Durch die Einstellung 0 wird die Erweiterung deaktiviert. Durch die Einstellung 2 werden USB-Speichergeräte entsprechend der Angaben im USB-Manager weitergeleitet.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/freerdp/connections/<UUID>/username	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/freerdp/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/freerdp/connections/<UUID>/windowMode	Bei einer Einstellung auf `Remote Application` wird RDP im Remote Application Integrated Local (RAIL) ausgeführt. Dies erfordert, dass der RemoteApp-Server die gewünschte Anwendung als Remoteanwendung ausführen kann. Die Anwendung wird in einem separaten Fenster innerhalb der Desktop-Umgebung angezeigt, sodass es wirkt, als wäre die Anwendung Teil des lokalen Systems. Siehe auch den Registrierungsschlüssel `RemoteApp`. Bei einer Einstellung auf `Alternate Shell` wird eine nicht-standardmäßige Shell aufgerufen. Siehe auch die Registrierungsschlüssel `application` und `directory`.
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	Legt eine XKB-Layout-ID für die Umgehung der Systemtastatur fest. Um Zugriff auf die Liste der verfügbaren IDs zu erhalten, geben Sie Folgendes in ein X-Terminal ein: `xfreerdp --kbd-list`.
root/ConnectionType/freerdp/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/freerdp/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning	Wenn der Wert 1 ist, generiert das Betriebssystem keinen Dialog, der angibt, dass das Netzwerk ausgefallen ist, da das Verbindungsprotokoll solche Situationen bearbeitet.
root/ConnectionType/freerdp/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen

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

Registrierungsschlüssel	Beschreibung
	Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/freerdp/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/freerdp/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/freerdp/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	Legt die Anzahl der Sekunden fest, die gewartet werden, um eine erste Reaktion vom RDP-Server zu erhalten, bis der Versuch aufgegeben wird.
root/ConnectionType/freerdp/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.
root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/freerdp/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/freerdp/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen `AppName` angegebene Verbindung überwacht. 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 bedient. 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. Wenn der Wert 0 ist, warten die Dialogen unbegrenzt auf eine Benutzerinteraktion.
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. Wenn diese Taste auf 1 eingestellt ist, werden die Schaltfläche und das Dialogfeld nicht angezeigt.
root/ConnectionType/freerdp/general/enableMMR	Bei Einstellung des Werts auf 1 wird die `Multimedia Redirection` aktiviert, sodass unterstützte Codecs, die über

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

Registrierungsschlüssel	Beschreibung
	den Windows Media Player abgespielt werden, an den Client umgeleitet werden. Dies verbessert erheblich die Videowiedergabe im Vollbild- und High-Definition-Modus für Codecs wie z. B. WMV9, VC1 und MPEG4.
root/ConnectionType/freerdp/general/preferredAudio	Legt das Standard-Audio-Backend für High-Level-Audio-Umleitung (sowohl Ein- als auch Ausgang) fest.
root/ConnectionType/freerdp/general/rdWebFeedUrlPattern	Legt das Muster fest, das verwendet wird, um die RD Web-Access-URL zu erstellen. Der Host der URL wird durch den Wert im Feld **Address** (Adresse) der Verbindung ersetzt. Dieses Muster wird nicht verwendet, wenn die Adresse bereits eine URL ist.
root/ConnectionType/freerdp/general/sendHostname	Wenn der `hostname` eingestellt ist, wird der System-Hostname an den Remote-Host gesendet. Dies wird in der Regel verwendet, um den mit einer bestimmten RDP-Sitzung verknüpften Thin Client zu identifizieren. Der gesendete Host-Name kann mit `sendHostname` in den verbindungsspezifischen Einstellungen außer Kraft gesetzt werden. Bei der Einstellung `mac` wird die MAC-Adresse des ersten verfügbaren Netzwerkadapters anstelle des Hostnamen gesendet.
root/ConnectionType/freerdp/general/serialPortsDriver	Diese Einstellung sorgt für eine bessere Kompatibilität mit der erwarteten zugrunde liegenden Windowstreiber SerCx2.sys, SerCx.sys oder Serial.sys.
root/ConnectionType/freerdp/general/serialPortsPermissive	Wenn der Wert 1 ist, dann werden Fehler für nicht unterstützte Funktionen ignoriert.

root > ConnectionType > ssh

Tabelle E-7 root > ConnectionType > ssh

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/authorizations/user/add	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/ssh/authorizations/user/general	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/ssh/connections/<UUID>/address	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll.
root/ConnectionType/ssh/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/ssh/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen 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	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/ssh/connections/<UUID>/autoReconnect	Bei Einstellung auf den Wert 1 wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/ssh/connections/<UUID>/autoReconnectDelay	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn `autoReconnect` auf 1 eingestellt ist.
root/ConnectionType/ssh/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/ssh/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/ssh/connections/<UUID>/backgroundColor	Gibt die Hintergrundfarbe der Verbindung an.
root/ConnectionType/ssh/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der 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 Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/ssh/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/ssh/connections/<UUID>/font	Gibt die Schriftgröße für die Verbindung an.
root/ConnectionType/ssh/connections/<UUID>/foregroundColor	Gibt die Vordergrundfarbe der Verbindung an.
root/ConnectionType/ssh/connections/<UUID>/fork	Wenn die Auswahl 1 ist, dann ist die Option **Fork into background** (Prozess in den Hintergrund verschieben) für die Verbindung aktiviert.
root/ConnectionType/ssh/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf `Default Connection` eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/ssh/connections/<UUID>/port	Gibt die Portnummer an, die bei der Verbindungsherstellung mit dem SSH-Server verwendet wird. Die Standardeinstellung ist 22.
root/ConnectionType/ssh/connections/<UUID>/startMode	Wenn die Standardeinstellung `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	Wenn die Auswahl 1 ist, dann ist die Option **Force TTY allocation** (Force TTY-Zuordnung) ür die Verbindung aktiviert ist.
root/ConnectionType/ssh/connections/<UUID>/username	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/ssh/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/ssh/connections/<UUID>/x11	Wenn der Wert 1 ist, dann ist die Option **X11 connection forwarding** (X11 Verbindungsweiterleitung) für die Verbindung aktiviert.
root/ConnectionType/ssh/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/ssh/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/ssh/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/ssh/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/ssh/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/ssh/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp ist.
root/ConnectionType/ssh/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/ssh/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen `AppName` angegebene Verbindung überwacht. 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 bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/ssh/gui/SshManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/gui/SshManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/gui/SshManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/ssh/gui/SshManager/widgets/address	Steuert den Status des Widgets **Address** (Adresse) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Run application** (Ausführung der Anwendung) im Verbindungsmanager für diesen Verbindungstyp. 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-7 root > ConnectionType > ssh (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect	Steuert den Status des Widgets **Auto reconnect** (Automatisches Neuverbinden) im Verbindungsmanager für diesen Verbindungstyp. 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/autostart	Steuert den Status des Widgets **Auto start priority** (Automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Background color** (Hintergrundfarbe) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Compression** (Komprimierung) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Fallback Connection** (Ausweichverbindung) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Font** (Schriftart) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Foreground color** (Vordergrundfarbe) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Fork into background** (Prozess in Hintergrund verschieben) im Verbindungsmanager für diesen Verbindungstyp. Durch die Einstellung active wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit

Tabelle E-7 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/hasDesktopIcon`	Steuert den Status des Widgets **Show icon on desktop** (Symbol auf Desktop zeigen) im Verbindungsmanager für diesen Verbindungstyp. 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 Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/ssh/gui/SshManager/widgets/label`	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Port** (Anschluss) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Force TTY allocation** (TTY-Zuordnung-erzwingen) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **User name** (Benutzername) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Wait for network before connecting** (Vor dem Verbinden auf Netzwerk warten) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **X11 connection forwarding** (X11 Verbindungsweiterleitung) im Verbindungsmanager für diesen Verbindungstyp. 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 > ssh (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Widget ausgeblendet. Durch die Einstellung `read-only` wird das Widget im schreibgeschützten Modus angezeigt.

root > ConnectionType > teemtalk

Tabelle E-8 root > ConnectionType > teemtalk

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

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/teemtalk/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/teemtalk/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf `Default Connection` eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
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	Wenn der Wert 1 ist, dann sind Systemsignale für die Verbindung aktiviert.
root/ConnectionType/teemtalk/connections/<UUID>/ttsName	Gibt den TeemTalk-Profilnamen an.
root/ConnectionType/teemtalk/connections/<UUID>/waitForNetwork	Bei Einstellung des Werts auf 1 wird die Verbindung erst gestartet, wenn der Netzwerkbetrieb verfügbar ist. Dies stellt sicher, dass auf einem langsamen Netzwerk die Verbindung nicht gestartet wird, bevor der Netzwerkbetrieb verfügbar ist, was ansonsten einen Fehler verursachen würde.
root/ConnectionType/teemtalk/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/teemtalk/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/teemtalk/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/teemtalk/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/teemtalk/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/teemtalk/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.
root/ConnectionType/teemtalk/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/teemtalk/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp 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	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/gui/TeemtalkManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/gui/TeemtalkManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/autoReconnect	Steuert den Status des Widgets **Auto reconnect** (Automatisches Neuverbinden) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Auto start priority** (Automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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/hasDesktopIcon	Steuert den Status des Widgets **Show icon on desktop** (Symbol auf Desktop zeigen) im Verbindungsmanager für diesen

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

Registrierungsschlüssel	Beschreibung
	Verbindungstyp. 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 Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/teemtalk/gui/TeemtalkManager/widgets/label`	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Wait for network before connecting** (Vor dem Verbinden auf Netzwerk warten) im Verbindungsmanager für diesen Verbindungstyp. 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

Tabelle E-9 root > ConnectionType > telnet

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

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/telnet/connections/<UUID>/backgroundColor	Gibt die Hintergrundfarbe der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/telnet/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/telnet/connections/<UUID>/font	Gibt die Schriftgröße für die Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/foregroundColor	Gibt die Vordergrundfarbe der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/telnet/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf `Default Connection` eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/telnet/connections/<UUID>/locale	Gibt das Gebietsschema der Verbindung an.
root/ConnectionType/telnet/connections/<UUID>/port	Gibt die Portnummer an, die bei der Verbindungsherstellung mit dem Server verwendet wird. Die Standardeinstellung ist 23.
root/ConnectionType/telnet/connections/<UUID>/startMode	Wenn die Standardeinstellung `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.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/telnet/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/telnet/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/telnet/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/telnet/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/telnet/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.
root/ConnectionType/telnet/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/telnet/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp 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.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/gui/TelnetManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/gui/TelnetManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/gui/TelnetManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/telnet/gui/TelnetManager/widgets/address	Steuert den Status des Widgets **Address** (Adresse) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Auto reconnect** (Automatisches Neuverbinden) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Auto start priority** (Automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Background color** (Hintergrundfarbe) im Verbindungsmanager für diesen Verbindungstyp. 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/fallBackConnection	Steuert den Status des Widgets **Fallback Connection** (Ausweichverbindung) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Foreground color** (Vordergrundfarbe) im Verbindungsmanager für diesen Verbindungstyp. 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-9 root > ConnectionType > telnet (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon	Steuert den Status des Widgets **Show icon on desktop** (Symbol auf Desktop zeigen) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Port** (Anschluss) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Wait for network before connecting** (Vor dem Verbinden auf Netzwerk warten) im Verbindungsmanager für diesen Verbindungstyp. 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

Tabelle E-10 root > ConnectionType > view

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/authorizations/user/add	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/view/authorizations/user/general	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/view/connections/<UUID>/ExtraArgs	Gibt zusätzliche Argumente zum VMware Horizon View-Client an. Führen Sie view_client --help oder vmware-wiew --help über ein X-Terminal aus, um alle verfügbaren Argumente anzuzeigen.
root/ConnectionType/view/connections/<UUID>/SingleSignOn	
root/ConnectionType/view/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.

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

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

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/view/connections/<UUID>/desktop	Wenn angegeben, wird der benannte Desktop beim Anmelden automatisch gestartet. Standardmäßig wird, wenn nur ein Desktop verfügbar ist, dieser Desktop automatisch gestartet, ohne dass er angegeben werden muss.
root/ConnectionType/view/connections/<UUID>/desktopSize	Legt die Größe fest, in der der VMware Horizon View-Client den Desktop startet.
root/ConnectionType/view/connections/<UUID>/directory	
root/ConnectionType/view/connections/<UUID>/disableMaximizedApp	Wenn der Wert 1 ist, dann sind die Einstellungen für die Fenstergröße bei maximierten Anwendungen deaktiviert.
root/ConnectionType/view/connections/<UUID>/domain	Legt die Domäne fest, die dem View Connection Server zur Verfügung gestellt wird. Wenn keine Domäne angegeben ist, wird die Standarddomäne für den Server verwendet.
root/ConnectionType/view/connections/<UUID>/enableSingleMode	
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/view/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.
root/ConnectionType/view/connections/<UUID>/fullscreen	Wenn der Wert 1 ist, dann startet der VMware Horizon View-Client im Vollbildmodus, wenn er gestartet wird.
root/ConnectionType/view/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/view/connections/<UUID>/hideMenuBar	Bei Einstellung des Werts auf 1 wird die obere Menüleiste innerhalb des Desktops ausgeblendet. Diese Leiste wird zur Verwaltung von Remote-Geräten und zum Starten anderer Desktops verwendet.
root/ConnectionType/view/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/view/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf `Default Connection` eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/view/connections/<UUID>/lockServer	Wenn der Wert 1 ist, dann können Standardbenutzer die Serveradresse nicht ändern.
root/ConnectionType/view/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld **Domain** (Domäne) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/password	Wenn der Wert 1 ist, wird das Feld **Password** (Kennwort) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist,

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

Registrierungsschlüssel	Beschreibung
	wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen **Remember me** (Anmeldedaten merken) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/showpassword	Wenn der Wert 1 ist, wird die Schaltfläche **Show password** (Kennwort anzeigen) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird die Schaltfläche angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird die Schaltfläche ausgeblendet.
root/ConnectionType/view/connections/<UUID>/loginfields/smartcard	Wenn der Wert 1 ist, wird das Kontrollkästchen **Smart card login** (Smart Card-Anmeldung) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet. Dieses Kontrollkästchen wird möglicherweise nicht angezeigt, wenn keine Smart Card erkannt wird, auch wenn diese Option aktiviert ist.
root/ConnectionType/view/connections/<UUID>/loginfields/username	Wenn der Wert 1 ist, wird das Feld **User Name** (Benutzername) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/view/connections/<UUID>/password	Legt das Standardkennwort fest, das der Remote-Host während der Anmeldung benötigt. Dieser Wert ist normalerweise verschlüsselt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/view/connections/<UUID>/saveCredentials	
root/ConnectionType/view/connections/<UUID>/server	Die Adresse des Remote-Hosts, zu dem die Verbindung hergestellt werden soll. In der Regel ist dies eine URL, wie z. B. `http://server.domain.com`.
root/ConnectionType/view/connections/<UUID>/sessionEndAction	
root/ConnectionType/view/connections/<UUID>/singleDesktop	
root/ConnectionType/view/connections/<UUID>/smartcard	Wenn der Wert 1 ist, dann werden hierdurch alle lokal angeschlossenen Smart Cards an den Remote-Host weitergeleitet, damit sie von Anwendungen auf dem Remote-Host verwendet werden können. Dies ermöglicht nur Smart Card-Anmeldungen für den Remote-Host, nicht für View Connection Server.
root/ConnectionType/view/connections/<UUID>/startMode	Wenn die Standardeinstellung `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/view/connections/<UUID>/username	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.

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

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

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo	Dieser Wert ist der Lastenausgleich-Cookie, der zu Vermittlungszwecken beim Herstellen einer Verbindung an den Server gesendet wird und entspricht dem Feld Loadbalanceinfo in der Datei .rdp. Der Standardwert ist leer.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents	Bei Einstellung des Werts auf 0 werden Mausbewegungsereignisse nicht an den Server gesendet. Dies kann dazu führen, dass einige Benutzerfeedbacks, wie z. B. Quickinfos, nicht richtig funktionieren.
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. Das Ausschalten der Desktopgestaltung kann die Leistung für Verbindungen mit niedriger Bandbreite verbessern. Im Allgemeinen betrifft dies nur RemoteFX. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagFontSmoothing	Die Einstellung des Werts 1 ermöglicht eine Schriftglättung, wenn dies vom Server unterstützt wird und aktiviert ist. Das Ausschalten dieser Option kann die Leistung bei Verbindungen mit niedriger Bandbreite verbessern. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/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. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorShadow	Die Einstellung des Werts 1 schaltet den Mauscursor-Schatten aus, wodurch die Leistung bei RDP-Verbindungen mit niedriger Bandbreite verbessert werden kann. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
root/ConnectionType/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. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
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. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
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. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.
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. Wenn 2 eingestellt ist, dann wird der Wert basierend auf der Thin Client-Leistung ausgewählt.

Tabelle E-10 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	Wenn der Wert 1 ist, werden alle lokal über CUPS definierten Drucker zum Remote-Host weitergeleitet.
root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering	Wenn der Wert 1 ist, wird die Nicht-RemoteFX-Grafikleistung über weniger häufige Bildschirmaktualisierungen erhöht.
root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs	Wenn der Wert 1 ist, werden RDP 8-Codecs verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der RDP 8-Codecs deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
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/freerdp/connections/<UUID>/rdpH264Codec	Wenn der Wert 1 ist, werden RDP 8 H.264-Codecs verwendet, wenn verfügbar. Für diese Einstellung gibt es bekannte visuelle Fehler, insbesondere bei Konfigurationen mit mehreren Monitoren, daher sollte sie als experimentell und nicht unterstützt betrachtet werden. Durch Aktivieren dieser Einstellung wird einfach der Server darauf hingewiesen, dass der Thin Client H.264 für die Desktopanzeige unterstützt. Der Server muss auch H.264 unterstützen und der Server trifft die endgültige Entscheidung darüber, welche Codecs verwendet werden. Diese Einstellung wirkt sich nur auf die Desktop-Codecs aus. Codecs für die Multimedia-Umleitung sind davon nicht betroffen.
root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec	Wenn der Wert 1 ist, werden progressive RDP 8-Codecs verwendet, wenn verfügbar. Diese Einstellung sollte nur bei einem Fehler der progressiven RDP 8-Codecs deaktiviert werden. Durch das Deaktivieren dieser Einstellung können auch erweiterte Codecs deaktiviert werden.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/remoteFx	Wenn der Wert 1 ist, dann wird RemoteFX verwendet, wenn verfügbar.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/securityLevel	Legt die Sicherheitsstufen von Zertifikaten fest. Wenn der Wert 0 ist, sind alle Verbindungen zulässig. Wenn der Wert 1 ist, werden beibehaltene Hosts überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 2 ist, werden beibehaltene Hosts nicht überprüft und eine Warnung wird angezeigt, sofern die Überprüfung nicht erfolgreich ist. Wenn der Wert 3 ist, werden alle unsichere Verbindungen verweigert.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sendHostname	Legt den Thin Client-Hostnamen fest, der an den Remote-Host gesendet wird. Wenn keine Eintragung vorgenommen wird, wird der System-Host-Namen gesendet. Der Registrierungsschlüssel root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname muss auf den hostname eingestellt sein, damit diese Taste verwendet werden kann.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sound	Durch die Standardeinstellung Bring to this computer wird der Sound mithilfe eines virtuellen Kanals vom Remote-Host zum Client umgeleitet. Durch die Einstellung Leave at remote computer verbleibt der Sound am Remote-Host. Dies kann nützlich sein, wenn ein USB-umgeleitetes Audiogerät verwendet wird. Durch die Einstellung auf irgendeinen anderen

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

Registrierungsschlüssel	Beschreibung
	Wert, wird Audio deaktiviert. In der Regel empfiehlt HP, den Wert `Bring to this computer` einzustellen und USB-Wiedergabegeräte nicht zum Remote-Host umzuleiten. Dadurch wird die Audioqualität verbessert und sichergestellt, dass Client-Audio, das mittels anderer Methoden umgeleitet wird (wie zum Beispiel `Multimedia Redirection`), den lokalen Audioeinstellungen entspricht.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/xkbLayoutId`	Legt eine XKB-Layout-ID für die Umgehung der Systemtastatur fest. Um Zugriff auf die Liste der verfügbaren IDs zu erhalten, geben Sie Folgendes in ein X-Terminal ein: `xfreerdp --kbd-list`.
`root/ConnectionType/view/coreSettings/USBrelevant`	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
`root/ConnectionType/view/coreSettings/appName`	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/view/coreSettings/className`	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/view/coreSettings/editor`	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
`root/ConnectionType/view/coreSettings/icon16Path`	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
`root/ConnectionType/view/coreSettings/icon32Path`	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
`root/ConnectionType/view/coreSettings/icon48Path`	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
`root/ConnectionType/view/coreSettings/label`	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.
`root/ConnectionType/view/coreSettings/priorityInConnectionLists`	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
`root/ConnectionType/view/coreSettings/serverRequired`	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp 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

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

Registrierungsschlüssel	Beschreibung
	`wrapperScript`, mit dem Argument `stop` ausgeführt, um den Prozess ordnungsgemäß zu beenden.
`root/ConnectionType/view/coreSettings/watchPid`	Wenn der Wert 1 ist, wird die unter dem Namen `AppName` angegebene Verbindung überwacht. 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 wird. Um eine vollständige Liste der Optionen anzuzeigen, geben Sie den folgenden Befehl in ein X-Terminal ein: `rdesktop --help`
`root/ConnectionType/view/gui/viewManager/name`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/view/gui/viewManager/status`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/view/gui/viewManager/title`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/view/gui/viewManager/widgets/autostart`	Steuert den Status des Widgets **Auto start priority** (Automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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/gui/viewManager/widgets/fallBackConnection`	Steuert den Status des Widgets **Fallback Connection** (Ausweichverbindung) im Verbindungsmanager für diesen Verbindungstyp. 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/gui/viewManager/widgets/label`	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. 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

Tabelle E-11 root > ConnectionType > xdmcp

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/authorizations/user/add	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/xdmcp/authorizations/user/general	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/address	Legt den Hostnamen bzw. die IP-Adresse fest, zu der die Verbindung aufgebaut werden soll.
root/ConnectionType/xdmcp/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/xdmcp/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/edit	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/xdmcp/connections/<UUID>/autoReconnect	Bei Einstellung auf den Wert 1 wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
root/ConnectionType/xdmcp/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/xdmcp/connections/<UUID>/beforeStartingCommand	Gibt den Befehl an, der vor dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/xdmcp/connections/<UUID>/color	Legt die Farbtiefe für die Anzeige der Verbindung fest.
root/ConnectionType/xdmcp/connections/<UUID>/connectionEndAction	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/coord	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/dependConnectionId	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/key	Legt den Namen einer zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung fest.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/value	Gibt den Wert der zusätzlichen Umgebungsvariable für die Verwendung mit der Verbindung an.
root/ConnectionType/xdmcp/connections/<UUID>/fallBackConnection	Legt die alternative Verbindung über seine UUID fest.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/connections/<UUID>/fontServer	Legt die Adresse des zu verwendenden Font-Servers fest. Der Registrierungsschlüssel UseFontServer muss auch auf 1 eingestellt werden.
root/ConnectionType/xdmcp/connections/<UUID>/hasDesktopIcon	Wenn der Wert 1 ist, ist das Desktop-Symbol für diese Verbindung aktiviert. Diese Taste hat keine Auswirkungen auf Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/connections/<UUID>/label	Legt den Verbindungsnamen fest, der in der Benutzeroberfläche angezeigt wird. Für Smart Zero ist dies normalerweise auf Default Connection eingestellt und wird in der Benutzeroberfläche nicht angezeigt.
root/ConnectionType/xdmcp/connections/<UUID>/refreshRate	Legt die Bildwiederholungsrate für das Display der Verbindung fest.
root/ConnectionType/xdmcp/connections/<UUID>/startMode	Wenn die Standardeinstellung 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/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 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/xdmcp/connections/<UUID>/windowSize	Gibt die Fenstergröße für die Verbindung an.
root/ConnectionType/xdmcp/coreSettings/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/xdmcp/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/coreSettings/audio	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/coreSettings/desktopButton	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/xdmcp/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/xdmcp/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/xdmcp/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.
root/ConnectionType/xdmcp/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/xdmcp/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp ist.
root/ConnectionType/xdmcp/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/xdmcp/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen `AppName` angegebene Verbindung überwacht. 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 bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xdmcp/gui/XdmcpManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

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

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xdmcp/gui/XdmcpManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/gui/XdmcpManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/address	Steuert den Status des Widgets **Address** (Adresse) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Auto reconnect** (Automatisches Neuverbinden) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Auto start priority** (Automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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 Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/fontServer	Steuert den Status des Widgets **Font server** (Font-Server) im Verbindungsmanager für diesen Verbindungstyp. 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	Steuert den Status des Widgets **Show icon on desktop** (Symbol auf Desktop zeigen) im Verbindungsmanager für diesen Verbindungstyp. 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 Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/label	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. Durch die Einstellung `active` wird das Widget in der Benutzeroberfläche angezeigt und der Benutzer kann mit ihm interagieren. Durch die Einstellung `inactive` wird

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

Registrierungsschlüssel	Beschreibung
	das Widget ausgeblendet. Durch die Einstellung `read-only` wird das Widget im schreibgeschützten Modus angezeigt.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/refreshRate`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/type`	Steuert den Status des Widgets **Type** (Typ) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Use font server** (Font-Server verwenden) im Verbindungsmanager für diesen Verbindungstyp. 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`	Steuert den Status des Widgets **Wait for network before connecting** (Vor dem Verbinden auf Netzwerk warten) im Verbindungsmanager für diesen Verbindungstyp. 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 Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

root > ConnectionType > xen

Tabelle E-12 root > ConnectionType > xen

Registrierungsschlüssel	Beschreibung
`root/ConnectionType/xen/authorizations/user/add`	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Hinzufügen einer neuen Verbindung dieses Typs über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
`root/ConnectionType/xen/authorizations/user/general`	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der allgemeinen Einstellungen für diesen Verbindungstyp über den Verbindungsmanager. Diese Taste hat keine Auswirkungen auf Smart Zero.
`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`.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/connections/<UUID>/afterStartedCommand	Gibt den Befehl an, der nach dem Starten der Verbindung ausgeführt werden soll.
root/ConnectionType/xen/connections/<UUID>/afterStoppedCommand	Gibt den Befehl an, der nach dem Unterbrechen der Verbindung ausgeführt werden soll.
root/ConnectionType/xen/connections/<UUID>/anonymousLogin	Wenn der Wert 1 ist, dann ist eine anonyme Anmeldung für PNAgent und direkte Verbindungen zulässig.
root/ConnectionType/xen/connections/<UUID>/appInMenu	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung im Menü der Taskleiste angezeigt.
root/ConnectionType/xen/connections/<UUID>/appOnDashboard	Bei Einstellung des Werts auf 1 werden alle Anwendungen für diese Verbindung in der Taskleiste 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	Wenn der Wert 1 ist, dann hat der Standardbenutzer die Berechtigung zum Ändern der Verbindungseinstellungen für diese Verbindung.
root/ConnectionType/xen/connections/<UUID>/authorizations/user/execution	Wenn der Wert 1 ist, dann hat ein Standardbenutzer die Berechtigung zum Ausführen dieser Verbindung.
root/ConnectionType/xen/connections/<UUID>/autoLaunchSingleApp	Wenn der Wert 1 ist und wenn nur eine einzige veröffentlichte Anwendung oder Desktop vom Citrix-Server zurückgegeben wird, wird diese Ressource automatisch gestartet.
root/ConnectionType/xen/connections/<UUID>/autoReconnect	Bei Einstellung auf den Wert 1 wird die Verbindung neu gestartet, wenn sie beendet oder getrennt wurde.
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	Legt die Wartezeit in Sekunden fest, bevor die Verbindung neu gestartet wird. Beim Standardwert 0 wird die Verbindung sofort neu gestartet. Diese Einstellung wird nur wirksam, wenn `autoReconnect` auf 1 eingestellt ist.
root/ConnectionType/xen/connections/<UUID>/autoRefreshInterval	Steuert die Zeit in Sekunden, bevor die Ressourcen gelöscht und vom Server erneut aktualisiert werden. Stellen Sie zum Deaktivieren den Wert -1 ein. Es ist in der Regel nicht erforderlich, die Ressourcen häufig vom Server zu aktualisieren.
root/ConnectionType/xen/connections/<UUID>/autoStartDesktop	Wenn der Wert 1 ist, dann wird der erste Desktop, der zur Verfügung steht, wenn die Verbindung gestartet wird, automatisch geöffnet.
root/ConnectionType/xen/connections/<UUID>/autoStartResource	Legt den Namen des Desktops oder der Anwendung fest, der oder die automatisch startet, wenn die Verbindung gestartet wird.
root/ConnectionType/xen/connections/<UUID>/autostart	Wenn der Wert zwischen 1 und 5 liegt, dann wird die Verbindung automatisch nach dem Systemstart gestartet, wobei der Wert 1 die höchste Priorität hat.
root/ConnectionType/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.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

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

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/connections/<UUID>/loginfields/domain	Wenn der Wert 1 ist, wird das Feld **Domain** (Domäne) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/password	Wenn der Wert 1 ist, wird das Feld **Password** (Kennwort) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/rememberme	Wenn der Wert 1 ist, wird das Kontrollkästchen **Remember me** (Anmeldedaten merken) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/showpassword	Wenn der Wert 1 ist, wird die Schaltfläche **Show password** (Kennwort anzeigen) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird die Schaltfläche angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird die Schaltfläche ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/loginfields/smartcard	Wenn der Wert 1 ist, wird das Kontrollkästchen **Smart card login** (Smart Card-Anmeldung) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Kontrollkästchen angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Kontrollkästchen ausgeblendet. Dieses Kontrollkästchen wird möglicherweise nicht angezeigt, wenn keine Smart Card erkannt wird, auch wenn diese Option aktiviert ist.
root/ConnectionType/xen/connections/<UUID>/loginfields/username	Wenn der Wert 1 ist, wird das Feld **User Name** (Benutzername) im Anmeldedialog für die Verbindung angezeigt. Wenn der Wert 2 ist, wird das Feld angezeigt, ist aber deaktiviert. Wenn der Wert 0 ist, wird das Feld ausgeblendet.
root/ConnectionType/xen/connections/<UUID>/password	Legt das Standardkennwort fest, das der Remote-Host während der Anmeldung benötigt. Dieser Wert ist normalerweise verschlüsselt. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeines Kennwort für die Anmeldung benutzt wird.
root/ConnectionType/xen/connections/<UUID>/requireCredentialsDirectConnect	Wenn der Wert 0 ist, dann werden Anmeldeinformationen nicht benötigt, um eine direkte Verbindung zu initiieren. Jedoch sind Anmeldeinformationen benötigt, um eine Anwendung zu starten.
root/ConnectionType/xen/connections/<UUID>/savePassword	
root/ConnectionType/xen/connections/<UUID>/smartCardModuleKey	Gibt das Sicherheitsmodul an, das für eine Smart Card-Verbindung verwendet werden soll.
root/ConnectionType/xen/connections/<UUID>/startMode	Wenn die Standardeinstellung `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/xen/connections/<UUID>/unplugSmartCardAction	Legt die Aktion fest, die durchgeführt werden soll, wenn eine Smart Card während einer Verbindung ausgesteckt wird. Mit `logoff` wird die aktuelle Sitzung abgemeldet. Mit `close` werden alle geöffneten Ressourcen geschlossen. Mit `noaction` wird keine Aktion ausgeführt.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/connections/<UUID>/username	Legt den Standard-Benutzernamen fest, der vom Remote-Host während der Anmeldung benötigt wird. Im Allgemeinen wird diese Einstellung für Anwendungen im Kiosk-Stil verwendet, bei denen ein allgemeiner Benutzername für die Anmeldung benutzt wird.
root/ConnectionType/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/USBrelevant	Gibt an, ob dieser Verbindungstyp für USB relevant ist. Falls ja, ist möglicherweise ein USB-Plug-In für die Umleitung von USB-Geräten verfügbar.
root/ConnectionType/xen/coreSettings/appName	Legt den internen Namen der Anwendung fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch	Diese Einstellung gilt für Citrix-Server mit mehreren veröffentlichten Ressourcen. Bei einem Wert unter 0 wird keine automatische Abmeldung ausgeführt. Andernfalls legt diese Einstellung die Anzahl der Sekunden festgelegt, die zur Verfügung stehen zwischen dem Schließen der letzten von Xen veröffentlichten Ressource und dem automatischen Abmelden des Benutzers und Zurückkehren zum Anmeldebildschirm. Citrix-Prozessverzögerungen können die Zeit bis zur automatischen Abmeldung verlängern.
root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch	Diese Einstellung gilt für Citrix-Server mit mehreren veröffentlichten Ressourcen. Bei einem Wert unter 0 wird keine automatische Abmeldung ausgeführt. Andernfalls legt diese Einstellung die Anzahl der Sekunden festgelegt, die ohne das Starten neuer Anwendungen vergehen bis zum automatischen Abmelden des Benutzers und Zurückkehren zum Anmeldebildschirm. Citrix-Prozessverzögerungen können die Zeit bis zur automatischen Abmeldung verlängern.
root/ConnectionType/xen/coreSettings/className	Legt den internen Klassennamen fest, der für diesen Verbindungstyp verwendet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/editor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Verbindungsmanager für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/generalSettingsEditor	Legt den internen Namen der Anwendung fest, der verwendet wird, wenn der Manager für Allgemeine Einstellungen für diesen Verbindungstyp gestartet wird. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/icon16Path	Legt den Pfad auf das Symbol mit 16 x 16 Pixel für diese Anwendung fest.
root/ConnectionType/xen/coreSettings/icon32Path	Legt den Pfad auf das Symbol mit 32 x 32 Pixel für diese Anwendung fest.
root/ConnectionType/xen/coreSettings/icon48Path	Legt den Pfad auf das Symbol mit 48 x 48 Pixel für diese Anwendung fest.
root/ConnectionType/xen/coreSettings/label	Legt den Namen fest, der für diesen Verbindungstyp im Auswahlmenü der Verbindungstypen angezeigt wird.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/coreSettings/priorityInConnectionLists	Legt die Priorität für diesen Verbindungstyp fest, wenn diese im Verbindungsmanager angezeigt wird und für den Konfigurationsassistenten, der während der Erstinstallation angezeigt wird. Ein höherer Wert bewegt den Verbindungstyp in der Liste nach oben. Wenn der Wert auf 0 gesetzt ist, dann ist der Verbindungstyp im Konfigurationsassistenten nicht sichtbar ist und wird als letzter im Verbindungsmanager angezeigt. Typen der Verbindungen mit derselben Priorität sind in alphabetischer Reihenfolge aufgeführt.
root/ConnectionType/xen/coreSettings/serverRequired	Legt fest, ob ein Servername oder eine Adresse `unused`, `optional` oder `required` für diesen Verbindungstyp 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 ordnungsgemäß zu beenden.
root/ConnectionType/xen/coreSettings/watchPid	Wenn der Wert 1 ist, wird die unter dem Namen `AppName` angegebene Verbindung überwacht. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/coreSettings/wrapperScript	Der Name des Skripts oder der Binärdatei, das bzw. die beim Starten dieses Verbindungstyps ausgeführt werden soll. Dies ist das primäre Skript, das alle Verbindungseinstellungen und Befehlszeilenargumente für die Verbindung bedient. Dieser Schlüssel sollte keine Änderung erfordern.
root/ConnectionType/xen/general/TWIMode	Steuert den nahtlosen Modus für veröffentlichte Anwendungen. Diese Einstellung ist der Citrix INI-Dateieinstellung `TWIMode` direkt zugeordnet.
root/ConnectionType/xen/general/TWIModeResizeType	Diese Einstellung ist der Citrix INI-Dateieinstellung `TWIMoveResizeType` direkt zugeordnet.
root/ConnectionType/xen/general/allowReadOn<AthruZ>	Wenn der Wert 1 ist, kann ein Benutzer das zugeordnete Laufwerk lesen.
root/ConnectionType/xen/general/allowWriteOn<AthruZ>	Wenn der Wert 1 ist, kann ein Benutzer im zugeordneten Laufwerk auch schreiben.
root/ConnectionType/xen/general/async	Wenn der Wert 1 ist, ist die asynchrone Abfrage aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung `CommPollSize` direkt zugeordnet.
root/ConnectionType/xen/general/autoReconnect	Bei Einstellung des Werts auf 1 ist das automatische Neuverbinden der Sitzung aktiviert. Dies ist nicht identisch mit dem verbindungsspezifischen "autoReconnect" (automatisches Neuverbinden). Diese Neuverbindung findet intern statt, innerhalb des Citrix-Clients, ohne Neustart der Verbindung. Diese Einstellung ist der Citrix INI-Dateieinstellung `TransportReconnectEnabled` direkt zugeordnet.
root/ConnectionType/xen/general/bitmapCacheSize	Legt die minimale Größe für die Bitmap-Zwischenspeicherung fest. Diese Einstellung ist der Citrix INI-Dateieinstellung `PersistentCacheMinBitmap` direkt zugeordnet.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/bottomMonitor	Legt fest, dass auf dem Bildschirmbereich des unteren Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/colorDepth	Erzwingt die Verwendung einer bestimmten Farbtiefe für alle Verbindungen. Dies erfolgt in der Regel entweder in speziellen Umgebungen, in denen die automatische Tiefenauswahl fehlschlägt, oder in sehr langsam Netzwerken, um eine Überlastung zu vermeiden.
root/ConnectionType/xen/general/colorMapping	Bei der Auswahl von `Shared - Approximate Colors` werden ungefähre Farben aus der Standard-Farbzuordnungstabelle verwendet. Bei der Auswahl von `Private - Exact Colors` werden präzise Farben verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung `ApproximateColors` direkt zugeordnet.
root/ConnectionType/xen/general/contentRedirection	Wenn der Wert 1 ist, dann werden Links von Web-Inhalten vom Server an den Client gesendet, so dass der Client versuchen kann, sie lokal zu öffnen.
root/ConnectionType/xen/general/defaultBrowserProtocol	Steuert das Protokoll, das verwendet wird, um den Host für die Verbindung zu finden. Wenn kein Wert angegeben wird, wird der Standardwert vom Abschnitt `[WFClient]` der wfclient.ini verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung `BrowserProtocol` direkt zugeordnet.
root/ConnectionType/xen/general/drivePathMappedOn<AthruZ>	Legt das Verzeichnis des lokalen Dateisystems zur Zuordnung zum Remote-Host fest. 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	Wenn der Wert 1 ist, sind Windows-Warntöne aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung `DisableSound` direkt zugeordnet.
root/ConnectionType/xen/general/enableClipboard	Wenn der Wert 1 ist, wird die Umleitung der Zwischenablage aktiviert.
root/ConnectionType/xen/general/enableCursorColors	Bei Einstellung des Werts auf 1 werden farbige Cursor aktiviert. Bei Einstellung auf 0 können in einigen Fällen grafische Cursorstörungen behoben werden.
root/ConnectionType/xen/general/enableDataCompression	Wenn der Wert 1 ist, dann ist Datenkomprimierung aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung `Compress` direkt zugeordnet.
root/ConnectionType/xen/general/enableDriveMapAndRedirect	Wenn der Wert 1 ist, werden Zuordnung und Umleitung von USB-Speichergeräten aktiviert.
root/ConnectionType/xen/general/enableDriveMapping	Bei Einstellung auf 1 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, ext3.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/enableDynamicDriveMapping	Wenn der Wert 1 ist, werden USB-Speichergeräte auf dem Citrix-Server dynamisch zugeordnet. Bei Einstellung des Werts auf 0 ist die Speichererweiterung für die USB-Speichergeräte deaktiviert.
root/ConnectionType/xen/general/enableForceDirectConnect	Stellen Sie den Wert 1 ein, um die Verbindung zur Citrix-Web-Benutzeroberfläche und PNAgent-Dienste zu umgehen. Die Authentifizierung findet am Server statt, nachdem die erste Verbindung hergestellt wurde.
root/ConnectionType/xen/general/enableH264Compression	Wenn der Wert 1 ist, wird die H.264-Komprimierung aktiviert. Der H.264-Codec bietet mehr Leistung bei umfangreichen und professionellen Grafikanwendungen auf WAN-Netzwerken im Vergleich zum JPEG-Codec.
root/ConnectionType/xen/general/enableHDXFlashRedirection	Steuert das Verhalten der HDX Flash-Umleitung. Wenn `Always` eingestellt ist, dann wird, wenn möglich, die HDX Flash-Umleitung verwendet und der Benutzer wird nicht aufgefordert. Wenn `Ask` eingestellt ist, dann wird der Benutzer aufgefordert. Durch die Einstellung `Never` wird diese Funktionalität deaktiviert.
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	Steuert das Verhalten des Side Content Fetching (Abrufen der Seiteninhalte) des HDX Flash Servers. Wenn deaktiviert, wird der Client Inhalte abrufen.
root/ConnectionType/xen/general/enableHDXMediaStream	Wenn der Wert 1 ist, dann ist HDX MediaStream aktiviert. Wenn der Wert 0 ist, werden Mediendateien weiterhin über Standard-Streaming wiedergegeben, aber die Qualität ist möglicherweise nicht so gut.
root/ConnectionType/xen/general/enableHWH264	Wenn der Wert 1 ist und auch `enableH264Compression` 1 ist, wird die Hardwarekomprimierung für H.264 aktiviert. Wenn der Wert 0 ist, wird die H.264 Komprimierung von Software bearbeitet.
root/ConnectionType/xen/general/enableMapOn<AthruZ>	Wenn hier der Wert 1 eingestellt wird, kann diesem Laufwerk auf dem Remote-Host ein lokales Dateisystem zugeordnet werden. Der entsprechende Registrierungsschlüssel `DrivePathMappedOn` muss auf ein gültiges lokales Verzeichnis eingestellt sein, damit die Laufwerkszuordnung einwandfrei funktioniert.
root/ConnectionType/xen/general/enableMultiMedia	Wenn der Wert 1 ist, dann ist Multimedia aktiviert. Mit HDX Lync liegt möglicherweise ein Gerätekonflikt vor, wenn diese Einstellung aktiviert ist. Diese Einstellung ist der Citrix INI-Dateieinstellung `MultiMedia in Virtual Channels` direkt zugeordnet.
root/ConnectionType/xen/general/enableOffScreenSurface	Wenn der Wert 1 ist, dann kann der Server das Format `X PixMap` für Offscreen-Zeichnungen verwenden. Reduziert die Bandbreite in 15-Bit- und 24-Bit-Farbe auf Kosten des X-Serverspeichers und der Prozessorzeit. Diese Einstellung ist der Citrix INI-Dateieinstellung `EnableOSS` direkt zugeordnet.
root/ConnectionType/xen/general/enableSessionReliability	Wenn der Wert 1 ist, wird die Citrix-Sitzungszuverlässigkeit aktiviert. Die Sitzungszuverlässigkeit ändert die Art, wie Sitzungen nach dem Verlust einer Netzwerkverbindung fortgesetzt werden. In der Citrix-Dokumentation finden Sie weitere Informationen zur Sitzungszuverlässigkeit.
root/ConnectionType/xen/general/enableSmallFrames	Wenn der Wert 1 ist, werden kleine Nicht-H.264-Frame-Aktualisierungen für H.264 aktiviert. `enableTextTracking` muss auch aktiviert sein, damit dies einen Effekt hat.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/enableSmartCard	Bei Einstellung des Werts auf 1 wird Smart-Card-Anmeldung aktiviert.
root/ConnectionType/xen/general/enableTextTracking	Wenn der Wert 1 ist, werden optimierte verlustfreie Textüberlagerungen für H.264 aktiviert.
root/ConnectionType/xen/general/enableUSBRedirection	Wenn der Wert 1 ist, werden USB-Speichergeräte umgeleitet.
root/ConnectionType/xen/general/enableWindowsAlertSounds	
root/ConnectionType/xen/general/encryptionLevel	Legt die Ebene der Verschlüsselung fest. Die Verschlüsselungsprotokolle für alle Stufen sind im Abschnitt [EncryptionLevelSession] der module.ini definiert. Diese Einstellung ist der Citrix INI-Dateieinstellung [EncryptionLevelSession] direkt zugeordnet.
root/ConnectionType/xen/general/fontSmoothingType	Legt die Art der Schriftartglättung fest.
root/ConnectionType/xen/general/hotKey<1thru15>Char	Legt fest, dass die Tastenkombination zur Remote-Sitzung weitergeleitet wird, wenn die Taste bzw. Tastenkombination, die in der entsprechenden HotKeyShift eingerichtet ist, betätigt wird.
root/ConnectionType/xen/general/hotKey<1thru15>Shift	Legt die Taste bzw. Tastenkombination fest, die zur Aktivierung der Tastenkombination dient, die in der entsprechenden HotKeyChar eingerichtet ist.
root/ConnectionType/xen/general/httpAddresses/<UUID>/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Legt die Taste auf der Tastatur zur Deaktivierung des transparenten Tastaturmodus fest. Diese Einstellung ist der Citrix INI-Dateieinstellung KeyPassthroughEscapeChar direkt zugeordnet.
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Legt die Tastatur-Tastenkombination zum Deaktivieren des transparenten Tastaturmodus fest. Diese Einstellung ist der Citrix INI-Dateieinstellung KeyPassthroughEscapeShift direkt zugeordnet.
root/ConnectionType/xen/general/lastComPortNum	Legt die Anzahl der zugeordneten seriellen Ports fest. Wenn der Wert 0 ist, dann ist Zuordnung des seriellen Anschlusses deaktiviert.
root/ConnectionType/xen/general/leftMonitor	Legt fest, dass auf dem Bildschirmbereich des linken Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/localTextEcho	Steuert die Tastatur-Latenzreduktion. Diese Einstellung ist der Citrix INI-Dateieinstellung ZLKeyboardMode direkt zugeordnet.
root/ConnectionType/xen/general/monitorNetwork	Wenn der Wert auf Off eingestellt ist, dann wird die Netzwerkkonnektivität nicht überwacht. Wenn die Einstellung Local network link status only gewählt wurde, wird nur der Local Area Network Linkstatus überwacht. Wenn die Einstellung Server online status gewählt wurde, dann werden sowohl der Local Area Network Linkstatus und die Server-Konnektivität überwacht.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/mouseClickFeedback	Steuert die Maus-Latenzreduktion. Diese Einstellung ist der Citrix INI-Dateieinstellung ZLMouseMode indirekt zugeordnet.
root/ConnectionType/xen/general/mouseMiddleButtonPaste	Wenn der Wert 1 ist, dann ist die mittlere Maustaste zum Einfügen der Emulation für Windows-Sitzungen aktiviert. Diese Einstellung ist der Citrix INI-Dateieinstellung MouseSendsControlV direkt zugeordnet.
root/ConnectionType/xen/general/noInfoBox	Wenn der Wert 1 ist, dann wird der Client Manager (Wfcmgr) nicht angezeigt, wenn eine Clientsitzung beendet wird. Diese Einstellung ist der Citrix INI-Dateieinstellung PopupOnExit direkt zugeordnet.
root/ConnectionType/xen/general/printerAutoCreation	Durch die Einstellung 0 wird die Druckerzuordnung deaktiviert. Wenn der Wert 1 ist, dann werden lokal definierte Drucker der Verbindung zugeordnet. Durch die Einstellung 2 werden USB-Drucker entsprechend der Angaben im USB-Manager weitergeleitet.
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 Kennwort 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 wird nur unterstützt, wenn ein lokaler Browser installiert ist.
root/ConnectionType/xen/general/proxyUser	Der zu verwendende Proxy-Benutzername, wenn eine manuelle Proxy-Einstellung über proxyType ausgewählt ist.
root/ConnectionType/xen/general/rightMonitor	Legt fest, dass auf dem Bildschirmbereich des rechten Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/saveLogs	Wenn der Wert 1 ist, werden detaillierte Protokollinformationen gespeichert, nachdem die Sitzung beendet wurde. Diese Protokollinformationen werden im folgenden Verzeichnis gespeichert: /tmp/debug/citrix/<Datum>/
root/ConnectionType/xen/general/serverCheckTimeout	
root/ConnectionType/xen/general/sessionSharingClient	Wenn auf 1 gesetzt, werden Anforderungen zur Sitzungsfreigabe an andere Citrix-Sitzungen auf dem gleichen X-Display gesendet. Diese Einstellung ist der Citrix INI-Dateieinstellung EnableSessionSharingClient direkt zugeordnet.
root/ConnectionType/xen/general/showOnAllMonitors	Wenn der Wert 1 ist, wird der virtuelle Desktop auf allen Monitoren angezeigt.
root/ConnectionType/xen/general/smartCardModuleMap/CoolKeyPK11	Gibt den Pfad zum Smart Card-Sicherheitsmodul CoolKey PKCS #11 an.
root/ConnectionType/xen/general/smartCardModuleMap/GemaltoDotNet	Gibt den Pfad zum Smart Card-Sicherheitsmodul Gemalto .NET an.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/general/smartCardModuleMap/OpenSC	Gibt den Pfad zum Smart Card-Sicherheitsmodul Open SC an.
root/ConnectionType/xen/general/sound	Legt die Audioqualität fest. Diese Einstellung ist der Citrix INI-Dateieinstellung AudioBandwidthLimit indirekt zugeordnet.
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/<UUID>/address	
root/ConnectionType/xen/general/topMonitor	Legt fest, dass auf dem Bildschirmbereich des oberen Monitors der virtuelle Desktop angezeigt wird. Wenn der Wert 0 ist, wird der Monitor nicht verwendet, um den virtuellen Desktop anzuzeigen.
root/ConnectionType/xen/general/transparentKeyPassthrough	Steuert, wie bestimmte Windows Tastenkombinationen behandelt werden. Wenn der Wert Translated eingestellt ist, dann gilt die Tastenkombinationen für den lokalen Desktop. Wenn der Wert Direct in full screen desktops only eingestellt ist, dann gilt die Tastenkombinationen nur für die Remote-Sitzung, wenn sich diese im Vollbildmodus befindet. Wenn der Wert Direct eingestellt ist, dann gilt die Tastenkombinationen immer für die Remote-Sitzung gelten, solange das Fenster aktiv ist. Diese Einstellung ist der Citrix INI-Dateieinstellung TransparentKeyPassthrough indirekt zugeordnet.
root/ConnectionType/xen/general/twRedundantImageItems	Regelt die Anzahl der Display-Bereiche, die in Thinwire nachverfolgt werden, um ein überflüssiges Zeichnen von Bitmap-Bildern zu verhindern. Ein ausreichender Wert für 1024 x 768 Sitzungen ist 300.
root/ConnectionType/xen/general/useAlternateAddress	Wenn der Wert 1 ist, dann wird eine alternative Adresse für Firewall Verbindungen verwendet. Diese Einstellung ist der Citrix INI-Dateieinstellung UseAlternateAddress direkt zugeordnet.
root/ConnectionType/xen/general/useBitmapCache	Bei Einstellung des Werts auf 1 wird der permanente Disk-Cache aktiviert. Der permanente Disk-Cache speichert häufig verwendete grafische Objekte wie Bitmaps auf der Festplatte des Thin Client. Die Verwendung des permanenten Disk-Cache verbessert die Leistung für Verbindungen mit niedriger Bandbreite, reduziert aber die Größe des verfügbaren Speicherplatzes auf dem Thin Client. Für Thin Clients in Hochgeschwindigkeits-LANs ist die Verwendung des permanenten Disk-Cache nicht notwendig. Diese Einstellung ist der Citrix INI-Dateieinstellung PersistentCacheEnabled direkt zugeordnet.
root/ConnectionType/xen/general/useEUKS	Regelt die Verwendung von Extended Unicode Keyboard Support (EUKS - Erweiterte Unicode-Tastaturunterstützung) auf Windows-Servern. Wenn der Wert 0 ist, dann wird EUKS nicht verwendet. Wenn der Wert 1 ist, dann wird EUKS als Ausweichmöglichkeit verwendet. Wenn der Wert 2 ist, dann wird EUKS verwendet, wenn möglich.
root/ConnectionType/xen/general/useLocalIM	Wenn diese Einstellung aktiviert ist, wird die lokale X Eingabemethode verwendet, um die Tastatureingabe zu interpretieren. Dies wird nur für europäische Sprachen

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	unterstützt. Diese Einstellung ist der Citrix INI-Dateieinstellung `useLocalIME` direkt zugeordnet.
`root/ConnectionType/xen/general/userAgent`	Die Zeichenfolge dieses Schlüssels wird vom Citrix-Client präsentiert und ist nützlich für Administratoren, um zu wissen, woher die Verbindungsanforderung stammt.
`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/webcamFramesPerSec`	Steuert die `HDXWebCamFramesPerSec` Variable in der All_Regions.ini-Datei.
`root/ConnectionType/xen/general/webcamSupport`	Wenn der Wert 0 ist, dann sind die Webcam und die Webcam-Soundwiedergabe deaktiviert. Wenn er auf 1 gesetzt ist, dann sind die Webcam und das Webcam Audio mit der Komprimierung aktiviert. Wenn der Wert 2 ist, dann ist die USB-Umleitung der Webcam und das Webcam Audio aktiviert.
`root/ConnectionType/xen/general/windowHeight`	Legt die Höhe des Fensters in Pixel fest, wenn `windowSize` auf `Fixed Size` eingestellt ist.
`root/ConnectionType/xen/general/windowPercent`	Legt die Größe des Fensters als Prozentsatz fest, wenn `windowSize` auf `Percentage of Screen Size` eingestellt ist.
`root/ConnectionType/xen/general/windowSize`	Wenn als `Default` festgelegt, dann werden die serverseitige Einstellungen verwendet. Wenn `Full Screen` eingestellt ist, wird die Verbindung auf allen verfügbaren Bildschirmen ohne Ränder maximiert. Bei der Einstellung auf `Fixed Size` können die Schlüssel `windowWidth` und `windowSizeHeight` verwendet werden, um die Größe des Fensters in Pixel anzugeben. Wenn `Percentage of Screen Size` eingestellt ist, kann der Schlüssel `WindowPercent` verwendet werden, um die Größe des Fensters als Prozentsatz des gesamten Bildschirmbereichs anzugeben. Damit die Einstellung `Percentage of Screen Size` wirksam ist, muss `EnableForceDirectConnect` auf 1 eingestellt werden und `TWIMode` muss auf 0 eingestellt werden. Diese Einstellung funktioniert nur mit XenApp und nur, wenn der Server direkte Verbindungen erlaubt. Diese Einstellung funktioniert nicht mit XenDesktop.
`root/ConnectionType/xen/general/windowWidth`	Legt die Breite des Fensters in Pixel fest, wenn `windowSize` auf `Fixed Size` eingestellt ist.
`root/ConnectionType/xen/gui/XenDesktopPanel/disabled`	Wenn der Wert 1 ist, dann sind das Xen-Desktop-Fenster und seine Taskleiste deaktiviert. Wird in der Regel verwendet, wenn `autoStartResource` oder `autoStartDesktop` aktiviert ist.
`root/ConnectionType/xen/gui/XenManager/name`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`root/ConnectionType/xen/gui/XenManager/status`	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/gui/XenManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xen/gui/XenManager/widgets/address	Steuert den Status des Widgets **Service URL** im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/appInMenu	Steuert den Status des Widgets **Show applications on taskbar** (Anwendungen auf der Taskleiste anzeigen) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/appOnDesktop	Steuert den Status des Widgets **Show applications on desktop** (Anwendungen auf Desktop anzeigen) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/autoReconnect	Steuert den Status des Widgets **Auto reconnect** (automatisches Neuverbinden) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/autoStartDesktop	Steuert den Status des Widgets **Auto Start Desktop** (Automatisches Starten des Desktops) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/autoStartResource	Steuert den Status des Widgets **Auto Start Resource** (Automatisches Starten der Ressource) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/autostart	Steuert den Status des Widgets **Auto start priority** (automatisches Starten der Priorität) im Verbindungsmanager für diesen Verbindungstyp. 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-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ConnectionType/xen/gui/XenManager/widgets/domain	Steuert den Status des Widgets **Domain** (Domäne) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/fallBackConnection	Steuert den Status des Widgets **Fallback Connection** (Ausweichverbindung) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/folder	
root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon	Steuert den Status des Widgets **Show icon on desktop** (Symbol auf Desktop zeigen) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/isInMenu	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/ConnectionType/xen/gui/XenManager/widgets/label	Steuert den Status des Widgets **Name** im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/password	Steuert den Status des Widgets **Password** (Kennwort) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/username	Steuert den Status des Widgets **Username** (Benutzername) im Verbindungsmanager für diesen Verbindungstyp. 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/xen/gui/XenManager/widgets/waitForNetwork	Steuert den Status des Widgets **Wait for network before connecting** (Vor dem Verbinden auf Netzwerk warten) im Verbindungsmanager für diesen Verbindungstyp. 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

Tabelle E-12 root > ConnectionType > xen (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Einstellung `read-only` wird das Widget im schreibgeschützten Modus angezeigt.
`root/ConnectionType/xen/gui/fbpanel/autohide`	Wenn der Wert `true` ist, dann wird automatisch die Taskleiste ausgeblendet.
`root/ConnectionType/xen/gui/fbpanel/edge`	Legt die Standard-Position der Taskleiste fest, wenn mehr als ein veröffentlichter Desktop oder mehr als eine veröffentlichte Anwendung verfügbar ist.
`root/ConnectionType/xen/gui/fbpanel/hidden`	Bei Auswahl 1, ist die Taskleiste vollständig ausgeblendet, aber nur, wenn `autoStartResource` oder `autoStartDesktop` aktiviert ist.

root > CpuMgr

Tabelle E-13 root > CpuMgr

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

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

HINWEIS: Das Dashboard entspricht der Taskleiste.

Tabelle E-14 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/Search	Wenn der Wert 1 ist, wird die Schaltfläche „Suchen“ auf der Taskleiste angezeigt.
root/Dashboard/GUI/SystemInformation	Bei Einstellung auf den Standardwert 1 wird die Schaltfläche „Systeminformation“ 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	Wenn der Wert 1 ist, dann wird der Anwendungsbereich auf der Taskleiste angezeigt.
root/Dashboard/General/AlwaysOnTop	Wenn der Wert 1 ist, wird die Taskleiste immer im Vordergrund benutzt.
root/Dashboard/General/AutoHide	Wenn der Wert 1 ist, wird die Taskleiste automatisch ausgeblendet.
root/Dashboard/General/EnterLeaveTimeout	Legt die Dauer in Millisekunden fest, bevor die Taskleiste ausgeblendet bzw. einblendet wird, wenn AutoHide aktiviert ist.
root/Dashboard/General/IconSize	Regelt die Größe der Symbole in der Taskleiste.
root/Dashboard/General/Length	Legt die Länge der Taskleiste fest.
root/Dashboard/General/LengthToScreenSide	Bei Einstellung auf den Standardwert 1 ist die Länge der Taskleiste fest und entspricht der Länge der Bildschirmseite, an der sie angeheftet ist.
root/Dashboard/General/PanelDockSide	Legt die Seite des Bildschirms fest, an der die Taskleiste angedockt ist.
root/Dashboard/General/RemainPixel	Legt die Anzahl an Pixeln fest, die sichtbar sind, wenn die Taskleiste ausgeblendet ist.
root/Dashboard/General/SlidingTimeout	Legt die Dauer in Millisekunden fest, die benötigt werden, um die Taskleiste ein- oder auszublenden, wenn AutoHide aktiviert ist.
root/Dashboard/General/Width	Legt die Breite der Taskleiste fest.

root > Display

Tabelle E-15 root > Display

Registrierungsschlüssel	Beschreibung
root/Display/Configuration/AMDOptions/SWCursor	Wenn der Wert 1 ist, wird ein von der Software gerenderter Mauscursor verwendet, was Probleme mit Cursorbeschädigungen beheben, aber Probleme mit der Multimedia-Wiedergabe und

Tabelle E-15 root > Display (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	Touchscreens verursachen kann. Wenn der Wert 0 ist, wird ein von der Hardware gerenderter Mauscursor verwendet, was Probleme mit der Multimedia-Wiedergabe und Touchscreens behebt.
root/Display/Configuration/displaymode	Legt den Anzeigemodus fest. Wenn der Wert 0 ist, dann wird der Standard-Modus (einer 1 – 4-Monitor-Konfiguration) verwendet. Wenn der Wert 1 ist, dann kann eine 6-Monitor-Konfiguration verwendet werden, aber nur auf unterstützten Plattformen mit der entsprechenden Add-on-Karte.
root/Display/Configuration/hexlayout	Gibt das Layout in Sechs-Monitor-Modus an.
root/Display/Configuration/hexprofile	Gibt das im Sechs-Monitor-Modus verwendete Profil an.
root/Display/Configuration/primaryprofile	Legt das Profil fest, das für den primären Monitor über den Profilnamen verwendet wird. Für Smart Zero muss dies immer auf `Standard` eingestellt werden.
root/Display/Configuration/quaternarymode	Legt die Position des vierten Monitors im Verhältnis des in `Quaternaryrelative` angegebenen Monitors fest. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.
root/Display/Configuration/quaternaryprofile	Legt das Profil fest, das für den vierten Monitor über den Profilnamen verwendet wird.
root/Display/Configuration/quaternaryrelative	Zeigt an, welcher Monitor referenziert wird, um die Position des vierten Monitors einzustellen.
root/Display/Configuration/secondaryConnector	Gibt den sekundären Anschluss an.
root/Display/Configuration/secondarymode	Gibt die Position des sekundären Monitors in Bezug auf den primären Monitor an. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.
root/Display/Configuration/secondaryorientation	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Display/Configuration/secondaryprofile	Legt das Profil fest, das für den sekundären Monitor über den Profilnamen verwendet wird.
root/Display/Configuration/swapstate	Gibt an, welcher Anschluss den Hauptmonitor verbindet. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. in der Regel bedeutet 0, dass der primäre Monitor am VGA-Anschluss ist, und 1 bedeutet, dass er am „anderen“ Anschluss ist. Für den t510 bedeutet 0, dass der primäre Monitor am DVI-I-Anschluss ist, und 1 bedeutet, dass der primäre Monitor am DVI-D-Anschluss ist. Für Plattformen mit einer Video-Add-on-Karte bedeutet 0, dass der primäre Monitor sich auf der integrierten Grafikkarte befindet und 1 bedeutet, dass der primäre Monitor auf der Add-on-Videokarte ist.
root/Display/Configuration/tertiarymode	Legt die Position des dritten Monitors im Verhältnis des in `tertiaryrelative` angegebenen Monitors fest. Dies ist Hardware-abhängig und wird nicht bei allen Modellen unterstützt. Werte sind wie folgt definiert: 0 = identisch; 1 = Oben; 2 = Rechts daneben; 3 = Links daneben; 4 = Unten.

Tabelle E-15 root > Display (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Display/Configuration/tertiaryprofile	Legt das Profil fest, das für den dritten Monitor über den Profilnamen verwendet wird.
root/Display/Configuration/tertiaryrelative	Zeigt an, welcher Monitor referenziert wird, um die Position des dritten Monitors einzustellen.
root/Display/Profiles/<UUID>/colorScaling	Legt die Farbtemperatur oder direkte RGB-Skalierung für ThinClients mit integrierten Monitoren fest. 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	Legt die Display-Farbtiefe in Bits pro Pixel fest. Eine höhere Farbtiefe bedeutet bessere Qualität, aber geringere Leistung.
root/Display/Profiles/<UUID>/height	Legt die gewünschte Monitor-Auflösungshöhe fest. Wenn der Wert 0 ist, wird die Auflösung automatisch erkannt. <
root/Display/Profiles/<UUID>/label	Legt den Profilnamen in der Anzeige fest. Für Smart Zero muss dies immer auf Standard eingestellt werden.
root/Display/Profiles/<UUID>/orientation	Legt die Monitorausrichtung wie folgt fest: 0 = Normal; 1 = Nach links drehen; 2 = Nach rechts drehen; 3 = Invertieren.
root/Display/Profiles/<UUID>/refresh	Gibt die gewünschte Bildwiederholungsrate für den Monitor an. Nicht alle Bildwiederholungsraten werden für alle Auflösungen unterstützt. Wenn der Wert 0 ist, dann wird die Aktualisierungsrate automatisch erkannt. Die unterstützten Werte sind abhängig vom Monitor. Das Einrichten einer Aktualisierungsrate, die von dem angeschlossenen Monitor nicht unterstützt wird, wird zu einem schwarzen Bildschirm führen. HP empfiehlt, diese Einstellung auf 0 zu lassen.
root/Display/Profiles/<UUID>/width	Legt die gewünschte Monitor-Auflösungsbreite fest. Wenn der Wert 0 ist, dann wird die Auflösung automatisch erkannt.
root/Display/userLock	Wenn der Wert 1 ist und die Anzeigeeinstellungen vom Benutzer geändert wurden, werden die Anzeigeeinstellungen beim Import eines ThinPro-Profils beibehalten.
root/Display/userLockEngaged	Dieser Registrierungsschlüssel wird automatisch auf 1 gesetzt, nachdem die Anzeigeeinstellungen vom Benutzer geändert wurden. Sie müssen diese Einstellung in der Regel nicht ändern.

root > Network

Tabelle E-16 root > Network

Registrierungsschlüssel	Beschreibung
root/Network/ActiveDirectory/Domain	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/DynamicDNS	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.

Tabelle E-16 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/ActiveDirectory/Enabled	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Method	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Password	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/ActiveDirectory/Username	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/Network/DNSServers	Hier kann ein zusätzlicher DNS-Server für die Auflösung des 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	Legt das Standard-Hostnamensmuster fest, das zu verwenden ist, wenn neue Hostnamen generiert werden. Dies wird verwendet, wenn sowohl der Registrierungsschlüssel `Hostname` als auch `/etc/hostname` leer ist. Verwenden Sie im Muster des Hostnamen `%` als Trennzeichen. Im Beispiel `HPTC%MAC:1-6%` wäre `HPTC` das Präfix und die ersten sechs Zeichen der MAC-Adresse des Thin Client würden folgen. Wenn die MAC-Adresse des Thin Client also `11:22:33:44:55:66` ist, dann wäre der generierte Hostname `HPTC112233`. Ist das Muster `TC%MAC%`, wäre der generierte Hostname `TC112233445566`. Wenn das Muster `HP%MAC:7%` ist, dann wäre der generierte Hostname `HP1122334`.
root/Network/FtpProxy	Legt die FTP-Proxy-Adresse fest. HP empfiehlt, dass das folgende Format für diesen Wert verwendet wird, da das http-Präfix besser unterstützt ist: `http://ProxyServer:Port`
root/Network/Hostname	Legt den Hostnamen des Thin Client fest.
root/Network/HttpProxy	Legt die HTTP-Proxy-Adresse fest. HP empfiehlt die Verwendung des folgenden Format: `http://ProxyServer:Port`
root/Network/HttpsProxy	Legt die HTTPS-Proxy-Adresse fest. HP empfiehlt, dass das folgende Format für diesen Wert verwendet wird, da das http-Präfix besser unterstützt ist: `http://ProxyServer:Port`
root/Network/IPSec/IPSecRules/<UUID>/DstAddr	Legt die Zieladresse für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethod	Legt die Authentifizierungsmethode für die IPSec Regel fest. `PSK` wird für einen Pre-shared-Schlüssel verwendet und `Certificate` für die Verwendung der Zertifikat-Dateien.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodCACert	Wenn die Authentifizierungsmethode `Certificate` ist, wird der Dateipfad des CA-Zertifikats in diesem Registrierungsschlüssel gespeichert.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodClientCert	Wenn die Authentifizierungsmethode `Certificate` ist, wird der Dateipfad des Client-Zertifikats in diesem Registrierungsschlüssel gespeichert.

Tabelle E-16 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPresharedKey	Wenn die Authentifizierungsmethode PSK ist, wird der Pre-shared-Key-Wert in diesem Registrierungsschlüssel gespeichert.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPrivateKey	Wenn die Authentifizierungsmethode Certificate ist, wird der private Schlüsseldatei-Pfad, der dem Client-Zertifikat entspricht, in diesem Registrierungsschlüssel gespeichert.
root/Network/IPSec/IPSecRules/<UUID>/MMDHGroup	Legt die Phase 1 der Diffie-Hellman-Gruppe fest.
root/Network/IPSec/IPSecRules/<UUID>/MMEncryptionAlg	Legt die Phase 1 des Verschlüsselungsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/MMIntegrityAlg	Legt die Phase 1 des Integritätsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/MMLifetimeMinutes	Legt die Phase 1 der Lebensdauer fest.
root/Network/IPSec/IPSecRules/<UUID>/QMAHEnable	Ermöglicht Phase 2 AH.
root/Network/IPSec/IPSecRules/<UUID>/QMAHIntegrityAlg	Legt die Phase 2 AH des Integritätsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEnable	Ermöglicht Phase 2 ESP.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEncryptionAlg	Legt die Phase 2 ESP des Verschlüsselungsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/QMESPIntegrityAlg	Legt die Phase 2 ESP des Integritätsalgorithmus fest.
root/Network/IPSec/IPSecRules/<UUID>/QMLifetimeSeconds	Legt die Phase 2 der Lebensdauer fest.
root/Network/IPSec/IPSecRules/<UUID>/RuleDescription	Legt die Beschreibung für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/RuleEnable	Bei Einstellung des Werts auf 1 ist die Regel aktiviert.
root/Network/IPSec/IPSecRules/<UUID>/RuleName	Legt den Namen für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/SrcAddr	Legt die Quell-Adresse für die IPSec-Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/TunnelDstAddr	Legt die Tunnel-Zieladresse für die IPSec Regel fest.
root/Network/IPSec/IPSecRules/<UUID>/TunnelEnable	Ermöglicht Tunnelmodus für die IPSec Regel.
root/Network/IPSec/IPSecRules/<UUID>/TunnelSrcAddr	Legt die Tunnel-Quell-Adresse für die IPSec-Regel fest.
root/Network/KeepPreviousDNS	Wenn der Wert 1 ist, werden bereits konfigurierte DNS-Server und Suchdomänen, die nicht vom Netzwerkmanager generiert wurden, in resolv.conf aufbewahrt. Wenn der Wert 0 ist, dann wird resolv.conf komplett überschrieben.
root/Network/SearchDomains	Zusätzliche Suchdomänen für die FQDN-Auflösung können hier angegeben werden. Die angegebenen Domänen werden an alle unvollständigen Definitionen angehängt werden, als Versuch,

Tabelle E-16 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	einen FQDN zu erzeugen, der über DNS aufgelöst werden kann. Zum Beispiel wird eine Suchdomäne `mydomain.com` die Serverdefinition `Myserver` ordnungsgemäß zu `myserver.mydomain.com` lösen, auch wenn der DNS-Server `Myserver` nicht in seinem Namenslösungsverzeichnis hat. Bis zu fünf zusätzliche Suchdomänen können angegeben werden.
`root/Network/VPN/AutoStart`	Wenn der Wert 1 ist, startet VPN automatisch beim Systemstart.
`root/Network/VPN/PPTP/Domain`	Legt die PPTP-Domäne fest.
`root/Network/VPN/PPTP/Gateway`	Legt das PPTP-Gateway fest.
`root/Network/VPN/PPTP/Password`	Legt das PPTP-Benutzerkennwort fest.
`root/Network/VPN/PPTP/Username`	Legt den PPTP-Benutzernamen fest.
`root/Network/VPN/Type`	Legt den VPN-Typ fest.
`root/Network/VPN/VPNC/Domain`	Legt die VPNC-Domäne fest.
`root/Network/VPN/VPNC/Gateway`	Legt das VPNC-Gateway fest.
`root/Network/VPN/VPNC/Group`	Legt die VPNC-Gruppe fest.
`root/Network/VPN/VPNC/GroupPassword`	Legt das VPNC-Gruppenkennwort fest.
`root/Network/VPN/VPNC/IKEDHGroup`	Legt die VPNC IKE Diffie-Hellman-Gruppe fest.
`root/Network/VPN/VPNC/LocalUDPPort`	Legt den lokalen UDP-Port für VPNC fest. Wenn der Wert 0 ist, wird ein zufälliger Port verwendet. Diese Einstellung gilt nur, wenn der NAT-Traversal-Modus (`NATTMode`) auf `cisco-udp` festgelegt ist.
`root/Network/VPN/VPNC/NATTMode`	Legt den NAT-Traversal-Modus für VPNC fest.
`root/Network/VPN/VPNC/Password`	Legt das VPNC-Benutzerkennwort fest.
`root/Network/VPN/VPNC/PerfectForwardSecrecy`	Legt für die VPNC Diffie-Hellman-Gruppe fest, dass Perfect Forward Secrecy (PFS) verwendet werden soll.
`root/Network/VPN/VPNC/Security`	Legt die VPNC-Sicherheitsstufe fest.
`root/Network/VPN/VPNC/Username`	Legt den VPNC-Benutzernamen fest.
`root/Network/Wired/DefaultGateway`	Legt das Standard-Gateway fest, das vom Gerät für die Kommunikation mit dem Internet verwendet wird. In der Regel ist dies die IP-Adresse des Routers. Diese Einstellung wird nur wirksam, wenn `Method` auf `Static` eingestellt ist.
`root/Network/Wired/EnableDefGatewayAsDNS`	Wenn der Wert 1 ist, dann wird der Standard-Gateway auch als Namensservers benutzt.
`root/Network/Wired/EthernetSpeed`	Legt die Verbindungsgeschwindigkeit der primären Ethernet-Netzwerkschnittstelle fest. `Automatic` ermöglicht, dass die schnellste verfügbare Verbindungsgeschwindigkeit verwendet wird, die in der Regel 1 Gbit/s oder 100 Mbit/s/Full je nach Switch ist. Die Verbindungsgeschwindigkeit kann auch erzwungen werden, um eine einzige Geschwindigkeit (100 Mbit/s oder 10 Mbit/s) und einen Duplexmodus (Voll oder Halb) zu verwenden, sodass Switches oder Hubs unterstützt werden, die keine angemessene Autonegotiation durchführen.

Tabelle E-16 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/Wired/IPAddress	Legt die IPv4-Adresse des Thin Client fest. Diese Einstellung wird nur wirksam, wenn Method auf Static eingestellt ist.
root/Network/Wired/IPv6Enable	Wenn der Wert 1 ist, dann ist IPv6 aktiviert.
root/Network/Wired/Interface	Legt die Standard-Ethernet-Schnittstelle oder NIC fest.
root/Network/Wired/MTU	Legt die MTU fest. Es spielt dabei keine Rolle, wenn die IP-Adresse statisch oder DHCP-erworben wird.
root/Network/Wired/Method	Wenn Automatic eingestellt ist, verwendet der Thin Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn Static eingestellt ist, werden die Werte der Registrierungsschlüssel IP-Adresse, SubnetMask und DefaultGateway verwendet. HP rät, in einem generischen ThinPro-Profil Static nicht zu verwenden, da es dazu führt, dass alle Thin Clients die gleiche IP-Adresse erhalten.
root/Network/Wired/Security/CACert	Legt den Pfad zu der CA-Zertifikatsdatei fest.
root/Network/Wired/Security/EnableMachineAuth	Wenn der Wert 1 ist, wird die Computerauthentifizierung für PEAP aktiviert.
root/Network/Wired/Security/Identity	Legt die Identität oder anonyme Identität fest.
root/Network/Wired/Security/InnerAuth	Legt das PEAP innere Authentifizierung-Protokoll fest.
root/Network/Wired/Security/InnerAuthTTLS	Legt das TTLS innere Authentifizierung-Protokoll fest.
root/Network/Wired/Security/PEAPVersion	Legt die PEAP-Version fest.
root/Network/Wired/Security/Password	Legt das Kennwort fest.
root/Network/Wired/Security/PrivateKey	Legt den Pfad zu einer privaten Schlüsseldatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wired/Security/Type	Legt den 802.1x-Authentifizierungstyp fest.
root/Network/Wired/Security/UserCert	Legt den Pfad zu einer Benutzer-Zertifikatsdatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wired/Security/Username	Legt den Benutzernamen fest.
root/Network/Wired/SubnetMask	Legt die Subnetzmaske des Geräts fest, z. B. 255.255.255.0 (für ein Standard-Klasse C Subnetz). Diese Einstellung wird nur wirksam, wenn Method auf Static eingestellt ist.
root/Network/Wireless/DefaultGateway	Legt das Standard-Gateway fest, das vom Gerät für die Kommunikation mit dem Internet verwendet wird. In der Regel ist dies die IP-Adresse des Routers. Diese Einstellung wird nur wirksam, wenn Method auf Static eingestellt ist.
root/Network/Wireless/EnableDefGatewayAsDNS	Wenn der Wert 1 ist, dann wird der Standard-Gateway auch als Namensservers benutzt.
root/Network/Wireless/IPAddress	Legt die IPv4-Adresse des Thin Client fest. Diese Einstellung wird nur wirksam, wenn Method auf Static eingestellt ist.
root/Network/Wireless/IPv6Enable	Wenn der Wert 1 ist, dann ist IPv6 aktiviert.
root/Network/Wireless/Interface	Legt die drahtlose Standardschnittstelle oder den kabellosen Netzwerkadapter fest.

Tabelle E-16 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/Wireless/Method	Wenn Automatic eingestellt ist, verwendet der Thin Client DHCP, um die Netzwerkeinstellungen abzurufen. Wenn Static eingestellt ist, werden die Werte der Registrierungsschlüssel IP-Adresse, SubnetMask und DefaultGateway verwendet. HP rät, in einem generischen ThinPro-Profil Static nicht zu verwenden, da es dazu führt, dass alle Thin Clients die gleiche IP-Adresse erhalten.
root/Network/Wireless/PowerEnable	Wenn der Wert 1 ist, dann ist das Energiemanagement der drahtlosen Netzwerk-Karte aktiviert.
root/Network/Wireless/SSID	Legt den drahtlosen Zugangspunkt fest, der über SSID verwendet wird.
root/Network/Wireless/SSIDHidden	Gibt an, ob die SSID des drahtlosen Zugangspunkts ausgeblendet ist.
root/Network/Wireless/SSIDWhiteList	Gibt eine Positivliste für WLAN-Access Points an. Wenn der Wert dieses Registrierungsschlüssels nicht leer ist, werden nur die im Wert angegebenen SSIDs in den Prüfergebnissen für WLAN-Access Points angezeigt. Verwenden Sie ein Semikolon, um die SSIDs zu trennen.
root/Network/Wireless/Security/CACert	Legt den Pfad zu der CA-Zertifikatsdatei fest.
root/Network/Wireless/Security/EAPFASTPAC	Legt den Pfad der PAC-Datei für die EAP-FAST-Authentifizierung fest.
root/Network/Wireless/Security/EAPFASTProvision	Legt die bereitgestellte Option für die EAP-FAST-Authentifizierung fest.
root/Network/Wireless/Security/Identity	Legt die Identität oder anonyme Identität fest.
root/Network/Wireless/Security/InnerAuth	Legt das PEAP innere Authentifizierung-Protokoll fest.
root/Network/Wireless/Security/InnerAuthTTLS	Legt das TTLS innere Authentifizierung-Protokoll fest.
root/Network/Wireless/Security/PEAPVersion	Legt die PEAP-Version fest.
root/Network/Wireless/Security/Password	Legt das Kennwort fest.
root/Network/Wireless/Security/PrivateKey	Legt den Pfad zu einer privaten Schlüsseldatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wireless/Security/Type	Legt den drahtlosen Authentifizierungstyp fest.
root/Network/Wireless/Security/UserCert	Legt den Pfad zu einer Benutzer-Zertifikatsdatei fest. Dies dient nur der TLS-Authentifizierung.
root/Network/Wireless/Security/Username	Legt den Benutzernamen fest.
root/Network/Wireless/Security/WEPAuth	Legt den WEP-Authentifizierungstyp fest.
root/Network/Wireless/Security/WEPIndex	Legt den WEP-Kennwortindex fest.
root/Network/Wireless/SubnetMask	Legt die Subnetzmaske des Geräts fest, z. B. 255.255.255.0 (für ein Standard-Klasse C Subnetz). Diese Einstellung wird nur wirksam, wenn Method auf Static eingestellt ist.
root/Network/disableLeftClickMenu	Wenn der Wert 1 ist, dann ist das Linksklick-Menü für das Netzwerk-Taskleistensymbol deaktiviert.
root/Network/disableRightClickMenu	Wenn der Wert 1 ist, dann ist das Rechtsklick-Menü für das Netzwerk-Taskleistensymbol deaktiviert.

Tabelle E-16 root > Network (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Network/iPeak/ShowStatus	Wenn der Wert 1 ist, dann wird der HP Velocity-Status als Teil des Symbols in der Taskleiste angezeigt. HP Velocity wird auf HP t420 nicht unterstützt.
root/Network/iPeak/Status	Bei Einstellung des Werts auf 1 wird HP Velocity aktiviert. Wenn der Wert 2 ist, dann ist HP Velocity im Monitor-Modus aktiviert. Durch die Einstellung 0 wird HP Velocity deaktiviert. HP Velocity wird auf HP t420 nicht unterstützt.
root/Network/userLock	Wenn der Wert 1 ist und die Netzwerkeinstellungen vom Benutzer geändert wurden, werden die Netzwerkeinstellungen beim Import eines ThinPro-Profils beibehalten.
root/Network/userLockEngaged	Dieser Registrierungsschlüssel wird automatisch auf 1 gesetzt, nachdem die Netzwerkeinstellungen vom Benutzer geändert wurden. Sie müssen diese Einstellung in der Regel nicht ändern.

root > SCIM

Tabelle E-17 root > SCIM

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

root > ScepMgr

Tabelle E-18 root > ScepMgr

Registrierungsschlüssel	Beschreibung
root/ScepMgr/General/AutoRenew/Enabled	Wenn der Wert 1 ist, werden Zertifikate automatisch erneuert, bevor sie ablaufen.
root/ScepMgr/General/AutoRenew/TimeFrame	Legt die Anzahl der Tage vor dem Ablaufdatum eines Zertifikats fest, die der SCEP-Manager versucht, das Zertifikat automatisch zu erneuern.
root/ScepMgr/IdentifyingInfo/CommonName	Legt den allgemeinen Namen fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. Ihr Name oder der vollständig qualifizierte Domänenname (Fully-Qualified Domain Name, FQDN) des Geräts. Der FQDN wird standardmäßig verwendet, wenn dieser Wert nicht angegeben wird.
root/ScepMgr/IdentifyingInfo/CountryName	Legt das Land bzw. die Region fest, das bzw. die für SCEP-Identifizierungsdaten verwendet werden soll.
root/ScepMgr/IdentifyingInfo/EmailAddress	Legt die E-Mail-Adresse fest, die für SCEP-Identifizierungsdaten verwendet werden soll.
root/ScepMgr/IdentifyingInfo/LocalityName	Legt den Ortsnamen fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. den Namen einer Stadt.
root/ScepMgr/IdentifyingInfo/OrganizationName	Legt den Organisationsnamen fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. einen Firmennamen oder einen Behördennamen.

Tabelle E-18 root > ScepMgr (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/ScepMgr/IdentifyingInfo/OrganizationUnitName	Legt den Namen einer Organisationseinheit fest, der für SCEP-Identifizierungsdaten verwendet werden soll, z. B. einen Abteilungsnamen oder einen Gruppennamen.
root/ScepMgr/IdentifyingInfo/StateName	Legt den Staat bzw. das Bundesland fest, der bzw. das für SCEP-Identifizierungsdaten verwendet werden soll.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/CertFileChanged	Der Registrierungsschlüssel dient nur dazu, die anderen Anwendungen zu informieren, dass eine Zertifikatsdatei geändert wurde. Dieser Schlüssel sollte keine Änderung erfordern.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/KeySize	Legt die Schlüsselgröße fest, die für das generierte Schlüsselpaar verwendet werden soll.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerName	Legt den Namen des SCEP-Servers fest.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerUrl	Legt die URL des SCEP-Servers fest, die erforderlich ist, damit der SCEP-Client ein Zertifikat registrieren kann.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Code	Enthält den Statuscode der SCEP-Registrierung. Dieser Wert ist schreibgeschützt.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Detail	Enthält detaillierte Informationen über die SCEP-Registrierung. Dieser Wert ist schreibgeschützt.

root > Search

Tabelle E-19 root > Search

Registrierungsschlüssel	Beschreibung
root/Search/Category/Applications/ConnectionManager/checked	
root/Search/Category/Applications/ConnectionManager/enabled	
root/Search/Category/Applications/Connections/checked	
root/Search/Category/Applications/Connections/enabled	
root/Search/Category/Applications/ControlPanel/checked	
root/Search/Category/Applications/ControlPanel/enabled	
root/Search/Category/Applications/Desktop/checked	
root/Search/Category/Applications/Desktop/enabled	
root/Search/Category/Applications/icon	
root/Search/Category/Applications/name	
root/Search/Category/FileSystem/caseSensitive	

Tabelle E-19 root > Search (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/Search/Category/FileSystem/enabled	
root/Search/Category/FileSystem/folderFilter	Gibt die Ordner im Dateisystem an, die der Benutzer durchsuchen darf. Verwenden Sie ein Semikolon, um Ordner zu trennen. Beispiel: /home/user;/usr/bin
root/Search/Category/FileSystem/location	
root/Search/Category/FileSystem/subFolder	
root/Search/Category/Miscellaneons/ CheckForUpdate	
root/Search/Category/Miscellaneons/Logout	
root/Search/Category/Miscellaneons/Reboot	
root/Search/Category/Miscellaneons/ShutDown	
root/Search/Category/Miscellaneons/Sleep	
root/Search/Category/Miscellaneons/ SwitchToAdmin	
root/Search/Category/Regeditor/byDir	
root/Search/Category/Regeditor/byKey	
root/Search/Category/Regeditor/byValue	
root/Search/Category/Regeditor/byWhole	
root/Search/GUI/showCategory	

root > Serial

Tabelle E-20 root > Serial

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

root > SystemInfo

Tabelle E-21 root > SystemInfo

Registrierungsschlüssel	Beschreibung
root/SystemInfo/Pages/General	Wenn der Wert 0 ist, dann wird die Registerkarte **General** (Allgemein) im Fenster „Systeminformationen“ für Standardbenutzer ausgeblendet.
root/SystemInfo/Pages/NetTools	Wenn der Wert 0 ist, dann wird die Registerkarte **Net Tools** (Netzhilfsmittel) im Fenster „Systeminformationen“ für Standardbenutzer ausgeblendet.
root/SystemInfo/Pages/Network	Wenn der Wert 0 ist, dann wird die Registerkarte **Network** (Netzwerk) im Fenster „Systeminformationen“ für Standardbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/ServicePacks	Wenn der Wert 0 ist, dann wird die Registerkarte **Service Packs** im Abschnitt **Software Information** (Softwareinformationen) für Standardbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInformation	Wenn der Wert 0 ist, dann wird die Registerkarte **Software Information** (Softwareinformation) im Fenster „Systeminformationen“ für Standardbenutzer ausgeblendet.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInstalled	Wenn der Wert 0 ist, dann wird die Registerkarte **Software Installed** (Installierte Software) im Abschnitt **Software Information** (Softwareinformationen) für Standardbenutzer ausgeblendet.
root/SystemInfo/Pages/SystemLogs	Wenn der Wert 0 ist, dann wird die Registerkarte **System Logs** (Systemprotokolle) im Fenster „Systeminformationen“ für Standardbenutzer ausgeblendet.
root/SystemInfo/authorized	Wenn der Wert 0 ist, dann ist die Schaltfläche „Systeminformationen“ in der Taskleiste für Standardbenutzer deaktiviert.

root > TaskMgr

Tabelle E-22 root > TaskMgr

Registrierungsschlüssel	Beschreibung
root/TaskMgr/General/AlwaysOnTop	Bei Auswahl 1 ist das Task-Manager-Fenster immer im Vordergrund.

root > USB

Tabelle E-23 root > USB

Registrierungsschlüssel	Beschreibung
root/USB/Classes/<ClassType>/ClassID	Legt die ID-Nummer der USB-Klasse fest.
root/USB/Classes/<ClassType>/DisplayName	Legt den Namen der USB-Klasse fest.
root/USB/Classes/<ClassType>/State	Legt fest, ob die Klasse zum Remote-Host zugeordnet ist.

Tabelle E-23 root > USB (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/USB/Classes/<ClassType>/Visible	Legt fest, ob die Klasse in der Benutzeroberfläche angezeigt wird, nicht in der Benutzeroberfläche angezeigt wird oder deaktiviert ist.
root/USB/Classes/ShowTab	Wenn der Wert 1 ist, dann wird der Abschnitt **Classes** (Klassen) im USB-Manager angezeigt.
root/USB/Devices/<UUID>/DisplayName	Legt den Namen fest, der im USB-Manager anzeigt wird. Wenn der Name nicht angegeben wird, versucht der USB-Manager einen passenden Namen anhand der Geräteinformationen zu generieren.
root/USB/Devices/<UUID>/ProductID	Legt die Produkt-ID des Geräts fest.
root/USB/Devices/<UUID>/State	Legt fest, ob das Gerät dem Remote-Host wie folgt zugeordnet ist: 0 = Nicht umleiten; 1 = Standardeinstellungen verwenden; 2 = Umleitung.
root/USB/Devices/<UUID>/VendorID	Legt die Vendor-ID des Geräts fest.
root/USB/root/autoSwitchProtocol	Wenn der Wert 1 ist, wird das Remote-USB-Protokoll basierend auf dem ausgewählten Protokoll automatisch umgeschaltet.
root/USB/root/mass-storage/allowed	Wenn der Wert 1 ist, werden Massenspeichergeräte automatisch bereitgestellt, wenn das Protokoll `local` ist.
root/USB/root/mass-storage/read-only	Wenn der Wert 1 ist und wenn Massenspeichergeräte automatisch bereitgestellt werden, werden diese schreibgeschützt bereitgestellt.
root/USB/root/opendebug	Wenn der Wert 1 ist, wird eine Debug-Nachricht auf `/tmp/USB-mgr-log` geschrieben.
root/USB/root/protocol	Legt das Protokoll fest, dem Remote-USB zugewiesen ist. Gültige Werte sind abhängig von den auf dem System installierten Protokollen, können jedoch `local`, `xen`, `freerdp` und `View` einschließen.

root > auto-update

Tabelle E-24 root > auto-update

Registrierungsschlüssel	Beschreibung
root/auto-update/DNSAliasDir	Legt das Standard-Root-Verzeichnis für den DNS-Alias-Modus auf dem Server fest, der HP Smart Client-Dienste hostet.
root/auto-update/ManualUpdate	Wenn der Wert 1 ist, sind die DHCP-Kennung, die DNS-Alias und die Aktualisierungsmethoden der Übertragung für Automatic Update deaktiviert. Wenn eine manuelle Aktualisierung durchgeführt wird, müssen die Registrierungsschlüssel `password`, `path`, `protocol`, `user` und `ServerURL` eingestellt werden, um sicherzustellen, dass der Updateserver bekannt ist.
root/auto-update/ScheduledScan/Enabled	Wenn der Wert 1 ist, prüft der Thin Client in regelmäßigen Abständen den Automatic Update-Server, um nach Aktualisierungen zu suchen. Wenn der Wert 0 ist, wird vom Thin Client nur beim Systemstart auf Aktualisierungen geprüft.

Tabelle E-24 root > auto-update (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/auto-update/ScheduledScan/Interval	Legt die Zeit fest, die zwischen geplanten Updates gewartet wird. Dies sollte im Format HH:MM angegeben werden. Mehr als 24-Stunden-Intervalle können angegeben werden. Beispiel: um alle 48 Stunden auftretende Scans zu haben, stellen Sie hier 48:00 ein.
root/auto-update/ScheduledScan/Period	Thin Clients aktivieren die geplante Prüfung während des definierten Zeitraums nach dem Zufallsprinzip. Die Verwendung längerer Zeitabstände verhindert Fälle, in denen alle Thin Clients zur gleichen Zeit aktualisiert werden, was eine Netzwerküberlastung verursachen könnte. Die Dauer sollte im Format HH:MM angegeben werden. Beispiel: Um die Thin Client-Aktualisierungen über einen Zeitraum von 2,5 Stunden zu verteilen, stellen Sie hier 02:30 ein.
root/auto-update/ScheduledScan/StartTime	Legt die Startzeit von der ersten Periode des geplanten Update-Scans im Format HH:MM fest, unter Verwendung des 24-Stunden-Zeitformats. Beispiel: 4:35 nachmittags wäre 16:35.
root/auto-update/ServerURL	Legt die IP-Adresse oder den Domännamen des Update-Servers fest, der verwendet wird, wenn ManualUpdate aktiviert ist.
root/auto-update/VisibleInSystray	Wenn der Wert 1 ist, dann ist die Automatic Update-Taskleistensymbol aktiviert.
root/auto-update/enableOnBootup	Wenn der Wert 1 ist, dann ist die automatische Aktualisierung beim Systemstart aktiviert.
root/auto-update/enableSystrayLeftClickMenu	Wenn der Wert 1 ist, dann ist das Linksklick-Menü für das Automatic Update-Taskleistensymbol aktiviert.
root/auto-update/enableSystrayRightClickMenu	Wenn der Wert 1 ist, dann ist das Rechtsklick-Menü für das Automatic Update-Taskleistensymbol aktiviert.
root/auto-update/gui/auto-update/ManualUpdate	Zum Einstellen des Status für das Widget **Enable manual configuration** 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 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

Tabelle E-24 root > auto-update (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	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 Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
`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`	Legt das Kennwort fest, das verwendet wird, wenn `ManualUpdate` aktiviert ist. Dies wird nur verwendet, wenn das `protocol` auf `ftp` eingestellt ist. Dieser Wert ist normalerweise verschlüsselt.
`root/auto-update/path`	Legt den relativen Pfad von der Standard-Server-URL fest, wenn `ManualUpdate` aktiviert ist. Dies ist normalerweise leer oder auf `auto-update` eingestellt.
`root/auto-update/preserveConfig`	Wenn der Wert 1 ist, dann werden die aktuellen Einstellungen der Thin Client-Konfiguration bei einem Image-Update über Automatic Update beibehalten.
`root/auto-update/protocol`	Legt das Protokoll fest, das verwendet wird, wenn `ManualUpdate` aktiviert ist.
`root/auto-update/tag`	Der Registrierungsschlüssel ist veraltet. Er hat zuvor die für DHCP (137) verwendete Tag-Nummer festgelegt. Dies wird jetzt über den Tag-Namen `Auto-Update` erkannt.
`root/auto-update/user`	Legt den Benutzernamen fest, der verwendet wird, wenn `ManualUpdate` aktiviert ist. Dies wird nur verwendet, wenn 'Protocol' auf 'ftp' eingestellt ist.

root > background

Tabelle E-25 root > background

Registrierungsschlüssel	Beschreibung
`root/background/desktop/color`	Durch die Einstellung von `theme` auf `none` für das Design, speichert dieser Schlüssel die Standardfarbe, die das benutzerdefinierte Design verwendet.
`root/background/desktop/imagePath`	Durch die Einstellung von `theme` auf `none` für das Design, speichert dieser Schlüssel den Image-Pfad des Desktop-Hintergrunds, die das benutzerdefinierte Design verwendet.

Tabelle E-25 root > background (Fortsetzung)

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

root > config-wizard

Tabelle E-26 root > config-wizard

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

root > desktop

Tabelle E-27 root > desktop

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

root > entries

Tabelle E-28 root > entries

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

root > keyboard

Tabelle E-29 root > keyboard

Registrierungsschlüssel	Beschreibung
root/keyboard/DrawLocaleLetter	Wenn der Wert 1 ist, dann wird das Tastatur-Taskleistensymbol die lokale Sprachzeichenfolge statt statischer Bilder verwenden.
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 Sprach-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	Wenn Auswahl 1 ist, dann wird das Tastatur-Taskleistensymbol angezeigt, und gibt das aktuelle Tastaturlayout an.
root/keyboard/XkbLayout	Dies ist ein interner Schlüssel, der verwendet wird, um ein XKB-Tastaturlayout zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbModel	Dies ist ein interner Schlüssel, der verwendet wird, um ein XKB-Tastaturmodell zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbOptions	Dies ist ein interner Schlüssel, der verwendet wird, um XKB-Tastaturoptionen zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/XkbVariant	Dies ist ein interner Schlüssel, der verwendet wird, um eine XKB-Tastaturvariante zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/enable2	Wenn der Wert 1 ist, dann kann über die durch switch definierte Tastenkombination auf das sekundäre Tastaturlayout umgeschaltet werden.

Tabelle E-29 root > keyboard (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/keyboard/layout	Legt das primäre Tastaturlayout fest.
root/keyboard/layout2	Legt das sekundäre Tastaturlayout fest.
root/keyboard/model	Legt das primäre Tastaturmodell fest.
root/keyboard/model2	Legt das sekundäre Tastaturmodell fest.
root/keyboard/numlock	Wenn der Wert 1 ist, dann wird die Funktion NUM Lock beim Systemstart aktiviert.
root/keyboard/rdp_kb	Dies ist ein interner Schlüssel, der verwendet wird, um eine RDP-Tastaturkarte zuzuordnen. Dieser Schlüssel sollte keine Änderung erfordern.
root/keyboard/switch	Legt die Tastenkombination zum Umschalten zwischen dem ersten und dem zweiten Tastaturlayout fest (enable2 muss auch auf 1 eingestellt sein). Gültige Werte sind wie folgt: grp:ctrl_shift_toggle, grp:ctrl_alt_toggle, grp:alt_shift_toggle.
root/keyboard/variant	Legt die primäre Tastaturvariante fest.
root/keyboard/variant2	Legt die sekundäre Tastaturvariante fest.

root > logging

Tabelle E-30 root > logging

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

root > mouse

Tabelle E-31 root > mouse

Registrierungsschlüssel	Beschreibung
root/mouse/MouseHandedness	Wenn der Wert 0 ist, dann ist die Maus für Rechtshänder. Wenn der Wert 1 ist, dann ist die Maus für Linkshänder.
root/mouse/MouseSpeed	Legt die Beschleunigung des Mauszeigers fest. In der Regel ist ein Wert von 0 bis 25 der nutzbare Bereich. Ein Wert von 0 deaktiviert

Tabelle E-31 root > mouse (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	die Beschleunigung vollständig, wodurch die Maus sich in einem konstant langsamen, aber messbaren Tempo bewegt.
root/mouse/MouseThreshold	Legt die Anzahl an Pixeln fest, bevor Mausbeschleunigung aktiviert wird. Ein Wert von 0 legt die Beschleunigung als eine natürliche Kurve fest, welche die Beschleunigung graduell skaliert, sodass sowohl präzise als auch schnelle Bewegungen möglich sind.

root > restore-points

Tabelle E-32 root > restore-points

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

root > screensaver

Tabelle E-33 root > screensaver

Registrierungsschlüssel	Beschreibung
root/screensaver/SlideShowAllMonitors	Wenn der Wert 1 ist, wird die Bildschirmschoner-Diashow auf allen Monitoren angezeigt. Wenn der Wert 0 ist, wird die Diashow nur auf dem primären Monitor angezeigt.
root/screensaver/SlideShowInterval	Legt das Intervall in Sekunden für Bilderwechsel in der Bildschirmschoner-Diashow fest.
root/screensaver/SlideShowPath	Gibt das Verzeichnis an, das die Bilder für die Bildschirmschoner-Diashow enthält.
root/screensaver/enableCustomLogo	Wenn der Wert 1 ist, dann werden die in LogoPath definierten, benutzerdefinierten Image für den Bildschirmschoner verwendet.
root/screensaver/enableDPMS	Wenn der Wert 0 ist, dann ist die Monitor-Energieverwaltung deaktiviert. Dies bewirkt, dass der Monitor eingeschaltet bleibt, bis er manuell ausgeschaltet wird.
root/screensaver/enableScreensaver	Bei Einstellung des Werts auf 1 wird der Bildschirmschoner aktiviert.
root/screensaver/enableSleep	Wenn der Wert 1 ist, dann ist der Energiesparmodus aktiviert.
root/screensaver/lockScreen	Bei Auswahl von 1, ist ein Kennwort erforderlich, um vom Bildschirmschoner zum Desktop zurückkehren.
root/screensaver/logoPath	Legt den Pfad zu einem benutzerdefinierten Image für den Bildschirmschoner fest.
root/screensaver/mode	Legt den wiedergebenden Modus für die Anzeige des Bildschirmschoners fest (z. B. Center, Tile und Stretch). Bei Auswahl von Default (Standard), wird das Bild ohne jegliche Verarbeitung angezeigt. Wenn der Wert SlideShow ist,

Tabelle E-33 root > screensaver (Fortsetzung)

Registrierungsschlüssel	Beschreibung
	durchläuft der Bildschirmschoner die Bilder im Verzeichnis, das von `SlideShowPath` angegebene wird.
`root/screensaver/off`	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Monitor ausgeschaltet wird.
`root/screensaver/origImageCopyPath`	Dies ist der Pfad, auf dem das benutzerdefinierte Image gespeichert ist, wenn `mode` auf `Default` eingestellt ist.
`root/screensaver/standby`	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Monitor in den Standby-Modus wechselt.
`root/screensaver/suspend`	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Monitor in den Suspend-Modus wechselt.
`root/screensaver/timeoutScreensaver`	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Bildschirmschoner startet.
`root/screensaver/timeoutSleep`	Legt die Zeitüberschreitung-Zeitverzögerung in Minuten fest, bevor der Thin Client in den Sleep-Modus wechselt.

root > security

Tabelle E-34 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

Tabelle E-35 root > sshd

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

root > time

Tabelle E-36 root > time

Registrierungsschlüssel	Beschreibung
`root/time/NTPServers`	Gibt zu verwendende NTP-Server über eine Liste mit Kommas als Trennzeichen an. 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.

Tabelle E-36 root > time (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/time/TimeServerIPAddress	Dies ist der Zeitserver, der vom Linux-Befehl net verwendet wird. Diese Server sind in der Regel die DC-Server im Unternehmensnetzwerk. Dies sollte verwendet werden, wenn NTP-Server nicht konfiguriert sind oder nicht auf Tastatureingaben reagieren. Der Linux-Befehl net identifiziert diese Server selbstständig. Es kann hier jedoch eine spezifische Server-IP-Adresse bereitgestellt werden, falls gewünscht.
root/time/WebServerURL	Legt die Web-Server-URL (wie hp.com) fest, die verwendet wird, wenn unter Verwendung des http-Protokoll die Zeit abgerufen wird. Diese URL kann sich innerhalb des Intranets oder im Internet befinden.
root/time/timezone	Legt die Zeitzone fest. Zeitzonen sollten angegeben werden, wie von **Linux Timezone** (Linux Zeitzone) im Dienstprogramm für **Date and Time** (Datum und Uhrzeit) in der Systemsteuerung definiert und sollten in folgendem Format sein: <region>/<subregion>.
root/time/use24HourFormat	Falls auf -1 festgelegt, wählt das System das Format automatisch entsprechend dem Gebietsschema. Bei Einstellung des Werts auf 0 wird das englische Format a.m./p.m. verwendet. Bei Einstellung des Werts auf 1 wird das 24-Stunden-Format verwendet.
root/time/useDHCPTimezone	Wenn der Wert 1 ist, versucht der Thin Client, die Zeitzone über DHCP einzustellen. Um die Zeitzone über diesen Registrierungsschlüssel korrekt einzustellen, stellen Sie sicher, dass der DHCP-Server für den Thin Client die DHCP-Kennung tcode weiterleitet (was normalerweise die Kennung 101 ist, jedoch auch 100 und 2 sein kann).
root/time/useNTPServers	Wenn der Wert 1 ist, ist die Verwendung von NTP-Zeitservern zum Synchronisieren der Thin Client-Uhr aktiviert. Wenn dies aktiviert ist, stellen Sie sicher, dass ein NTP-Server über DHCP oder über NTPServers angegeben ist.

root > touchscreen

Tabelle E-37 root > touchscreen

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

Tabelle E-37 root > touchscreen (Fortsetzung)

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

root > translation

Tabelle E-38 root > translation

Registrierungsschlüssel	Beschreibung
root/translation/coreSettings/localeMapping/<LanguageCode>	Dies sind interne Tasten, die verwendet werden, um die Textzeichenfolge neben der entsprechenden Sprache in der Sprachauswahl bereitzustellen. Dieser Schlüssel sollte keine Änderung erfordern.
root/translation/coreSettings/localeSettings	Legt das Gebietsschema für den Thin Client fest. Dieses Gebietsschema wird außerdem an die Remote-Verbindung weitergeleitet. Gültige Gebietsschemas sind en_US (Englisch), de_DE (Deutsch), es_ES (Spanisch), fr_FR (Französisch), ru_RU (Russisch), ja_JP (Japanisch), ko_KR (Koreanisch), zh_CN (vereinfachtes Chinesisch) und zh_TW (traditionelles Chinesisch).
root/translation/gui/LocaleManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/translation/gui/LocaleManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/translation/gui/LocaleManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/translation/gui/LocaleManager/widgets/localeSettings	Zum Einstellen des Widgets „Locale Setting“ (Gebietsschema-Einstellung) in den USA. 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 > usb-update

Tabelle E-39 root > usb-update

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

root > users

Tabelle E-40 root > users

Registrierungsschlüssel	Beschreibung
root/users/gui/hptc-user-rights/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/gui/hptc-user-rights/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/gui/hptc-user-rights/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/root/password	Legt das Administratorkennwort fest. Wenn leer, ist der Administratormodus gesperrt.
root/users/user/SSO	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/user/WOL	Wenn der Wert 1 ist, wird Wake-on-LAN (WOL) aktiviert.
root/users/user/XHostCheck	Wenn der Wert 1 ist, dann sind nur die in Root/Users/User/Xhosts aufgelisteten Systeme in der Lage, den Thin Client Remote zu steuern.
root/users/user/apps/hptc-ad-dns-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **AD/DDNS Manager** für Benutzer aktiviert.
root/users/user/apps/hptc-agent-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **HPDM Agent** für Benutzer aktiviert.
root/users/user/apps/hptc-auto-update/authorized	Bei Einstellung des Werts auf 1 wird das Element **Automatic Update** (automatisches Update) für Benutzer aktiviert.
root/users/user/apps/hptc-background-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Background Manager** (Hintergrundmanager) für Benutzer aktiviert.
root/users/user/apps/hptc-cert-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Certificate Manager** (Zertifkatsmanager) für Benutzer aktiviert.
root/users/user/apps/hptc-clientaggregation-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Client Aggregation** (Clientaggregation) für Benutzer aktiviert.
root/users/user/apps/hptc-date-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Date and Time** (Datum und Uhrzeit) für Benutzer aktiviert.
root/users/user/apps/hptc-dhcp-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **DHCP Option Manager** (DHCP Optionsmanager) für Benutzer aktiviert.
root/users/user/apps/hptc-display-prefs/authorized	Bei Einstellung des Werts auf 1 wird das Element **Display Preferences** (Anzeigeneinstellungen) für Benutzer aktiviert.
root/users/user/apps/hptc-easy-update/authorized	Bei Einstellung des Werts auf 1 wird das Element **Easy Update** (Leichtes Update) für Benutzer aktiviert.
root/users/user/apps/hptc-i18n-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Language** (Sprache) für Benutzer aktiviert.
root/users/user/apps/hptc-keyboard-layout/authorized	Bei Einstellung des Werts auf 1 wird das Element **Keyboard Layout** (Tastaturlayout) für Benutzer aktiviert.

Tabelle E-40 root > users (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/users/user/apps/hptc-mixer/authorized	Bei Einstellung des Werts auf 1 wird das Element **Sound** (Audio) für Benutzer aktiviert.
root/users/user/apps/hptc-mouse/authorized	Bei Einstellung des Werts auf 1 wird das Element **Mouse** (Maus) für Benutzer aktiviert.
root/users/user/apps/hptc-network-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Network Manager** (Netzwerkmanager) für Benutzer aktiviert.
root/users/user/apps/hptc-printer-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Printers** (Drucker) für Benutzer aktiviert.
root/users/user/apps/hptc-restore/authorized	Bei Einstellung des Werts auf 1 wird das Element **Snapshots** (Schnappschüsse) für Benutzer aktiviert.
root/users/user/apps/hptc-screenlock-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Screensaver** (Bildschirmschoner) für Benutzer aktiviert.
root/users/user/apps/hptc-security/authorized	Bei Einstellung des Werts auf 1 wird das Element **Security** (Sicherheit) für Benutzer aktiviert.
root/users/user/apps/hptc-shortcut-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Keyboard Shortcut Manager** (Manager für Tastaturverknüpfungen) für Benutzer aktiviert.
root/users/user/apps/hptc-sshd-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **SSHD Manager** (SSHD Manager) für Benutzer aktiviert.
root/users/user/apps/hptc-task-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **Task Manager** (Taskmanager) für Benutzer aktiviert.
root/users/user/apps/hptc-text-editor/authorized	Bei Einstellung des Werts auf 1 wird das Element **Text Editor** (Texteditor) für Benutzer aktiviert.
root/users/user/apps/hptc-thinstate/authorized	Bei Einstellung des Werts auf 1 wird das Element **ThinState** (ThinState) für Benutzer aktiviert.
root/users/user/apps/hptc-touchscreen/authorized	Bei Einstellung des Werts auf 1 wird das Element **Touch Screen** (Touchbildschirm) für Benutzer aktiviert.
root/users/user/apps/hptc-usb-mgr/authorized	Bei Einstellung des Werts auf 1 wird das Element **USB Manager** (USB-Manager) für Benutzer aktiviert.
root/users/user/apps/hptc-user-rights/authorized	Bei Einstellung des Werts auf 1 wird das Element **Customization Center** (Anpassungszentrum) für Benutzer aktiviert.
root/users/user/apps/hptc-vncshadow/authorized	Bei Einstellung des Werts auf 1 wird das Element **VNC Shadow** für Benutzer aktiviert.
root/users/user/apps/hptc-xterm/authorized	Bei Einstellung des Werts auf 1 wird das Element **X Terminal** (X-Terminal) für Benutzer aktiviert. **ACHTUNG:** Das Aktivieren des Zugriffs auf ein X-Terminal stellt ein Sicherheitsrisiko dar und wird in einer Produktionsumgebung nicht empfohlen. Das X-Terminal sollte nur zur Verwendung der Fehlersuche (Debugging) in geschützten, nicht produktiven Umgebung aktiviert werden.
root/users/user/apps/scim-setup/authorized	Bei Einstellung des Werts auf 1 wird das Element **SCIM Input Method Setup** (Einrichten der SCIm Eingabemethode) für Benutzer aktiviert.

Tabelle E-40 root > users (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/users/user/hideDesktopPanel	Bei Einstellung des Werts auf 1 werden Desktop-Bedienfelder, wie z. B. die Taskleiste, nicht gestartet oder auf dem Desktop angezeigt.
root/users/user/kioskMode	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/user/launchConnectionManager	Wenn der Wert 1 ist, dann wird der Verbindungsmanager beim Systemstart gestartet.
root/users/user/rightclick	Wenn der Wert 1 ist, dann ist das Rechtsklick-Menü für den Desktop aktiviert.
root/users/user/ssoconnectiontype	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/users/user/switchAdmin	Bei Einstellung des Werts auf 1 wird der Administratormodus aktiviert.
root/users/user/xhosts/<UUID>/xhost	Gibt die IP-Adresse oder den Hostnamen eines Systems an, die bzw. der Zugriff zur Remotesteuerung des Thin Clients erhalten soll, wenn XHostCheck aktiviert ist.

root > vncserver

Tabelle E-41 root > vncserver

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

Tabelle E-41 root > vncserver (Fortsetzung)

Registrierungsschlüssel	Beschreibung
root/vncserver/coreSettings/vncTakeEffectRightNow	Wenn der Wert 1 ist, dann werden VNC-Einstellungen sofort wirksam, nachdem sie geändert wurden.
root/vncserver/coreSettings/vncUsePassword	Wenn der Wert 1 ist, dann ist das in VncPassword angegebene Kennwort für VNC-shadowing erforderlich.
root/vncserver/coreSettings/vncUseSSL	Wenn der Wert 1 ist, dann wird SSL für VNC-Verbindungen verwendet.
root/vncserver/gui/VNCShadowManager/name	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/vncserver/gui/VNCShadowManager/status	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
root/vncserver/gui/VNCShadowManager/title	Dieser Registrierungsschlüssel ist entweder intern verwendet oder für zukünftige Verwendung reserviert. Der Wert sollte nicht geändert werden.
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 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 des numerischen Widget 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/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.

Tabelle E-41 root > vncserver (Fortsetzung)

Registrierungsschlüssel	Beschreibung
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 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/vncUseSSL	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 11
Add-Ons 1
Aktualisieren von Thin Clients
  Aktualisieren per DHCP-Kennung 70
  Aktualisieren per DNS-Alias 71
  Aktualisierung per Übertragung 70
  Manuelle Aktualisierung 71
Anzeigeeinstellungen 15
Anzeigeprofile 15
Audioeinstellungen 10
Audioumleitung
  RDP 49
  VMware Horizon View 56
Auslieferungszustand 11

B

Background Manager 10
Benutzeroberfläche
  Navigieren 6
Bildschirmschoner-Einstellungen 10

C

Certificate Manager 26
Citrix
  Einstellungen, allgemeine 36
  Einstellungen, verbindungsspezifisch 39
  HDX MediaStream 33
  HP True Graphics 34
  Supportmatrix 35
Clientaggregation 13
  Clientkonfiguration 14
  Serverkonfiguration 15
Connection Manager-Bedienelemente 7
Custom-Verbindungen 67

D

Datums- und Uhrzeiteinstellungen 10
DHCP-Optionen 27
Drucker 16
Druckerkonfiguration 75
Druckerumleitung
  RDP 49
  VMware Horizon View 56

E

Easy Update 11
Einführung 4

F

Fehlerbeseitigung 78
  Firmware-Beschädigung 79
  Netzwerkverbindung 78
  verwenden der Systemdiagnose 79

G

Geräteumleitung
  RDP 47
  VMware Horizon View 55

H

HDX MediaStream 33
HP Device Manager. *Siehe* HPDM Agent
HPDM Agent 11
HP Smart Client Services
  Installation 68
  Profile Editor. *Siehe* Profile Editor
  Übersicht 68
  unterstützte Betriebssysteme 68
HP TeemTalk. *Siehe* TeemTalk
HP Velocity 20

I

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

K

Kennwörter, ändern 10
Kioskmodus 30
Komponenten-Manager 20
Konfiguration eines parallelen Druckers 75
Konfiguration eines seriellen Druckers 75

M

Massenspeicherumleitung
  RDP 48
  VMware Horizon View 55
Mauseinstellungen 10
MMR
  VMware Horizon View 55
Momentaufnahmen 11
Multimedia-Umleitung
  RDP 47

N

Netzwerkeinstellungen
  DNS 19
  drahtgebunden 17
  HP Velocity 20
  IPSec 19
  VPN 20
  Wireless 18
  Zugreifen 17

P

Profile Editor
  verwenden 72

R

RDP
  Audioumleitung 49
  Druckerumleitung 49
  Einstellungen, allgemeine 41
  Einstellungen, verbindungsspezifisch 42
  Geräteumleitung 47
  Massenspeicherumleitung 48
  Multimedia-Umleitung 47
  Multi-Monitor-Sitzungen 47
  RemoteFX 46
  Smart Card-Umleitung 50
  USB-Umleitung 48
Registrierungsschlüssel 94

RemoteFX 46
RFX. *Siehe* RemoteFX

S
SCEP Manager 12, 27
SCIM 10
Serial Manager 12
Sicherheitseinstellungen 10
Smart Card-Umleitung
RDP 50
VMware Horizon View 57
Smart Zero-Anmeldebildschirm
Anpassen 85
Snipping Tool 12
So finden Sie weitere Informationsquellen 1
Spracheinstellungen 10
SSH 65
SSHD Manager 11
Systemdiagnose 79
System information (Systeminformationen)
Anzeigen 8
Systeminformations-Bildschirmanzeigen
Ausblenden 8
Systemsteuerung
AD/DDNS Manager 11
Anpassungscenter 10
Auslieferungszustand 11
Bildschirmschoner 10
Client Aggregation (Clientaggregation) 13
Datum und Uhrzeit 10
DHCP Options Manager 27
Dienstprogramme, ausblenden 10
Display Preferences (Anzeigeeinstellungen) 15
Easy Update 11
Hintergrundeinstellungen 10
Komponenten-Manager 20
Language (Sprache) 10
Maus 10
Momentaufnahmen 11
Netzwerk 17
SCEP Manager 12
SCIM Input Method Setup (Einstellung der Eingabemethode) 10
Security (Sicherheit) 10
Serial Manager 12
Snipping Tool 12
Sound 10
SSHD Manager 11
Task Manager 12
Tastenkombinationen 12
Text Editor 12
ThinState. *Siehe* HP ThinState
Touchscreen 10
Übersicht 9
VNC Shadow 26
Wireless-Statistiken 12
X Terminal 12

T
Taskleiste
Verwenden 6
Task Manager 12
Tastenkombinationen 12
TeemTalk 62
Telnet 66
Text Editor 12
Thin Clients
Aktualisieren. *Siehe* Aktualisieren von Thin Clients
ThinPro-Profil
Ändern 72
Hinzufügen eines symbolischen Links 75
Hinzufügen von Dateien 74
Laden 72
Registrierungseinstellungen 73
Speichern 75
Zertifikate 74
ThinState. *Siehe* HP ThinState
Touchscreen-Einstellungen 10

U
USB-Umleitung
RDP 48
USB-Manager 16
VMware Horizon View 55

V
Verbindungen
Ausblenden 10
Gemeinsame Einstellungen 29
Typen 2
VMware Horizon View
Audioumleitung 56
Druckerumleitung 56
Einstellungen 51
Geräteumleitung 55
Massenspeicherumleitung 55
MMR 55
Multi-Monitor-Sitzungen 54
Protokolle ändern 58
Sicherheitsstufen von Zertifikaten 58
Smart Card-Umleitung 57
Tastaturbefehle 55
USB-Umleitung 55
Webcamumleitung 57
Zertifikate 58
VNC-Shadowing 26

W
Web Browser
Einstellungen, allgemeine 60
Einstellungen, verbindungsspezifisch 60
Webcamumleitung
VMware Horizon View 57
Webseiten
Citrix-Support 1
HP-Support 1
Microsoft-Support 1
VMware-Support 1
Wireless-Statistiken 12

X
XDMCP 64
X Terminal 12

Z
Zertifikate
Installation 26
VMware Horizon View 58